Autorité de protection des données
Gegevensbeschermingsautoriteit

Avis n° 69/2025 du 26 août 2025

Objet : Avis concernant la « Nationale Cybersecurity Strategie 3.0, 2026-2030 » (CO-A-2025-108).

Mots-clés : cybersécurité – stratégie – Centre pour la Cybersécurité Belgique.

Version originale

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

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

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

Vu la demande d'avis de Monsieur Bart De Wever, Premier ministre, reçue le 17 juillet 2025 ;

Le Service d'Autorisation et d'Avis de l'Autorité de protection des données (ci-après « l'Autorité ») émet, le 26 août 2025, l'avis suivant :

I. OBJET ET CONTEXTE DE LA DEMANDE D'AVIS

1. Le demandeur a introduit auprès de l'Autorité une demande d'avis concernant la « Nationale Cybersecurity Strategie 3.0, 2026-2030 » (ci-après, « **la Stratégie** ») qui a été préparée par le Centre pour la Cybersécurité Belgique (ci-après, « **le CCB** »).

2. L'article 28, § 1er, 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* (ci-après, « **la Loi NIS2** ») dispose en effet que « *Les ministres réunis en Conseil adoptent la stratégie nationale en matière de cybersécurité et la mettent à jour au moins tous les cinq ans, sur la base d'indicateurs de performance,* ***après avis*** *du Conseil national de sécurité, des autorités visées à l'article 15, du NCCN* ***et, le cas échéant, des autorités de protection des données*** » (mis en gras par l'Autorité). Et conformément à l'article 23, § 2, de la LCA, le Service d'Autorisation et d'Avis de l'Autorité « *exerce les autres pouvoirs d'avis et d'autorisation visés à l'article 58, § 3, du Règlement 2016/679, à l'exception du pouvoir visé à l'article 58, § 3, e) du Règlement 2016/679* ». Or la présente demande d'avis relève bien de l'article 58, § 3, du RGPD.

3. L'Autorité souligne néanmoins que l'essentiel de l'exercice de sa compétence d'avis porte sur des projets de textes normatifs[1] et non sur des textes de portée plus stratégique telle que la Stratégie soumise pour avis. De telle sorte que le présent avis sera **limité à certaines considérations en lien avec la protection des personnes physiques à l'égard du traitement des données à caractère personnel**, sans préjudice de toute position ultérieure à propos des règles régissant d'une manière ou d'une autre, la cybersécurité et les traitements de données à caractère personnel prévus dans ce domaine.

4. **L'Autorité rappelle également que ses avis sont en général focalisés sur les points à améliorer ou développer dans les projets soumis pour avis et ce, pour des raisons d'efficacité et compte-tenu des contraintes** dans lesquelles elle exerce sa compétence. Un avis ne peut donc pas être lu comme un commentaire exhaustif du projet soumis. Par exemple, en l'occurrence, l'Autorité n'insistera pas en particulier sur l'importance de la cybersécurité à laquelle la Stratégie est dédiée et renvoie à ce sujet, à celle-ci même. Mais il est **évident qu'elle soutient l'objectif général poursuivi par la Stratégie** qui d'ailleurs, comme les développements suivants le souligneront, opère en synergie avec la protection des données.

[1] Pour un cas particulier où sa compétence d'avis porte néanmoins sur des protocoles d'accord, voir l'article 9 de la loi du 21 mars 2007 *réglant l'installation et l'utilisation de caméras de surveillance*.

II. EXAMEN DE LA STRATEGIE

Le présent avis est structuré comme suit :

II.1. L'Autorité, un acteur public de la cybersécurité du niveau de pouvoir fédéral

5. Avant tout, **l'Autorité** attire l'attention du demandeur sur le fait qu'elle **considère être aussi un acteur du niveau de pouvoir fédéral disposant de compétences et d'expertise dans le domaine de la cybersécurité et de la sécurité de l'information en général**, **lorsqu'est impliqué un traitement de données à caractère personnel**. Notamment, **l'article 32 du RGPD** (« *Sécurité du traitement* »), imposant au responsable du traitement la mise en place de mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, et **les articles 33 et 34 du RGPD** concernant les violations de données à caractère personnel, illustrent clairement le rôle de l'Autorité dans le domaine de la sécurité. Dans ce cadre, protection des données et cybersécurité sont en synergie.

6. Plus concrètement, en 2024, **le Secrétariat Général de l'Autorité** a reçu 1455 notifications relatives à des violations de données, dont 35 ont été transmises au Service d'Inspection de l'Autorité[2]. Concernant les causes les plus fréquentes des violations de données, la catégorie « *hacking, phishing & malware* » représentait 35% des violations notifiées[3]. C'est à la suite de la notification d'une violation de données que **la Chambre Contentieuse** de l'Autorité s'est par exemple déjà prononcée dans une affaire impliquant un *ransomware* dans le milieu hospitalier[4].

---

[2] Voir le Rapport annuel 2024 de l'Autorité, disponible sur https://www.autoriteprotectiondonnees.be/publications/rapport-annuel-2024.pdf, p. 17.

[3] *Ibid.*, p. 52. 40% sont liées à une erreur humaine et 5% à un usage impropre des droits d'accès.

[4] Voir la Décision quant au fond 166/2024 du 17 décembre 2024, disponible sur https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n0-166-2024.pdf.

7. Le **Service d'Autorisation et d'Avis** s'exprime également dans sa pratique d'avis, sur des questions techniques de sécurité de l'information et de minimisation des données[5], et il est également compétent pour autoriser l'accès aux métadonnées de communications électroniques traitées par les opérateurs de télécommunications belges, par le CCB en tant que CSIRT National et par l'Institut Belge des Services Postaux et des Télécommunications (ci-après, « l'IBPT »), dans l'exercice de certaines de leurs missions[6]. La première autorisation délivrée par le Service d'Autorisation et d'Avis à l'IBPT est d'ailleurs relative à une recherche à mener concernant les vulnérabilités du protocole SS7[7]. A l'heure de la rédaction du présent avis, une première autorisation (non encore publiée) a également été délivrée au CCB (CSIRT National).

8. Enfin plus généralement, **les traitements de données à caractère personnel mis en œuvre afin de garantir la sécurité de systèmes d'information relèvent de la compétence générale de l'Autorité** qui doit en la matière, veiller à ce que soit atteint un juste équilibre entre les droits et libertés en présence, conforme à la Charte des droits fondamentaux de l'Union européenne, au RGPD, à la Convention Européenne des Droits de l'Homme et à la Constitution belge. Si légitimes puissent-ils être, les traitements de données à caractère personnel nécessaires à l'approche de la cybersécurité promue dans la Stratégie, une approche à la fois réactive et proactive, doivent être mis en œuvre conformément aux règles de protection des données.

9. Pour ces raisons, **l'Autorité est d'avis qu'elle devrait être renseignée dans la liste de la Stratégie reprenant les acteurs publics du niveau de pouvoir fédéral**, et introduite en ces termes : « *Verschillende publieke en private actoren dragen, elk vanuit hun eigen bevoegdheden en expertise, bij aan de realisatie van de missie en doelstellingen van deze cyberstrategie. De volgende entiteiten of organisaties (per categorie in alfabetische volgorde) spelen hierin een belangrijke rol op het gebied van cyberbeveiliging in ons land* »[8]. Ceci rejoint l'objectif opérationnel n° 1, sous le titre « *BEHEREN* » de la Stratégie : « *Een duidelijk overzicht van rollen en verantwoordelijkheden op het gebied van cyberbeveiliging definiëren en onderhouden* ». Notamment, **l'Autorité veille à la sécurité des traitements de données à caractère personnel**.

---

[5] Voir par exemple, Autorité de Protection des Données, Service d'Autorisation et d'Avis, « La pratique d'avis du Service d'Autorisation et d'Avis, Secteur public et obligations légales », 01/09/2024, disponible sur https://www.autoriteprotectiondonnees.be/index.php/publications/brochure-informative-le-secteur-public-et-obligations-legales.pdf, pp. 57 ; 60-67. Plus récemment, voir notamment, concernant un protocole d'accès en temps réel à des caméras de surveillance, l'Avis n° 118/2027 du 23 décembre 2024 *concernant un protocole d'accord réglementant l'accès en temps réel de la Police Fédérale aux images des caméras installées sur le réseau de la SNCB (CO-A-2024-268)*, considérants nos 67 et s., voir aussi la note de bas de page n° 15.

[6] Voir l'article 21, § 2, 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*, concernant le CCB (CSIRT National), et l'article 15 de la loi du 17 janvier 2003 *relative au statut du régulateur des secteurs des postes et des télécommunications belges*.

[7] Voir l'Autorisation (délivrée) n° 001/2024 du 6 novembre 2024 *concernant une demande d'autorisation visée à l'article 15, § 2, al. 2, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges (AH-2024-0010)*.

[8] Stratégie, pp. 32-33. La liste des acteurs publics du niveau de pouvoir fédéral comporte 22 entités dont Belnet, la police fédérale, la FSMA, la Banque Nationale, l'AFMPS, l'IBPT, le SPF BOSA, le SPF Economie et bien sûr le CCB lui-même.

II.2. Approche proactive de la sécurité et scans, analyses et monitoring continu de réseaux de communications électroniques, en temps réel

10. Deuxièmement, l'Autorité observe que la Stratégie développée met un accent important sur une **approche proactive de la cybersécurité et sur la nécessité y liée d'identifier rapidement les menaces** afin de pouvoir adopter dès que possible les contremesures pertinentes. Cette approche repose notamment sur la nécessité **de scans, d'analyses et de monitoring continu de réseaux, en temps réel**, augmentant la visibilité des menaces. Bref, il s'agit d'**une activité de surveillance et de collecte et de partage de renseignements et données renforcée, dans l'objectif d'assurer une meilleure cybersécurité en Belgique**.

11. Cette approche apparaît de manière transversale dans la Stratégie. Les extraits suivants des objectifs opérationnels (mis en gras par l'Autorité) l'illustrent effectivement :

- Objectif n° 8 (« *Extend Early Warning Systems* ») : le point II., reprenant les objectifs opérationnels nos 8 à 10, prévoit notamment que « *Door **realtime informatie, continue monitoring en mechanismen voor het delen** van bedreigingen te integreren, kunnen organisaties overschakelen van een reactieve houding naar een proactieve cybersecurity strategie* » ;

- Objectif n° 9 (« *Het scannen analyseren en delen van informatie over ketsbaarheden versterken* ») : « *Door de Belgische capaciteiten voor **het scannen** van kwetsbaarheden, analyse en **het delen van informatie** te versterken, kunnen we onze **zichtbaarheid** in onze meest kritieke kwetsbaarheden aanzienlijk verbeteren. Door digitaal België **beter te scannen op nationaal niveau** zal het CCB, samen met nationale en internationale partners, eigen **informatie over cyberdreigingen (CTI) verzamelen en produceren** die grondig kan worden geanalyseerd. Het doel is om kwetsbare systemen te identificeren en **hun eigenaars rechtstreeks te waarschuwen**, niet alleen van NIS2-entiteiten, maar **van alle organisaties in België**. Dit zal resulteren in **het delen van betere en gerichte informatie**, bekend als "Spear Warnings," een bedacht door het CCB* » ;

- Objectif n° 11 (« *Verminder e-fraude : een nationale noodzaak* ») : « *Effectieve en efficiënte maatregelen zijn essentieel voor dit initiatief. Ten eerste moet **de verzameling van informatie** over (potentiële) fraude worden **gestroomlijnd tussen alle betrokken partijen** om een volledige gegevensvergaring te garanderen* » ;

- Objectif n° 18 (« *Efficiënte AI-gestuurde dreigingsdetectiemechanismen implementeren* ») : « *Het CCB zal efficiënte **AI-gestuurde dreigingsdetectiemechanismen** implementeren om voorop te blijven lopen op cyberdreigingen in het snel evoluerende digitale landschap van vandaag. Het doel is om **sneller verdachte activiteiten te identificeren,** de responstijden te verkorten en mogelijke schade te minimaliseren **door continu netwerkverkeer te monitoren en analyseren*** » ;

- Objectif n° 19 (« *Netwerkverkeer op indicatoren van bedreigingen monitoren en analyseren* ») : « *De **monitoring en analyse van mogelijk kwaadaardig netwerkverkeer** zullen worden verbeterd om **dreigingsindicatoren in bijna real-time te identificeren**. Het CCB zal samenwerken met de relevante partners en het bestaande wettelijke kader implementeren. Het doel is om potentiële cyberdreigingen **snel te detecteren en erop te reageren,** waardoor de integriteit en veiligheid van de digitale infrastructuur van België wordt gewaarborgd* » ; « *Door **mogelijk kwaadaardig netwerkverkeer te monitoren en analyseren**, kunnen we deze communicatie ontdekken, de acties van de aanvaller analyseren, nieuwe kwaadaardige servers **detecteren** en nieuwe slachtoffers **identificeren** die zich mogelijk nog niet bewust zijn dat ze zijn gecompromitteerd. Deze **proactieve benadering** is cruciaal voor het handhaven van een robuuste cyberweerbaarheid* » ;

- Objectif n° 20 (« *Nauw samenwerken met cloudserviceproviders om de zichtbaarheid en responsmogelijkheden te verbeteren* ») : « *Het CCB blijft prioriteit geven aan **samenwerking met CSP's*** [9]*, waarbij cloudservices worden erkend als kritieke digitale activa. Dit partnerschap levert tastbare voordelen op, waaronder verbeterde beveiliging door **realtime dreigingsdetectie**, robuuste encryptie en gelaagde toegangscontroles* » ; « *Bovendien verbetert de samenwerking met CSP'sde **zichtbaarheid van gegevens**, risicobeheer en naleving, terwijl het **geavanceerde analyses en monitoring** mogelijk maakt voor betere besluitvorming* » ;

- Objectif n° 21 (« *Toegang tot duidelijk kwaadaardige infrastructuur blokkeren* ») : « *De infrastructuur die door aanvallers wordt gebruikt, is cruciaal voor het succes van cyberaanvallen. Door toegang tot deze infrastructuur te blokkeren, kunnen we onmiddellijk invloed uitoefenen op lopende aanvallen en hun effectiviteit verminderen. Dit vereist het in kaart brengen van kwaadaardige infrastructuur **door middel van diepgaande CyberThreat Intelligence (CTI) verzamelingen analyse,** zodat we weten wat we moeten blokkeren. Deze **proactieve maatregel** is essentieel voor het handhaven van een robuuste cyberweerbaarheid* » ;

[9] Cloudserviceproviders.

- Et enfin, objectif n° 23 (« *Verstoring door cyberincidenten minimaliseren* ») : « *Om de continuiteit van essentiële diensten te waarborgen, is een proactieve en gecoordineerde aanpak nodig waarmee* ***dreigingen snel kunnen worden geïdentificeerd en geneutraliseerd voordat ze escaleren*** » ; « *Om de veerkracht verder te vergroten, zal het CCB zijn incidentresponsteam versterken met een dubbele focus op reactieve* ***en proactieve capaciteiten****, waaronder het opsporen van bedreigingen, veiligheidsbeoordelingen en technische adviesdiensten. Deze evolutie van incidentafhandeling naar een volledige responscapaciteit zal de* ***detectiesnelheid aanzienlijk verbeteren*** *en de hersteltijd verkorten* ».

12. L'Autorité perçoit que c'est dans cette optique que s'est inscrite la première demande d'autorisation qui lui a été adressée par le CCB (CSIRT national), afin de pouvoir collecter auprès d'opérateurs de télécommunications, les métadonnées de toutes les communications électroniques ayant eu lieu depuis et vers des adresses IP listées dédiées au trafic de *Command-and-Control servers* malicieux ou C2-servers. L'objectif poursuivi est de pouvoir identifier sur cette base les victimes potentielles, et ensuite, de les avertir. Que ces victimes soient ou pas des entités essentielles ou importantes soumises aux obligations de la Loi NIS2. Dans cette autorisation, s'agissant du projet concret concerné, l'Autorité a souligné qu'il conviendrait que le législateur confirme que son intention était bien de permettre le traitement de métadonnées de ces entités ou personnes qui ne sont pas essentielles ou importantes au sens de la Loi NIS2, ceci étant moins clair -et donc prévisible - compte-tenu du dispositif de la Loi NIS2.

13. Dans ce contexte, l'Autorité est d'avis que **la Stratégie devrait également apporter,** dans la mesure du possible, **une visibilité plus concrète quant à ce que constituerait la surveillance, le monitoring continu et l'analyse en temps réel des réseaux de communications électroniques publics** (fournis par les opérateurs de télécommunications) **ou privés** (prestataires de services *cloud*, entreprises, etc.) **envisagés par le CCB,** afin que puissent être mieux perçus les **traitements de données à caractère personnel** (collectes, échanges, etc.) **nécessaires à cette fin**.

14. Elle attire également l'attention du demandeur sur **l'importance, dans la mise en œuvre de la Stratégie, de la distinction entre d'une part, les activités de prévention et de protection de nature purement technique** (et « civile » ; il s'agit de se protéger, de mettre en œuvre des mesures techniques limitant l'impact des menaces concernées ou les entravant), **et d'autre part, les activités de recherche et de répression des infractions par les autorités compétentes**, qu'il s'agisse de sanctionner des infractions liées à des violations de la Loi NIS2, à la cybercriminalité voire plus largement, à toute autre infraction découverte par le CCB à l'occasion de l'exercice de ses missions. En effet le CCB, selon ses compétences et la manière dont celles-ci sont exercées, est susceptible d'avoir un accès privilégié aux réseaux publics (des opérateurs) et privés d'entités (essentielles ou importantes, ou autre).

15. Enfin, l'Objectif n° 18 (« *Efficiënte AI-gestuurde dreigingsdetectiemechanismen implementeren* ») déjà évoqué dans le considérant n° 11, évoque encore « *Het implementeren van AI-gestuurde dreigingsdetectie als een nationale CSIRT omvat snelle en efficiënte diagnose tijdens incidenten,* ***continue monitoring, data-analyse en geautomatiseerde reacties*** » (mis en gras par l'Autorité). Sans entrer ici dans les détails de la récente réglementation européenne relative à **l'intelligence artificielle**[10], l'Autorité rappelle que **l'article 22 du RGPD** limite les possibilités de prises de décisions à l'égard d'une personne concernée fondées exclusivement sur un traitement de données automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire[11]. **Un encadrement normatif spécifique** peut être requis en la matière dans le cas où un tel scénario serait envisagé dans l'exécution de la Stratégie.

II.3. Identification électronique

16. La Stratégie aborde le sujet de l'**identification électronique** et exprime notamment ce qui suit, à son sujet :

> « *In België is het vanzelfsprekend dat* ***de overheid instaat voor het beheer van onze fysieke identiteit****, bijvoorbeeld via en identiteitskaarten.* ***Diezelfde willen we doortrekken de digitale wereld: het waarborgen van digitale identiteit*** *op een manier die betrouwbaar,* ***publiek gestuurd*** *en veilig is — zonder afhankelijk te zijn van buitenlandse, vaak niet-Europese technologiebedrijven. Nu reeds wordt in ons land toegang tot gevoelige informatie voornamelijk geregeld via een publiek-private samenwerkingen dit willen we verder zetten.*
>
> *Het uitgangspunt is duidelijk: er moet vermeden worden dat we evolueren naar een digitale samenleving waarin grote technologiebedrijven volledige controle uitoefenen over hoe we ons online identificeren en gedragen.*
>
> *Tegelijk* ***is het cruciaal dat ook overheidsoplossingen geen systeem worden waarmee het gedrag van burgers systematisch kan worden gemonitord****. Een volledig anonieme samenleving is echter niet realistisch of veilig. Hoewel we in het dagelijks leven meestal anoniem kunnen blijven, zijn er situaties waarin identificatie noodzakelijk is; denk aan het openen van een bankrekening of het nemen van een vlucht* » (mis en gras par l'Autorité).

---

[10] 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)*.

[11] Voir notamment « La pratique d'avis du Service d'Autorisation et d'Avis, Secteur public et obligations légales », pp. 46-48, cité à la note de bas de page n° 5.

17. Le Service d'Autorisation et d'Avis s'est prononcé relativement récemment dans le domaine de l'identification électronique, en se référant notamment au Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 *sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (ci-après, « Règlement EIDAS »)*, tel que modifié par le Règlement (UE) n° 2024/1183 du Parlement Européen et du Conseil du 11 avril 2024 *modifiant le Règlement (UE) n° 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique*[12] (ci-après, « **Règlement EIDAS** ») et aux **portefeuilles européens d'identité numérique**.

18. L'Autorité souligne dans ce contexte que, s'il est vrai qu'une identification doit être fiable, **celle-ci ne peut être requise que lorsqu'elle est nécessaire et dans la mesure où elle est nécessaire**, conformément au principe de minimisation des données, **à l'aune de la finalité poursuivie**. Il existe de très fréquentes situations dans lesquelles l'identification des personnes concernées n'est pas nécessaire en ligne, quel que soit le moyen ou service d'identification concerné (fourni par l'Etat ou autre). Il est aussi possible que seul un attribut doive être attesté, qu'une adresse e-mail, un mot de passe et un deuxième facteur d'identification suffisent, etc. Le Règlement eIDAS lui-même prévoit différents niveaux de confiance en matière d'identification électronique. Pour un utilisateur moyen, l'anonymat en ligne peut par ailleurs également s'avérer tout relatif, compte-tenu des nombreuses traces qu'il (doit) laisse(r), selon la technologie utilisée et les informations collectées par les prestataires de services divers impliqués, la présence d'une transaction financière, etc. Dans un tel contexte, l'exigence d'une identification ne peut pas non plus être utilisée pour collecter des données non nécessaires au sujet des personnes concernées.

19. Dans ce domaine, d'une part, **le contrôle et l'autonomie de la personne concernée sur son identification sont déterminants.** Ceci bien entendu, **sans préjudice des obligations légales d'identification** applicables dans certains secteurs spécifiques réglementés, comme le secteur bancaire évoqué dans la Stratégie. Obligations légales **qui doivent elles-mêmes garantir une mise en œuvre conforme des principes de finalité et de proportionnalité**, entre autres. D'autre part, comme la Stratégie le souligne à très juste titre, **il est crucial que les solutions d'identification en général, ne puissent pas permettre le monitoring des activités des personnes concernées**. Par exemple, le Règlement EIDAS consacre des obligations en ce sens s'agissant des portefeuilles européens d'identité numérique, et prévoit le « *contrôle total* » de la personne concernée sur les données la concernant[13].

---

[12] Voir l'Avis n° 14/2025 du 27 février 2025 *concernant une proposition de loi relative au partage de données provenant de sources authentiques avec les prestataires de services d'identification électronique agréés (DOC56 0330/001) et un amendement y lié (DOC56 0330/002) (CO-A-2025-003)*.

[13] Voir l'article 5*bis* , 1., 4., a), b), 14., 15. et 16., du Règlement EIDAS.

II.4. Chiffrement et chiffrement de bout en bout des communications électroniques

20. L'objectif opérationnel n° 16 est lié au **chiffrement en relation, en particulier, avec l'informatique quantique** (« *Aan een kwantumveilige en flexibele cryptografie / toekomstbestendige beveiliging bijdragen* »)[14]. Dans ce contexte, « *De CCB zal de ontwikkeling en verspreiding van een nationaal cryptografiebeleid, een roadmap en richtlijnen voor niet-geclassificeerdegegevens coordineren, in nauwe samenwerking met, en op basis van input van, de nationale, regionale en internationale contextpartners* ».

21. A ce sujet, l'Autorité a souligné dans un avis récent **l'importance de sauvegarder le chiffrement de bout en bout des communications électroniques**[15] et profite de l'opportunité de la présente demande d'avis pour insister de nouveau sur ce point. Sans redévelopper ici des considérations détaillées à ce sujet dans l'avis précité auquel il est renvoyé, un extrait de la position exprimée par le European Data Protection Board lui-même peut être énoncé : « *the EDPB stresses again* [EDPB-EDPS Joint Opinion 4/2022 and EPDB Statement 1/2024] *that encryption is* ***essential for ensuring the security and confidentiality of personal data and electronic communications****, as it provides strong technical safeguards against access to that information by anyone other than the user and the recipients chosen by him, including by the provider. In particular, in the context of interpersonal communications, genuine end-to-end encryption ('E2EE') covering the terminal devices and the data therein, with the decryption keys held solely by the users is a crucial tool for ensuring the confidentiality of electronic communications.* ***Preventing the use of encryption or weakening the effectivity of the protection it provides, would have a severe impact on the respect for private life and confidentiality of users, on their freedom of expression as well as on innovation and the growth of the digital economy, which relies on the high level of trust and confidence that such technologies provide*** »[16] (mis en gras par l'Autorité).

22. La Stratégie pourrait également rappeler le **rôle central du chiffrement de bout en bout des communications électroniques,** en matière de cybersécurité (confidentialité) et la nécessité y liée de **préserver et garantir son bon fonctionnement**.

---

[14] A ce sujet, voir notamment
https://www.nist.gov/cybersecurity/what-post-quantum-cryptography ;
https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards ;
dernièrement consultés le 31/07/2025.

[15] Voir l'Avis n° 16/2025 du 27 mars 2025 *d'initiative relatif à la Convention des Nations-Unies contre la cybercriminalité (CO-A-2025-019)*.

[16] EDPB, « Statement 5/2024 on the Recommendations of the Hight-Level Group on Access to Data for Effective Law Enforcement », adopté le 4 novembre 2024, point n° 3, disponible sur https://www.edpb.europa.eu/system/files/2024-11/edpb_statement_20241104_ontherecommendationsofthehlg_en.pdf, dernièrement consulté le 30/07/2025.

II.5. Souveraineté

23. L'objectif opérationnel n° 17 a trait à la **souveraineté** (« *Voor een Soevereine cloud zorgen en de soevereiniteit van gegevens waarborgen* ») et prévoit notamment que « *Het CCB werkt samen met nationale partners aan* ***de ontwikkeling van een Soevereine Cloud*** *als strategische prioriteit om de nationale digitale autonomie te waarborgen,* ***gegevenssoevereiniteit te garanderen en de afhankelijkheid van niet-EU cloudserviceproviders te verminderen****. In een tijdperk waarin cloud computing zowel publieke als sectoractiviteiten ondersteunt, is het essentieel om* ***controle te behouden over gevoelige gegevens binnen de jurisdictie van de EU om privacy te beschermen, naleving van regelgeving te waarborgen en nationale belangen te beschermen****. Dit initiatief integreert regelgevende, operationele en technische dimensies binnen een uniform controle en governance kader. Het waarborgt regelgevende soevereiniteit door afstemming op nationale en EU wetgevingskaders, inclusief transparante gegevensverwerking, beperkte buitenlandse invloed en volledige zichtbaarheid op (sub)verwerkers en metadataflows* » (mis en gras par l'Autorité).

24. L'Autorité considère également qu'une telle approche peut **avoir des effets positifs sur le plan de la protection des personnes concernées** à l'égard du traitement des données à caractère personnel, bien que le régime juridique consacré aux flux transfrontières de données dans le RGPD contribue à limiter les risques pour les personnes concernées dans l'environnement international hors Union. **Qu'un traitement de données relève exclusivement de la compétences d'Etats de l'Espace Economique Européen garantit une meilleure effectivité des standards européens de protection des données**.

II.6. Evaluation de l'efficacité des traitements de données à caractère personnel

25. Enfin, la Stratégie[17] prévoit que « *Het Centrum voor Cybersecurity België (CCB) zal een reeks* ***prestatie-indicatoren ontwikkelen om de voortgang en effectiviteit van de Nationale Cybersecurity Strategie te meten****. De indicatoren zullen* ***kwantitatieve en kwalitatieve metingen omvatten*** *die toelaten om de evolutie naar de strategische objectieven in kaart te brengen. Jaarlijks zal het CCB een gedetailleerd rapport opstellen waarin de prestaties op basis van deze indicatoren worden geëvalueerd. Dit rapport zal een analyse bevatten van de behaalde resultaten, geïdentificeerde tekortkomingen, en aanbevelingen voor verbeteringen. Het rapport zal worden voorgelegd aan de regering, die op basis van de bevindingen de uitvoering van de strategie kan bijsturen* » (mis en gras par l'Autorité).

[17] P. 29.

26. Le Service d'Autorisation et d'Avis a déjà préconisé de mettre en place un **mécanisme d'évaluation de l'efficacité des traitements de données à caractère personnel** prévus par certaines législations, une fois ces traitements mis en œuvre, par exemple via la mise en place et publication de statistiques et rapports d'évaluation spécifiques, de nature à démontrer la légalité, l'efficacité et la proportionnalité du dispositif concerné et de sa mise en œuvre[18]. Il en a été ainsi par exemple dans le contexte de la rétention des métadonnées de communications électroniques, dans le domaine de l'identification de l'utilisateur final de services de communications électroniques accessibles au public fournis sur la base d'une carte prépayée et dans le cadre de l'utilisation de caméras de surveillance.

27. Il est important que les indicateurs mis en place afin d'évaluer l'exécution de la Stratégie portent **sur l'efficacité des mesures et systèmes de surveillance mis en œuvre dans le cadre de la Stratégie, en particulier s'agissant des traitements de métadonnées de communications électroniques et de données d'identification** des utilisateurs de services de communications électroniques. De cette manière, notamment, la capacité des traitements de données à caractère personnel réalisés à atteindre efficacement leur finalité pourra être étayée.

PAR CES MOTIFS,
L'Autorité est d'avis que, dans les limites rappelées aux considérants nos 3-4 :

1. Elle devrait être renseignée dans la liste de la Stratégie reprenant les acteurs publics du niveau de pouvoir fédéral, dès lors qu'elle est aussi un acteur du niveau de pouvoir fédéral disposant de compétences et d'expertise dans le domaine de la cybersécurité et de la sécurité de l'information en général, lorsqu'est impliqué le traitement de données à caractère personnel (**considérants nos 5-9**) ;

2. La Stratégie devrait apporter, dans la mesure du possible, une visibilité plus concrète quant à ce que constituerait la surveillance, le monitoring continu et l'analyse en temps réel des réseaux de communications électroniques publics (fournis par les opérateurs de télécommunications) ou privés (prestataires de services *cloud*, entreprises, etc.) envisagés par le CCB, afin que puissent être mieux perçus les traitements de données à caractère personnel (collectes, échanges, etc.) nécessaires à cette fin. Il est important dans la mise en œuvre de la Stratégie, de distinguer les activités de prévention et de protection de nature purement technique (et « civile » ; il s'agit de se protéger, de mettre en œuvre des mesures techniques limitant l'impact des menaces concernées ou les entravant), et les activités de recherche et de répression des infractions par les autorités compétentes. L'article 22 du RGPD peut

[18] Voir « La pratique d'avis du Service d'Autorisation et d'Avis, Secteur public et obligations légales », pp . 25 et 44, cité à la note de bas de page n° 5, et l'avis n° 16/2025, considérants nos 18 et 19, cités à la note de bas de page n° 15.

nécessiter, dans la mise en œuvre de la Stratégie, selon les scénarios envisagés, un encadrement normatif spécifique (**considérants nos 10-15**) ;

3. L'identification électronique ne peut être requise que lorsqu'elle est nécessaire et dans la mesure où elle est nécessaire. La personne concernée doit conserver le contrôle sur son identification, sans préjudice des obligations normatives applicables en matière d'identification. Et les services et moyens mis à disposition dans ce contexte ne peuvent mener au monitoring des activités des personnes concernées, comme la Stratégie le met également en évidence (**considérants nos 16-19**) ;

4. La Stratégie pourrait également rappeler le rôle central du chiffrement de bout en bout des communications électroniques, en matière de sécurité (confidentialité), et la nécessité y liée de préserver et garantir son bon fonctionnement (**considérants nos 20-22**) ;

5. Le développement d'un *cloud* souverain peut effectivement contribuer à et garantir l'application effective des standards européens en matière de protection des personnes à l'égard du traitement de données à caractère personnel (**considérants nos 23-24**) ;

6. Il est important que les indicateurs mis en place afin d'évaluer l'exécution de la Stratégie portent sur l'efficacité des mesures et systèmes de surveillance mis en œuvre dans le cadre de la Stratégie, en particulier s'agissant des traitements de métadonnées de communications électroniques et de données d'identification des utilisateurs de services de communications électroniques. De cette manière, notamment, la capacité des traitements de données à caractère personnel réalisés à atteindre efficacement leur finalité pourra être étayée (**considérants nos 25-27**).

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