ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE

Votre référence	Notre référence	Annexe(s)	Date
	DA250007		30.09.2025

<u>Objet :</u> Avis relatif à la proposition de loi modifiant la loi du 5 août 1992 sur la fonction de police et le Code d'instruction criminelle en ce qui concerne l'utilisation de techniques d'enquête policières disruptives en ligne et l'extension de la recherche numérique (DOC 56 0791/001).

L'Organe de contrôle de l'information policière (ci-après le 'COC' ou 'l'Organe de contrôle').

Vu la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (*M.B.* du 5 septembre 2018, ci-après 'la LPD'), en particulier l'article 59 §1er, 2e alinéa, l'article 71 et le Titre 7, en particulier l'article 236.

Vu la loi du 3 décembre 2017 portant création de l'Autorité de protection des données (ci-après 'la LAPD').

Vu la loi du 5 août 1992 sur la fonction de police (ci-après 'la LFP').

Vu la *Law Enforcement Directive* 2016/680 du 27 avril 2016 (ci-après 'la *LED*').

Vu la loi du 25 décembre 2016 relative au traitement des données des passagers.

Vu la transmission en date du 17 juillet 2025, par l'Autorité de protection des données (ci-après 'l'APD'), de la demande du Président de la Chambre des Représentants dans le cadre du principe du guichet unique (cf. article 54/1 §1er de la LAPD).

Vu le rapport de Monsieur Ronny Saelens, Membre-conseiller *a.i.* de l'Organe de contrôle.

Émet, le 30 septembre 2025, l'avis suivant.

I. Remarque préalable concernant la compétence de l'Organe de contrôle

1. À la lumière respectivement de l'application et de la transposition du Règlement 2016/679[1] et de la Directive 2016/680[2], le législateur a remanié en profondeur les tâches et missions de l'Organe de contrôle. L'article 4 §2, quatrième alinéa de la loi du 3 décembre 2017 portant création de l'Autorité de protection des données (ci-après 'la LAPD') dispose qu'à l'égard des services de police au sens de l'article 2, 2°, de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux, les compétences, missions et pouvoirs d'autorité de contrôle tels que prévus par le Règlement 2016/679 sont exercés par l'Organe de contrôle. Cela signifie notamment que l'Organe de contrôle est compétent également lorsque des services de police traitent des données à caractère personnel qui ne relèvent pas des missions de police administrative et judiciaire, par exemple dans le cadre de finalités socioéconomiques ou de traitements relevant de la gestion des ressources humaines. L'Organe de contrôle doit être consulté lors de la préparation de la législation ou d'une mesure réglementaire ayant trait au traitement de données à caractère personnel par les services de police de la police intégrée (voir les articles 59 §1er, 2e alinéa et 236 §2 de la LPD, l'article 36.4 du RGPD et l'article 28.2 de la directive Police-Justice). L'Organe de contrôle a dans ce contexte pour mission d'examiner si l'activité de traitement projetée par les services de police est conforme aux dispositions du Titre 1er (pour les traitements non opérationnels)[3] et du Titre 2 (pour les traitements opérationnels) de la LPD[4]. De plus, le COC est aussi chargé d'émettre des avis d'initiative, comme prévu à l'article 236 §2 de la LPD, et est investi conformément à l'article 240 de la LPD d'une mission générale d'information à l'égard du grand public, des personnes concernées, des responsables du traitement et des sous-traitants dans le domaine du droit à la protection des données et à la protection de la vie privée.

2. En ce qui concerne en particulier les activités de traitement dans le cadre des missions de police administrative et/ou judiciaire, l'Organe de contrôle émet dès lors des avis soit d'initiative, soit à la demande du Gouvernement ou de la Chambre des Représentants, d'une autorité administrative ou judiciaire ou d'un service de police, concernant toute matière ayant trait à la gestion de l'information policière telle que régie par la Section 12 du Chapitre 4 de la loi sur la fonction de police[5].

---

[1] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 *« relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE »* (règlement général sur la protection des données ou « RGPD »).

[2] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 *« relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil »* (ci-après dénommée « directive Police-Justice » ou *Law Enforcement Directive* (*LED*)).

[3] Article 4 §2, 4e alinéa de la LAPD.

[4] Article 71 §1er, 3e alinéa de la LPD.

[5] Articles 59 §1er, 2e alinéa et 236 §2 de la LPD.

3. Par ailleurs, l'Organe de contrôle est également chargé, à l'égard des services de police, de l'inspection générale de la police fédérale et de la police locale (en abrégé 'AIG') visée dans la loi du 15 mai 2007 sur l'Inspection générale et de l'Unité d'information des passagers (ci-après dénommée en abrégé 'BELPIU') visée au Chapitre 7 de la loi du 25 décembre 2016, de la surveillance de l'application du Titre 2 de la LPD et/ou du traitement de données à caractère personnel tel que visé aux articles 44/1 à 44/11/13 de la loi sur la fonction de police, et/ou de toute autre mission qui lui est confiée en vertu ou par d'autres lois[6].

4. L'Organe de contrôle est compétent à l'égard du Service Contentieux de l'Administration générale des Douanes et Accises en ce qui concerne les réquisitions adressées par ce service à la BELPIU dans des matières fiscales, et ce en vertu de l'article 281 §4 de la loi générale *« sur les douanes et accises »* du 18 juillet 1977, telle que modifiée par la loi du 16 mai 2024 *« modifiant la loi du 25 décembre 2016 relative au traitement des données des passagers »*.

5. Enfin, l'Organe de contrôle est également chargé, dans le cadre de la législation sur la rétention des données et en vertu de l'article 126/3 §1er, 8e alinéa de la loi du 13 juin 2005 relative aux communications électroniques (ci-après 'la LCE'), telle que modifiée par la loi du 20 juillet 2022 relative à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités (*M.B.* du 8 août 2022), de la validation des statistiques relatives au nombre de faits punissables et au délai de conservation pour chaque arrondissement judiciaire et chaque zone de police, une matière dans le cadre de laquelle il exerce toutes les compétences qui lui ont été attribuées par le Titre 7 de la loi du 30 juillet 2018. Il est par ailleurs également chargé, en application de l'article 42 §3, 2e et 3e alinéas de la LFP, du contrôle des requêtes de la Cellule Personnes disparues de la police fédérale en vue de la consultation des données relatives aux communications électroniques impliquant la personne disparue.

6. L'Organe de contrôle est compétent pour rendre des avis sur les aspects ayant trait au traitement des informations et des données à caractère personnel et à la protection de la vie privée par le traitement de données à caractère personnel pour autant qu'il existe un rapport avec le fonctionnement opérationnel et non opérationnel des services de police et/ou avec le personnel de la police intégrée (ci-après 'la GPI[7]') et/ou pour autant que le projet de texte soumis pour avis ait un impact sur la gestion de l'information policière en général.

7. Par ailleurs, l'Organe de contrôle n'est pas seulement une autorité de protection des données, mais est aussi une autorité de contrôle qui est légalement chargée de contrôler la légalité, l'efficacité, l'efficience et l'économie de la gestion de l'information policière[8].

---

[6] Article 71 §1er, troisième alinéa *juncto* article 236 §3 de la LPD.
[7] Geïntegreerde politie – Police Intégrée.
[8] Rapport d'activité 2021, www.organedecontrole.be, voir les points 3 et 52 et plus spécifiquement le point 71 : *« Il serait cependant faux de s'imaginer que le COC se préoccupe seulement de la protection des données ; il porte aussi énormément*

II. Objet de la demande

8. La demande d'avis a trait à une proposition de loi modifiant la loi du 5 août 1992 sur la fonction de police et le Code d'instruction criminelle en ce qui concerne l'utilisation de techniques d'enquête policières disruptives en ligne et l'extension de la recherche numérique (ci-après 'la proposition de loi'), déposée par Mesdames Sophie De Wit et Kristien van Vaerenbergh et Monsieur Christoph D'Haese.

9. À travers la proposition de loi, ses auteurs souhaitent par essence fournir également à la police une base légale explicite pour l'utilisation de techniques 'disruptives' (préventives) (outils) dans le cadre de l'exercice de missions de police administrative et judiciaire en ligne (c'est-à-dire dans le monde dit numérique ou virtuel). Il s'agit en réalité de permettre (également), en marge des méthodes (judiciaires) purement répressives, le recours à des techniques disruptives afin de ralentir les agissements punissables et de protéger les victimes[9].

Il convient d'emblée de faire remarquer que les auteurs de la proposition de loi ont omis de définir dans le corps de la proposition ce qu'il y a lieu d'entendre exactement par 'méthodes disruptives'. Selon les exemples évoqués dans l'exposé des motifs (outil développé en collaboration avec des hackers éthiques (*White Hat Hackers*), technique d'inondation (*flooding*), …), il s'agit (ou peut s'agir) somme toute déjà d'un exercice de la fonction de police judiciaire étant donné que des suspects sont visés (même s'ils ne sont pas nécessairement déjà identifiés à ce moment). Même lorsque la finalité consiste à éviter des victimes, il se peut parfaitement qu'il soit déjà question d'une enquête pénale, ou au moins d'un exercice de la fonction de police judiciaire. Les techniques (policières) disruptives peuvent donc se situer et se situeront souvent à la limite de la fonction de police administrative et de la fonction de police judiciaire. Leur nature exacte dépendra en fin de compte des circonstances concrètes, sachant que certains actes de police administrative peuvent rapidement relever de la police judiciaire.

Selon les auteurs de la proposition de loi, il s'impose de modifier la législation *« pour permettre aux services de police, dans un premier temps, d'empêcher que des personnes soient victimes d'actes de cybercriminalité et, dans un deuxième temps, de poursuivre effectivement les cybercriminels »*[10].

10. Les auteurs de la proposition de loi souhaitent à cette fin modifier d'une part l'article 26 de la loi sur la fonction de police (LFP), et d'autre part les articles 28*bis* et 46*sexies* du Code d'instruction criminelle. La première modification vise à étendre la portée du terme *« lieux accessibles au public »*

---

d'attention à tous les autres aspects opérationnels de la gestion de l'information policière et des informations des autres services qu'il contrôle, s'agissant là de matières relevant également de sa compétence. » ; article 71 §1er de la LPD.

[9] Exposé des motifs de la proposition de loi, p. 3.

[10] Exposé des motifs de la proposition de loi, p. 4.

qui est utilisé à l'article 26 de la LFP aux lieux accessibles au public dans le monde (l'environnement) virtuel (numérique) dans le cadre de l'exercice des missions générales de police administrative et judiciaire. Pour ce qui est de la deuxième modification, la proposition de loi prévoit d'une part de viser explicitement l'enquête proactive dans l'environnement numérique, et d'autre part de déléguer au Roi la compétence de préciser les techniques d'enquête policières virtuelles dans le cadre de l'infiltration en ligne par arrêté délibéré en Conseil des ministres, sur la proposition du ministre de la Justice et après avis du Collège des procureurs généraux.

11. À titre préliminaire, le COC se demande comment la proposition de loi se positionne par rapport au projet de loi annoncé dans l'exposé d'orientation politique du 14 mars 2025 du ministre de la Sécurité et de l'Intérieur[11] qui vise à rendre légalement possibles les *patrouilles sur Internet*, s'agissant d'un objectif qui est également poursuivi par la présente proposition de loi[12]. Bien que les membres de la Chambre des Représentants soient évidemment libres de déposer des propositions de loi, on peut tout de même s'interroger sur l'intérêt (avantage) social de disposer potentiellement de deux initiatives législatives parallèles poursuivant au moins en partie le même objectif, voire se recoupant (ce qui risque de nuire à la qualité du cadre normatif projeté, d'une part, et à la sécurité juridique du citoyen, d'autre part). Il semble donc indiqué de prévoir au moins une concertation avec le(s) ministre(s) compétent(s) afin d'éviter d'adopter en parallèle deux textes poursuivant par essence le même objectif.

12. Le COC se prononcera sur les aspects qui présentent un lien direct avec ses missions et compétences légales susmentionnées à l'égard de la police. Le COC n'est en effet pas compétent à l'égard des autorités judiciaires, ce qui n'empêche évidemment pas que l'efficacité, l'efficience et surtout la légalité de l'action policière sont liées au traitement d'informations et de données à caractère personnel effectué sur cette base par la GPI (gestion de l'information).

La proposition de loi comporte 3 articles opérationnels (les projets d'articles 2, 3 et 4), parmi lesquels seul le projet d'article 2 prévoit une modification de la LFP, et plus précisément de l'article 26 susmentionné de ladite loi. Les projets d'articles 3 et 4 ont toutefois eux aussi un impact sur la gestion de l'information telle qu'elle est réglementée dans la LFP dès lors que les missions de police judiciaire induisent le traitement d'informations et de données à caractère personnel dans les banques de données policières opérationnelles visées à l'article 44/2 §1er de la LFP.

[11] Doc. Parl. *Chambre* 2024-2025, n° 56-0767/019, p. 17.
[12] Exposé des motifs relatif à l'article 2 de la proposition de loi, p. 4.

III. Analyse de la demande

A) Antécédents et remarques générales

13. La proposition de modifier l'article 26 de la LFP n'est pas nouvelle.

Déjà en date du 13 mai 2015, c'est-à-dire il y a plus de 10 ans, l'Autorité de protection des données (auparavant la Commission de la protection de la vie privée) a émis un avis au sujet des *« avant-projets de loi portant dispositions diverses – modifications de la loi portant création d'un organe de recours en matière d'habilitations de sécurité, de la loi sur la fonction de police et de la loi du 18 mars 2014 relative à la gestion de l'information policière »* introduits à l'époque (avis n° 13/2015). L'article 10 de l'avant-projet n° 2 de l'époque visait une modification de l'article 26 de la LFP identique à celle proposée à présent. Dans cet avis, l'Autorité de protection des données s'était aux points 14 à 32 inclus exprimée dans des termes critiques au sujet du projet d'article 10, pour ensuite formuler aux points 33 et 34 des propositions d'amendements. L'article 26 de la LFP n'avait finalement pas été modifié.

14. Le projet d'article 2 de l'actuelle proposition de loi se propose de modifier l'article 26 de la LFP en y insérant un alinéa rédigé comme suit :
« Pour l'application de la présente loi, les lieux accessibles au public sur l'internet ou sur d'autres réseaux de communications électroniques, que leur accès requière ou non certaines formalités de forme, sont assimilés à des lieux accessibles au public. Les fonctionnaires de police peuvent visiter ces lieux, les étudier et en réaliser des copies. ».

15. Le COC constate que l'actuel projet d'article 2 est une reproduction exacte du projet d'article 10 susmentionné de l'avant-projet sur lequel l'APD s'est prononcée dans son avis du 13 mai 2015 évoqué plus haut. Les remarques susmentionnées formulées par l'APD dans son avis du 13 mai 2015 restent par conséquent pertinentes, en marge des remarques complémentaires et spécifiques qui sont formulées ci-après compte tenu de l'état actuel de la loi et de la technologie.

16. L'exposé des motifs relatif à l'article 2 de la proposition de loi[13] fait référence à l'arrêt de la Cour de cassation du 28 mars 2017. Selon les auteurs de la proposition de loi, cet arrêt confirme que la portée de la notion de *« lieux accessibles au public »* visée à l'article 26 de la LFP s'étend aussi aux lieux accessibles au public dans le monde en ligne (interprétation évolutive de la disposition). Bien que le COC puisse sur ce point se rallier à la conclusion des auteurs de la proposition de loi, il fait remarquer que la Cour ne s'est **pas** à proprement parler prononcée sur la portée de l'exercice des compétences et missions policières générales sur Internet. La signification de l'arrêt susmentionné de la Cour de

[13] Exposé des motifs de la proposition de loi, p. 4.

cassation doit donc être interprétée avec la prudence qui s'impose, dès lors que l'actuelle proposition de loi dépasse manifestement les questions juridiques qui avaient été posées à la Cour de cassation et auxquelles cette dernière avait répondu. En effet, contrairement à ce que les auteurs de la proposition de loi semblent et/ou pensent pouvoir déduire de l'arrêt de la Cour de cassation[14], **la Cour de cassation ne devait pas se prononcer sur l'exercice de missions de police administrative dans des lieux accessibles au public de l'environnement en ligne (monde virtuel), et ne l'a d'ailleurs pas fait. Il n'a pas non plus été demandé à la Cour si le fait d'accéder à ces lieux sur Internet en utilisant un système informatique (ordinateur, tablette, smartphone), (1) s'inscrit dans le cadre légal régissant le *traitement* d'informations et de *données à caractère personnel* visées à l'article 44/1 §1er de la LFP (article 26, 1° et 2° de la LPD) ni (2) si ce traitement doit ou non être considéré comme un *« moyen technique »* au sens de l'article 47*sexies*, 2e et 3e alinéas du Code d'instruction criminelle.** La seule chose que la Cour souligne dans cet arrêt – par souci d'exhaustivité – est le fait que sa décision ne porte nullement préjudice à l'application de la loi concernant les méthodes particulières de recherche (MPR) (autrement dit, des articles applicables du Code d'instruction criminelle relatifs aux MPR). **Le COC estime donc qu'il est indispensable, dans l'intérêt de la sécurité juridique, d'analyser et de clarifier la zone de tension – ou du moins la relation – qui existe entre les objectifs de la modification projetée de l'article 26 de la LFP d'une part et l'article 47*sexies*, 2e et 3e alinéas du Code d'instruction criminelle d'autre part[15].**

B) Remarques spécifiques

17. Le projet d'article 2 étend le terme *« lieux fermés accessibles au public »* aux *« lieux accessibles au public sur l'internet ou sur d'autres réseaux de communications électroniques »*. La distinction entre l'internet et les réseaux de communications électroniques manque de clarté. Le COC recommande, pour autant que telle soit l'intention des auteurs de la proposition de loi, de faire référence dans le projet d'article à l'article 2, 3° de la loi du 13 juin 2005 relative aux communications électroniques, où il est également question de l'internet sous la définition de la notion de *« service de communications électroniques »* (art. 2, 5°) et de *« service d'accès à l'internet »*.

18. Selon le même projet d'article, les fonctionnaires de police peuvent *« visiter ces lieux, les étudier et en réaliser des copies »*. La proposition de loi ne le précise pas, mais le COC part du principe que les termes *« visiter »* et *« étudier »* sont censés correspondre aux termes utilisés à l'article 26 de la LFP, à savoir *« pénétrer »* dans ces lieux et *« veiller »* au maintien de l'ordre public (comme on peut le déduire de l'arrêt susmentionné du 28 mars 2017 de la Cour de cassation). Si telle est en effet l'intention des auteurs de la proposition de loi, il est recommandé de le préciser dans l'exposé des

[14] Exposé des motifs relatif à l'article 2 de la proposition de loi, p. 4, 1er alinéa *in fine*.
[15] Voir par exemple en l'occurrence, en ce qui concerne l'utilisation non visible de caméras de police en application de la LFP et la zone de tension qui existe avec la réglementation des méthodes particulières de recherche, les articles 47*ter* et 47*sexies* du Code d'instruction criminelle et l'arrêt de la Cour de cassation du 8 juillet 2025, P.25.0964.N, www.juportal.be.

motifs relatif au projet d'article. Un autre point qui manque de clarté est ce que l'on entend par *« en réaliser des copies »*. Pour autant que les auteurs veuillent ainsi concrétiser l'application de l'article 26, 1° et 2° de la LPD lu conjointement avec l'article 44/1 §1er de la LFP (qui constitue la disposition de base pour le traitement d'informations et données à caractère personnel policières et concrétise les principes de nécessité et de proportionnalité visés à l'article 28, 2°, 3° et 5° de la LPD), les auteurs sont priés de le préciser explicitement à la fin du projet d'article 2 et de motiver ce choix dans l'exposé des motifs relatif au projet d'article. C'est en effet ici qu'apparaît une différence substantielle entre *patrouiller* dans le monde réel et *patrouiller* en ligne. La collecte et, le cas échéant, la conservation de données à caractère personnel doivent dans les deux cas être considérées comme un *« traitement »* au sens des dispositions légales susmentionnées. Mais alors que dans le cadre d'une patrouille de police classique (mission de police administrative) effectuée dans le monde réel, il n'est pas procédé au traitement de données à caractère personnel lorsque les observations ne peuvent pas être mises en relation avec des troubles de l'ordre public, il en va tout autrement lors d'une patrouille sur Internet. Lors d'une patrouille sur Internet, il arrivera souvent que des données à caractère personnel soient *collectées* (et donc traitées) (involontairement ou automatiquement) même en l'absence de faits pouvant être mis en relation avec des troubles de l'ordre public ou des faits pénaux. Il en va de même lorsque la police n'a *ab initio* pas l'intention de traiter des informations et des données à caractère personnel qui ne sont pas nécessaires et/ou proportionnelles. On peut donc se demander comment ce traitement de données peut être concilié avec l'article 44/1 §1er de la LFP, qui autorise uniquement le traitement d'informations et de données à caractère personnel pour autant que ces dernières présentent un caractère adéquat, pertinent et non excessif. À ce titre, il est recommandé de remplacer dans le projet d'article les termes *« étudier »* et *« en réaliser des copies »* par *« et traiter des informations et données à caractère personnel conformément à l'article 44/1 §1er de la présente loi »*. Cela signifie que la police ne peut pas conserver les données à caractère personnel qu'elle collecte en ligne lorsque ces données n'ont aucune nécessité ou valeur opérationnelle, et que seules des données à caractère personnel pertinentes (d'un point de vue opérationnel) sont par conséquent collectées et conservées.

19. Au point 28 de son avis susmentionné du 13 mai 2015, l'APD faisait remarquer que les limites de l'intervention autonome de la police devaient être clairement définies dans le projet d'article (soumis à l'époque), afin d'éviter que la surveillance d'Internet et les patrouilles sur Internet, qui constituent en soi une finalité légitime, ne dérivent en observations ou en infiltrations sans que les garanties de l'intégralité de la législation sur les méthodes particulières de recherche et du Code d'instruction criminelle ne soient d'application. Cette remarque se rapportait à un amendement que l'APD préconisait au point 33 de son avis, et qui consistait à ajouter à la fin du projet d'article la phrase suivante : *« Ils ne peuvent toutefois pas adopter une identité fictive crédible, ni utiliser des documents fictifs et ils ne peuvent avoir la moindre interaction personnelle avec une personne. »*[16]. L'article

[16] Cf. Europol, *Policing in an online world. Relevance in the 21st century*, 2024 : *« Online policing (also called online patrolling or net patrolling) is typically conducted through visible, uniformed patrolling on digital platforms frequented by citizens, with a*

46*sexies* §1er, 4e alinéa du Code d'instruction criminelle[17] a dans l'intervalle apporté une réponse partielle à cette remarque (à savoir pour la fonction de police judiciaire) en faisant en sorte de ne pas toucher à l'intervention autonome de la police visée à l'article 26 de la LFP, évidemment sans préjudice de l'application des dispositions pertinentes du Code d'instruction criminelle. À ce sujet, on peut lire dans l'exposé des motifs de la proposition de loi : *« Il est prévu, en substance, qu'il ne pourra pas y avoir de contacts prolongés entre l'agent et le suspect au cours d'une intervention autonome menée en application de l'article 26 de la loi sur la fonction de police. En cas de contacts prolongés, les règles spécifiques encadrant l'infiltration sur Internet (article 46sexies du Code d'instruction criminelle) seront en effet d'application. À l'inverse, au cours de cette première phase, dont l'objectif premier sera d'éviter des victimes, tout contact prolongé entre l'agent et le suspect sera exclu, en principe, si bien que l'article 26 précité pourra effectivement s'appliquer. »*[18].

La proposition d'ajout formulée par l'APD au sujet du projet de deuxième alinéa de l'article 26 de la LFP reste donc pertinente, de sorte que le COC demande d'ajouter à l'article 2 la phrase suivante (légèrement amendée)[19] : *« Ils ne peuvent toutefois pas adopter une identité fictive crédible, ni utiliser des documents fictifs et ils ne peuvent avoir la moindre interaction personnelle prolongée avec une personne. »*.

20. L'intention des auteurs de la proposition de loi est donc de considérer les contacts sur Internet entre la police et des *suspects*, lorsqu'ils ne sont pas prolongés, comme une mission policière autonome de police administrative et judiciaire relevant de l'application de l'article 26 de la LFP, sans qu'il ne faille appliquer notamment les articles 28*bis* (l'enquête proactive) et 46*sexies* du Code d'instruction criminelle (l'infiltration en ligne après autorisation du procureur du Roi ou du juge d'instruction). Pour autant qu'il faille appliquer l'article *28bis* du Code d'instruction criminelle, les auteurs de la proposition de loi souhaitent prévoir au projet d'article 3 de la proposition de loi de compléter l'article 28*bis* §2 du Code d'instruction criminelle d'un alinéa additionnel rédigé comme suit : *« L'enquête proactive s'étend également à l'internet ou à d'autres réseaux de communications électroniques. »*.

21. À cet égard, le projet d'article 4 de la proposition de loi prévoit de compléter l'article 46*sexies* §1er du Code d'instruction criminelle d'un alinéa habilitant le procureur du Roi à autoriser les services de

specific emphasis on building trust, crime prevention and crime disruption, although it may also involve preliminary investigative case building. », p. 6.

[17] *« Le présent article ne s'applique pas à l'interaction personnelle de fonctionnaires de police, dans l'exercice de leurs missions de police judiciaire, avec une ou plusieurs personnes sur Internet, qui n'a pour finalité directe qu'une vérification ciblée ou une arrestation, et ceci sans utiliser d'identité fictive crédible. »*. Article 46*sexies* du Code d'instruction criminelle, inséré par la loi du 25 décembre 2016 portant des modifications diverses au Code d'instruction criminelle et au Code pénal, en vue d'améliorer les méthodes particulières de recherche et certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications et créant une banque de données des empreintes vocales.

[18] Exposé des motifs de la proposition de loi, p. 5.

[19] L'amendement consistant en l'ajout du terme *« prolongée »*.

police à recourir à certaines *« techniques d'enquête »* policières virtuelles qui, comme nous le faisions remarquer plus haut au point 10, seront précisées par le Roi.

22. Ces articles cadrent donc clairement et exclusivement dans l'exercice de missions de police judiciaire, dans le cadre desquelles le traitement de données sera en règle générale ciblé, ce qui atténue en principe le risque d'un traitement de données (vraiment) excessif. Ce risque est par contre manifestement plus grand lors de patrouilles dans le monde en ligne, lesquelles cadrent dans une mission de police administrative et impliquent également une interaction entre les fonctionnaires de police et les citoyens. À cet égard, la remarque de l'APD (cf. point 19) demeure pertinente.

23. Dans le cadre de l'exercice de missions de police administrative et judiciaire dans l'environnement en ligne, la GPI recourt souvent pour 'visiter' l'internet à des outils d'*OSINT* (*Open Source Intelligence*) qui sont librement disponibles sur Internet (commercialement ou non). L'utilisateur (la police) n'a généralement aucune idée ni connaissance de l'architecture ni des logiciels sous-jacents de l'outil d'*OSINT*, ni a fortiori du système d'IA (intelligence artificielle) qui est utilisé. La police oublie souvent dans ce contexte qu'elle est responsable du respect des obligations découlant de la législation (européenne) qui s'applique à la police en matière de protection des données[20] et dans l'intervalle aussi (additionnellement) pour l'utilisation de systèmes d'IA[21].

Le COC préconise donc de profiter de l'occasion pour harmoniser la présente proposition de loi et/ou le projet de loi annoncé par le ministre de la Sécurité et de l'Intérieur avec la législation d'exécution qui est actuellement en cours d'élaboration (par le Gouvernement) pour la mise en œuvre du règlement européen sur l'intelligence artificielle.

PAR CES MOTIFS,

l'Organe de contrôle de l'information policière

[20] Il arrive fréquemment que les données policières soient traitées par un 'sous-traitant' (article 53 de la LPD) et un 'sous-traitant du sous-traitant', auquel cas on ignore souvent si le sous-traitant (du sous-traitant) est établi dans l'EEE ou dans un pays tiers (sachant que dans ce dernier cas, des garanties additionnelles sont requises pour le traitement de données à caractère personnel).

[21] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle).

prie le demandeur de tenir compte des remarques susmentionnées.

Avis approuvé par l'Organe de contrôle de l'information policière le 30 septembre 2025.

Pour l'Organe de contrôle,
Le président *a.i.,*
Frank SCHUERMANS (Sé)