Autorité de protection des données
Gegevensbeschermingsautoriteit

Avis n° 79/2025 du 11 septembre 2025

Objet : Avis concernant 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* (CO-A-2025-095)

Mots-clés : Titre 2 de la LTD - Directive (UE) 2016/680 - recherche proactive - cybercriminalité - ministère public - indépendance du pouvoir judiciaire - principe de légalité

Traduction

Le Service d'Autorisation et d'Avis de l'Autorité de protection des données (ci-après : l'Autorité) ;

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

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE* (ci-après : le RGPD) ;

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

Vu la demande d'avis de Monsieur Peter De Roover, Président de la Chambre des représentants, (ci-après : le demandeur), reçue le 17 juillet 2025 ;

Émet, le 11 septembre 2025, l'avis suivant :

I. Objet et contexte de la demande d'avis

1. Le 17 juillet 2025, le demandeur a sollicité l'avis de l'Autorité concernant 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 : le projet).

2. L'Exposé des motifs énonce qu'afin de lutter de manière efficace contre la cybercriminalité, il ne suffit pas d'adopter une stratégie purement répressive. Il convient donc de procéder à une révision fondamentale de la stratégie, à savoir passer de la répression à des méthodes innovantes et disruptives, pouvant être déployées directement.

3. On peut citer parmi ces techniques un outil d'intelligence artificielle développé par un fournisseur de télécommunications britannique en collaboration avec des hackers éthiques (*White Hat Hackers*), qui se fait passer pour une victime potentielle et mène de longues 'conversations' avec les cybercriminels afin de ralentir leurs activités. Une initiative similaire a été mise en place par la Computer Crime Unit de la Police judiciaire fédérale d'Anvers.

4. Cette technique d'inondation (*flooding*) empêche les cybercriminels de distinguer les véritables victimes des victimes fictives. En outre, des "vulnérabilités" ont été découvertes au niveau des *phishing panels*, permettant aux services de police d'en prendre le contrôle et d'identifier tant les victimes que les auteurs. La mise en œuvre concrète de cette technique requiert cependant une base légale qui n'existe pas encore aujourd'hui. Le projet tente de remédier à cette 'lacune'.

5. Les 'techniques disruptives' envisagées peuvent se répartir en deux phases, selon leur finalité. L'objectif de la première phase est d'éviter des victimes sans encore rassembler de preuves ou arrêter des auteurs. L'Exposé des motifs précise que cela consiste en : "*la possibilité d'accomplir les missions de police administrative en ligne également, en 'patrouillant sur internet', le démantèlement,* [NdT : il convient de lire "en démantelant"] *les réseaux criminels spécialisés dans l'hameçonnage, en les inondant de fausses victimes (sans qu'il s'agisse d'identités fictives), et le démantèlement de* [NdT : il convient de lire "en démantelant des"] *sites frauduleux liés aux cryptomonnaies en leur envoyant aussi des informations erronées ou une grande quantité de données inutiles, de manière à les faire planter.*"

6. Ainsi, le projet modifie l'article 26 de la loi du 5 août 1992 *sur la fonction de police* (ci-après : la loi sur la fonction de police) afin d'assimiler les lieux accessibles au public sur Internet ou sur d'autres réseaux de communications électroniques à des lieux accessibles au public. Ce qui est

crucial à cet égard, c'est qu'il ne pourra pas y avoir de contact prolongé entre l'agent et le suspect et que l'objectif premier est d'éviter des victimes.

7. La deuxième phase, lorsque les techniques policières à utiliser vont (doivent aller) plus loin, requiert de modifier l'article 28*bis* (relatif à l'enquête proactive) et l'article 46*sexies* (infiltration en ligne) du *Code d'Instruction criminelle*. L'article 28*bis*, § 2 du *Code d'instruction criminelle* est complété de manière à ce que l'enquête proactive s'étende également à Internet ou à d'autres réseaux de communications électroniques. À l'article 46*sexies*, § 1er du même Code, un alinéa est ajouté qui dispose ce qui suit : *"Le procureur du Roi peut également autoriser les services de police à recourir à certaines techniques d'enquête policières virtuelles, dans le cadre légal d'une infiltration et dans le respect de la finalité de celle-ci. Le Roi précise par un arrêté délibéré en Conseil des ministres, sur la proposition du ministre de la Justice et après avis du Collège des procureurs généraux, ces techniques d'enquête policières virtuelles."*

II. Examen quant au fond

8. En vertu de l'article 4, § 2, 4e alinéa de la LCA, 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 RGPD sont exercés par l'Organe de contrôle de l'information policière visé à l'article 44/6, § 1er de la loi *sur la fonction de police*[1]. Cette compétence de contrôle et d'avis s'étend à la fois aux traitements de données effectués par ces services de police et à la législation qui définit, modifie ou encadre d'une autre manière ces traitements. La modification de l'article 26 de loi *sur la fonction de police* ne relève donc pas de la compétence d'avis de l'Autorité.

9. Conformément au premier alinéa de ce même article, les traitements effectués par les autorités judiciaires (en ce compris le ministère public) dans le cadre de leurs missions judiciaires, comme par exemple l'octroi d'autorisations pour effectuer certains actes d'enquête, ne relèvent pas de la compétence de contrôle de l'Autorité.

10. Néanmoins, l'Autorité rappelle, comme expliqué en détail aux points 7 - 14 de l'avis n° 77/2020[2] (et confirmé ensuite dans l'avis n° 163/2023[3]), que "*Cette exclusion de la compétence de l'autorité de contrôle à l'égard des traitements liés à la fonction juridictionnelle vise le "contrôle" des*

[1] La présente demande d'avis a été transmise le 17 juillet 2025 au COC conformément à la procédure définie dans le protocole de coopération entre les autorités de contrôle fédérales belges en matière de protection des données. Consultable via le lien suivant : https://www.autoriteprotectiondonnees.be/publications/protocole-de-cooperation-entre-les-autorites-de-controle-federales-belges-en-matiere-de-protection-des-donnees.pdf.

[2] Consultable via le lien suivant : https://www.autoriteprotectiondonnees.be/publications/avis-n-77-2020.pdf.

[3] Consultable via le lien suivant : https://www.autoriteprotectiondonnees.be/publications/avis-n-163-2023.pdf.

"traitements" en ce domaine et ce, en vue de garantir l'indépendance du pouvoir judiciaire, et non "toute compétence" de l'Autorité à l'égard généralement, de la matière pénale. Autrement dit, elle n'exclut pas une compétence d'avis sur une législation, telle que celle en cause en l'espèce (...), se trouvant au cœur de la fonction juridictionnelle pénale."

11. La formulation d'avis ne porte en effet pas sur le contrôle du traitement de données à caractère personnel par le ministère public ou les cours et tribunaux, mais sur les actes posés par le pouvoir législatif, en exécution de sa fonction législative. Deuxièmement, l'exercice de cette compétence d'avis n'a pas d'impact sur l'indépendance du pouvoir judiciaire dans l'exercice de ses fonctions juridictionnelles.

12. Compte tenu donc du fait que les traitements qui découlent, le cas échéant, du projet ne relèvent pas en soi de la compétence d'avis et de contrôle de l'Autorité, cette dernière se limite à une analyse de l'impact des articles 3 et 4 du projet sur le droit à la protection des données. En outre, l'Autorité estime que, bien que l'extension des compétences en matière d'enquête proactive à Internet ou à d'autres moyens de communications électroniques, d'une part, et l'introduction de techniques d'enquête policières virtuelles – à définir plus précisément – dans le contexte de l'infiltration en ligne, d'autre part, puissent poursuivre un objectif légitime, il est regrettable, compte tenu de la nécessité et de la proportionnalité exigées pour de telles mesures, que les autorisations requises à cet égard soient délivrées par le procureur du Roi et non par le juge d'instruction.

13. En principe, l'État de droit prévoit en effet que les actes d'enquête tant classiques que numériques - dont par exemple les 'techniques d'enquête policières virtuelles[4]' - sont soumis au contrôle d'un juge indépendant et impartial (et ne peuvent donc pas être ordonnés uniquement par le ministère public)[5]. Le juge d'instruction remplit ce rôle étant donné que, contrairement au procureur du Roi, il n'est pas hiérarchiquement soumis à la politique du ministère public ou du ministre de la Justice, mais uniquement à la loi[6]. Dans la mesure en outre où le procureur du Roi intervient en tant que partie dans la procédure pénale, il convient d'éviter que l'instance qui engage les poursuites puisse également décider de manière unilatérale de la prise de certaines mesures (coercitives) qui représentent une ingérence importante dans les droits et libertés des personnes concernées.

14. En outre, lorsque ces techniques d'enquête policières virtuelles sont basées sur l'intelligence artificielle, l'Autorité souligne qu'il convient de tenir compte des obligations qui découlent du

[4] Dans la mesure où ces techniques doivent être définies ultérieurement, il est actuellement impossible pour l'Autorité de vérifier quel sera leur impact sur les droits et libertés des personnes concernées.

[5] Voir également dans ce contexte la jurisprudence de la Cour de justice de l'UE, et plus précisément les affaires jointes *C-511/18, C-512/18 et C-520/18 (La Quadrature du Net and Others), HvJ-EU (grande chambre), 6 octobre 2020, ECLI:EU:C:2020:791*.

[6] Voir l'article 151 de la *Constitution*.

Règlement (UE) 2024/1689 du Parlement européen et du Conseil *établissant des règles harmonisées concernant l'intelligence artificielle* (ci-après : le règlement IA). Ce règlement vise à créer un cadre uniforme pour l'utilisation de l'intelligence artificielle au sein de l'Union, en accordant une attention particulière à la gestion des risques, à la transparence et à la protection des droits fondamentaux. Lorsque dans le cadre d'une information ou d'une instruction judiciaire, le procureur du Roi (ou le juge d'instruction) autorise le recours à des systèmes d'IA - par exemple pour l'analyse de données, la reconnaissance de schémas ou des applications prédictives -, il convient de veiller à ce que ces techniques ne répondent pas uniquement aux exigences de proportionnalité et de légalité, telles que reprises dans le *Code d'instruction criminelle*, mais soient aussi conformes aux garanties matérielles et procédurales prescrites par le règlement IA.

15. Enfin, l'Autorité se demande, à la lumière du principe de légalité et de la nature des techniques d'enquête policières virtuelles, dans quelle mesure il est légitime que ces techniques soient déterminées par le Roi et pas par le parlement. À cet égard, l'Autorité rappelle que si ces techniques d'enquête impliquent un nouveau traitement de données à caractère personnel, il est requis, en vertu de l'article 6.3 du RGPD, lu en combinaison avec les articles 8 de la CEDH et 22 de la *Constitution*, que les éléments essentiels de ce traitement soient définis dans une norme légale formelle (et pas dans un arrêté d'exécution). Il s'agit à cet égard des éléments suivants[7] :
    - la (les) finalité(s) précise(s) et concrète(s) des traitements de données ;
    - la désignation du (des) responsable(s) du traitement (à moins que cela ne soit clair) ;
    - les (catégories de) données à caractère personnel traitées qui sont pertinentes et non excessives ;
    - les catégories de personnes concernées dont les données à caractère personnel seront traitées ;
    - les (catégories de) destinataires des données à caractère personnel ainsi que les circonstances dans lesquelles ils reçoivent les données et les motifs y afférents ;
    - le délai maximal de conservation des données à caractère personnel enregistrées ;
    - l'éventuelle limitation des obligations et/ou des droits visé(e)s aux articles 5, 12 à 22 et 34 du RGPD.

[7] Étant entendu que le niveau de précision requis ou la possibilité de développer certains aspects dans un arrêté d'exécution dépendent fortement de la gravité de l'ingérence, ainsi que de la nature et de l'ampleur des traitements de données prévus.

PAR CES MOTIFS
l'Autorité,

vu le fait que les traitements de données à caractère personnel prévus par le projet ne relèvent pas de sa compétence d'avis, se limite à la remarque générale que pour la garantie des droits et libertés des personnes concernées, il est en principe requis que des méthodes ou des techniques d'enquête intrusives puissent uniquement être ordonnées par un juge indépendant et impartial.

En outre, le demandeur doit vérifier dans quelle mesure, à la lumière du principe de légalité, il est légitime que la détermination des 'techniques d'enquête policières virtuelles' soit déléguée au Roi.

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