



Avis n° 31/2025 du 13 mai 2025

Objet : propositions de loi

- **ouvrant la voie civile aux victimes d'activités supposées illicites exercées de manière anonyme sur Internet et modifiant l'article XII.20 du Code de droit économique ;**
- **modifiant le Code de droit économique en vue d'offrir la possibilité d'agir au civil aux victimes de contenus supposés illicites diffusés de manière anonyme sur Internet (CO-A-2025-017)**

Mots-clés : cyberharcèlement - communication d'informations - procédure civile - plateformes

Traduction

Introduction :

L'avis de l'Autorité est sollicité concernant deux propositions de loi qui entendent lutter contre le cyberharcèlement en permettant au président du tribunal de première instance d'ordonner aux fournisseurs de services intermédiaires de communiquer "*toutes les informations dont ils disposent et qui sont utiles à la recherche et à la constatation des infractions commises par des tiers par leur intermédiaire*", en vue notamment d'identifier ces tiers.

L'Autorité précise que le but des propositions de loi est légitime mais elle propose également quelques points d'amélioration (termes vagues, limites des données à traiter, pondération obligatoire des intérêts, ...).

Pour la liste complète des remarques, il est renvoyé au [dispositif](#).

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) ;

Pour les textes normatifs émanant de l'Autorité fédérale, de la Région de Bruxelles-Capitale et de la Commission communautaire commune, les avis sont en principe disponibles en français et en néerlandais sur le site Internet de l'Autorité. La 'version originale' est la version qui a été validée.

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 (Règlement général sur la protection des données, 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 28 février 2025 ;

Émet, le 13 mai 2025, l'avis suivant :

I. OBJET DE LA DEMANDE D'AVIS

1. Le demandeur sollicite l'avis de l'Autorité concernant les propositions de loi :
 - ouvrant la voie civile aux victimes d'activités supposées illicites exercées de manière anonyme sur Internet et modifiant l'article XII.20 du Code de droit économique (ci-après : la proposition de loi n° 1) ;
 - modifiant le Code de droit économique en vue d'offrir la possibilité d'agir au civil aux victimes de contenus supposés illicites diffusés de manière anonyme sur Internet (ci-après : la proposition de loi n° 2).

Contexte et antécédents

2. Le cyberharcèlement est un mal qui frappe un nombre grandissant de personnes dans notre société. Une récente étude française a démontré que 20 % des adolescents et 60 % des 18-25 ans ont été victimes de cyberharcèlement.¹ Le cyberharcèlement est souvent anonyme ou est effectué sous couvert d'un pseudonyme, rendant dès lors difficile l'identification de ses auteurs.

3. Le demandeur souhaite en particulier ajouter un nouveau paragraphe à l'article XII.20 du Code de droit économique qui prévoit la possibilité, pour le président du tribunal de première instance, d'ordonner aux fournisseurs de services intermédiaires de communiquer " toutes les informations dont ils disposent et qui sont utiles à la recherche et à la constatation des infractions commises par des tiers par leur intermédiaire", en vue notamment d'identifier ces tiers.²

¹ <https://www.rtb.be/article/plus-d-un-jeune-sur-deux-a-deja-ete-victime-de-cyber-harcèlement-11100695> (8 novembre 2022).

² Résumé de la proposition de loi n° 1, p. 1.

4. En effet, à l'heure actuelle, les victimes de cyberharcèlement "*ne disposent, en pratique, d'aucune possibilité de connaître l'identité des auteurs : les solutions que les plateformes proposent à cette fin sont insuffisantes, les possibilités d'agir au civil font défaut et l'introduction d'une procédure pénale se révèle inefficace en raison de la compétence dévolue à la cour d'assises en matière de délits de presse.*"³

II. EXAMEN DE LA DEMANDE D'AVIS

Remarque préalable

5. L'Autorité fait remarquer que les deux propositions de loi sont similaires mais comportent d'importantes différences en ce qui concerne le texte de la proposition de loi proprement dit. Par conséquent, l'Autorité abordera d'abord les propositions de loi de manière générale et examinera ensuite distinctement les deux différentes propositions de loi (la proposition de loi n° 1 : proposition de loi *ouvrant la voie civile aux victimes d'activités supposées illicites exercées de manière anonyme sur Internet et modifiant l'article XII.20 du Code de droit économique* et la proposition de loi n° 2 : proposition de loi *modifiant le Code de droit économique en vue d'offrir la possibilité d'agir au civil aux victimes de contenus supposés illicites diffusés de manière anonyme sur Internet*).

6. Ainsi, l'Autorité se demande - **sous réserve d'éventuelles remarques du Conseil d'État à cet égard** - si cette nouvelle possibilité offerte au président du tribunal de première instance peut être insérée purement et simplement dans le *Code de droit économique* (et pas à l'article 584 du *Code judiciaire*). Sans préjudice de la considération susmentionnée, l'Autorité procède dans ce qui suit à une analyse sur le fond des propositions de loi et de leurs implications, telles qu'elles se présentent actuellement.

A. Généralités

7. L'Autorité souligne que toute ingérence dans le droit à la protection des données à caractère personnel n'est admissible que si elle est encadrée par une norme suffisamment claire et précise dont l'application est prévisible pour les personnes concernées. Toute norme encadrant le traitement de données à caractère personnel, en particulier quand ce traitement constitue une ingérence importante dans les droits et libertés des personnes concernées, doit répondre aux exigences de prévisibilité et de précision de sorte qu'à sa lecture, les personnes concernées sachent clairement à quels traitements leurs données sont soumises et dans quelles circonstances un traitement de données est autorisé.

³ Résumé de la proposition de loi n° 2, p. 1.

8. Afin de satisfaire à l'exigence de prévisibilité, la communication des données conservées par les fournisseurs de services intermédiaires aux autorités nationales doit, en droit national, être soumise à des règles claires et précises qui indiquent (à l'aide de critères objectifs) dans quelles circonstances et sous quelles conditions un accès aux données des destinataires du service intermédiaire doit être accordé aux autorités nationales compétentes.⁴ L'accès des autorités nationales *doit être basé sur une habilitation légale spécifique qui en délimite clairement et sans équivoque l'objet ainsi que le seuil pour y accéder*.⁵

9. Conformément à la jurisprudence de la Cour de justice, la réglementation nationale doit prévoir les conditions matérielles et procédurales suivantes⁶ :

- La réglementation nationale doit prévoir les finalités pour lesquelles l'accès peut être accordé aux données conservées par le fournisseur de services intermédiaires.
- La réglementation nationale concernée doit prévoir, à l'aide de critères objectifs, dans quelles circonstances et sous quelles conditions un accès aux données doit être accordé.
- L'accès aux données conservées doit, *en principe, sauf cas d'urgence dûment justifiés, être subordonné à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante*. Cette juridiction ou cette entité doit rendre sa décision à la suite d'une demande motivée.
- Les autorités auxquelles l'accès aux données a été accordé doivent en informer les personnes concernées si cela n'est pas susceptible de compromettre les investigations menées par ces autorités.

10. L'Autorité examinera ci-après dans quelle mesure les propositions de loi remplissent les conditions matérielles et procédurales susmentionnées.

➤ Objectif

11. L'identification difficile d'auteurs anonymes de "contenu supposé illicite" en l'espèce a déjà été reconnue à plusieurs reprises par la Cour européenne des droits de l'homme (ci-après : CEDH).⁷ Bien que l'anonymat soit un élément important sur Internet⁸, la CEDH admet que l'anonymat doit parfois *s'effacer devant d'autres impératifs légitimes (tels que la défense de l'ordre et la prévention des*

⁴ CJUE, 21 décembre 2016, C-203/15 et C-698/15, Tele2Sverige AB/ Post-och telestyrelsen ; § 119.

⁵ Cour Const. 18 novembre 2021, arrêt n° 158/2021, § B.29.2.

⁶ CJUE, 21 décembre 2016, C-203/15 et C-698/15, Tele2Sverige AB/ Post-och telestyrelsen ; § 118-121. Voir également CJUE, 8 avril 2014, C-293/12 et C-594/12, Digital Rights Ireland, § 61 et CJUE, 2 mars 2021, C-746/18, H.K/Prokuratuur, § 49.

⁷ Voir CEDH, 16 juin 2015, n° 64569/09, Delfi AS c. Estonie ; CEDH, 2 décembre 2008, n° 2872/02, K.U. c. Finlande ; CEDH, 7 décembre 2021, n° 39378/15, Standard Verlagsgesellschaft mbH c. Autriche.

⁸ Declaration on freedom of communication on the Internet ; CEDH, 16 juin 2015, n° 64569/09, Delfi AS c. Estonie, § 147 ; CEDH, 7 décembre 2021, n° 39378/15, Standard Verlagsgesellschaft mbH c. Autriche, § 76-78.

infractions pénales ou la protection des droits et libertés d'autrui).⁹ L'article 10 de la Convention européenne des droits de l'homme protège la liberté d'expression, y compris des déclarations anonymes. Toutefois, ce droit n'est pas absolu et peut donc être limité.

12. La jurisprudence de la CEDH indique clairement qu'*une victime potentielle de déclarations diffamatoires doit bénéficier d'un accès effectif à un tribunal afin de pouvoir exposer ses revendications devant lui*¹⁰ (et que dès lors, il doit y avoir une voie de recours permettant d'identifier le véritable auteur et de le poursuivre en justice).

13. Dans ce cadre, l'Autorité fait remarquer que selon la jurisprudence de la Cour de justice, une mesure légale concernant l'accès à des données relatives à l'identité civile des utilisateurs des moyens de communications électroniques dans le seul but d'identifier l'utilisateur concerné constitue une ingérence dans le droit à la vie privée qui "ne peut pas être qualifiée de 'grave'", étant donné que ces données ne permettent pas, à elles seules, de connaître la date, l'heure, la durée et les destinataires des communications effectuées, non plus que les endroits où ces communications ont eu lieu ou la fréquence de celles-ci avec certaines personnes pendant une période donnée.¹¹ Par conséquent, la Cour de justice admet qu'une telle ingérence peut être justifiée par des objectifs de prévention, de recherche, de détection et de poursuite d'infractions pénales en général.¹² Un tel règlement engendre certes une ingérence dans les droits fondamentaux de l'utilisateur d'un service intermédiaire mais il ne s'agit pas d'une ingérence grave au point que cet accès ne soit pas justifié en vue de détecter et de poursuivre des infractions pénales.

14. Le but des propositions de loi, à savoir identifier les auteurs de "contenu supposé illicite" pour que les victimes puissent intenter une action civile afin d'obtenir réparation du dommage qu'elles ont subi, est donc légitime.

➤ Circonstances et conditions

15. L'article 22 de la *Constitution*, lu conjointement avec l'article 8 de la Convention européenne des droits de l'homme et les articles 7, 8 et 52 de la Charte des droits fondamentaux de l'Union européenne, requiert qu'une ingérence dans le droit à la protection de la vie privée et dans le droit à la protection des données à caractère personnel soit formulée en des termes clairs et suffisamment précis, permettant de prévoir les hypothèses dans lesquelles le législateur autorise une telle ingérence dans le droit au respect de la vie privée. Cela implique qu'il faut définir de manière suffisamment précise dans

⁹ CEDH, 2 décembre 2008, n° 2872/02, K.U. c. Finlande, § 49.

¹⁰ CEDH, 7 décembre 2021, n° 39378/15, Standard Verlagsgesellschaft mbH c. Autriche, § 92.

¹¹ Voir notamment CJUE, 6 octobre 2020, C-511/18, C-512/18 et C-520/18, La Quadrature du Net, § 157 et 158.

¹² CJUE, 2 octobre 2018, C-207/16, Ministerio Fiscal, § 57.

quelles circonstances les traitements de données à caractère personnel sont autorisés. Les personnes concernées par le traitement de données doivent dès lors pouvoir avoir une idée suffisamment claire des données traitées et des conditions et finalités du traitement.

16. **L'Autorité constate que le texte des propositions de loi doit être amélioré sur ce point.**

- ***Circonstances***

17. Le texte de la proposition de loi n° 1 précise que le président du tribunal de première instance peut réclamer des informations dans le cadre de la recherche et de la constatation des "fautes commises par des tiers". Le texte de la proposition de loi n° 2 parle par contre d' "actes supposés illicites commis par des tiers".

18. L'Autorité fait également remarquer que les développements des propositions de loi précisent qu'il doit s'agir d'un contenu supposé illicite portant gravement atteinte aux droits d'autrui – tels que des contenus menaçants, harcelants, calomnieux, diffamatoires, injurieux, haineux, racistes, xénophobes, négationnistes ou révisionnistes.¹³

19. Les circonstances dans lesquelles le président du tribunal de première instance peut ordonner de fournir des informations doivent être claires. **L'Autorité constate dès lors que les notions de "fautes commises par des tiers" et d' "actes supposés illicites commis par des tiers" sont vagues et qu'une précision sur ce point est nécessaire.**

- ***Objet***

20. En vertu de la proposition de loi n° 1, les fournisseurs de services doivent "communiquer toutes les informations dont ils disposent et qui sont utiles à la recherche et à la constatation des fautes commises par des tiers par leur intermédiaire, dont notamment l'identification de ces tiers."

21. En vertu de la proposition de loi n° 2, les fournisseurs de services doivent "communiquer toutes les informations dont ils disposent et qui sont utiles à la recherche et à la constatation des actes supposés illicites commis par des tiers par leur intermédiaire, dont notamment l'identification de ces tiers".

¹³ Développements de la proposition de loi n° 1, p. 4 ; Développements de la proposition de loi n° 2, p. 3.

22. Ces projets de réglementation ne donnent aucune indication quant aux données qui peuvent être traitées en tant qu' "informations utiles". **Les projets de réglementation doivent dès lors être précisés de manière à poser au moins des limites aux données qui doivent être traitées. L'Autorité souligne le fait que seules les données à caractère personnel strictement nécessaires peuvent être fournies.**¹⁴

23. Le Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 *relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques)* (Digital Services Act, ci-après : DSA)¹⁵ indique clairement qu'il doit s'agir *d'informations spécifiques portant sur des destinataires particuliers du service intermédiaire concerné* (qui ont déjà été collectées aux fins de fournir le service et dont le fournisseur de services intermédiaires a le contrôle) *aux fins de déterminer si les destinataires du service respectent les règles de l'Union ou les règles nationales applicables. Il convient que ces injonctions demandent des informations destinées à permettre l'identification des destinataires du service concerné.*¹⁶

24. L'Autorité estime dès lors qu'il faut au moins préciser qu'il s'agit

- d'informations **spécifiques** portant sur des destinataires particuliers suspectés d'avoir diffusé du "contenu supposé illicite" ; et
- **qui ont déjà été collectées** par le fournisseur de services aux fins de fournir le service et **dont il a le contrôle** ; et
- **aux fins de** déterminer si les destinataires du service respectent les règles de l'Union ou les règles nationales applicables ; et
- **destinées à permettre l'identification des destinataires.**

➤ Contrôle préalable par une juridiction

25. L'Autorité fait remarquer que cette condition est **remplie**, étant donné que le président du tribunal de première instance peut charger les fournisseurs de services intermédiaires de communiquer les informations spécifiques visées.

¹⁴ Voir également la Cour Const., 18 novembre 2021, arrêt n° 15/2021, § B.29.2 : "Cet objet doit être limité à ce qui est nécessaire au regard de l'objectif légitime poursuivi, étant donné qu'un accès trop large [...] permettrait à l'autorité publique de se faire une idée détaillée de la vie privée de l'intéressé."

¹⁵ Article 10, paragraphe 1 du DSA. Voir ci-dessous les points 43-46.

¹⁶ Considérant 37 et article 10 du DSA.

26. En vertu de la jurisprudence constante de la Cour de justice, il doit s'agir d'une demande motivée¹⁷ d'une juridiction dont la décision vise à limiter l'accès aux données et leur utilisation à ce qui est strictement nécessaire aux fins d'atteindre l'objectif poursuivi.¹⁸

27. La CEDH précise qu'il peut s'agir d'un examen *prima facie* mais qu'en tout état de cause, un raisonnement et une mise en balance sont requis.¹⁹

28. Le DSA attend aussi "*un exposé des motifs expliquant dans quel but les informations sont requises et pourquoi la demande de fourniture d'informations est nécessaire et proportionnée pour déterminer si les destinataires des services intermédiaires respectent le droit de l'Union ou le droit national conforme au droit de l'Union applicable, à moins qu'un tel exposé ne puisse être fourni pour des raisons liées à la prévention et à la détection des infractions pénales et aux enquêtes et poursuites en la matière*".²⁰

29. L'Autorité fait toutefois remarquer dans ce cadre qu'en néerlandais, la proposition de loi n° 1 précise que "de voorzitter "in de mate van het mogelijke" een evenwicht" dient na te streven" alors que la proposition de loi n° 2 précise que "de voorzitter "na de belangen en grondrechten zo goed mogelijk" tegen elkaar te hebben afgewogen" de dienstverleners kan gelasten de voornoemde specifieke informatie te verschaffen". [NdT : cette nuance ne figure pas dans le texte en français qui utilise dans les deux propositions l'expression "dans la mesure du possible"]

30. **L'Autorité estime qu'il faut clairement préciser dans les propositions de loi que le président du tribunal de première instance doit mettre en balance les intérêts contradictoires** en jeu (le droit du requérant de protéger sa réputation, le droit de l'auteur à la liberté d'expression et à la protection des données à caractère personnel et le droit de la plateforme à la liberté de la presse et à la liberté d'expression en général), avant de décider si les données doivent être communiquées.

31. L'Autorité souligne que le président du tribunal de première instance devra vérifier si la communication des données poursuit un objectif légitime. À savoir que vu les faits, il existe un ensemble d'indices concordants et graves selon lesquels le destinataire du service intermédiaire est suspecté d'avoir diffusé du "contenu supposé illicite" et qu'il y a lieu de constater que la divulgation des données est nécessaire et qu'il n'y a pas de mesure moins intrusive possible.²¹

¹⁷ CJUE, 21 décembre 2016, C-203/15 et C-698/15, Tele2Sverige AB/ Post-och telestyrelsen ; § 120 ; CJUE, 8 avril 2014, C-293/12 et C-594/12, Digital Rights Ireland, § 62 ; CJUE, 2 mars 2021, C-746/18, H.K./Prokuratuur, § 49.

¹⁸ CJUE, 8 avril 2014, C-293/12 et C-594/12, Digital Rights Ireland, § 62.

¹⁹ CEDH, 7 décembre 2021, n° 39378/15, Standard Verlagsgesellschaft mbH c. Autriche, § 92.

²⁰ Article 10, paragraphe 2, a) iv) du DSA.

²¹ Cour Const., 18 novembre 2021, arrêt n° 158/2021, § B.29.2.

➤ Informer les personnes concernées

32. La Cour de justice précise que les personnes concernées doivent être informées de l'accès à leurs données, si cela ne peut pas compromettre l'investigation menée. Ces informations sont en fait nécessaires pour permettre aux personnes concernées d'exercer le droit de recours, prévu explicitement à l'article 10, § 5 du DSA, lu conjointement avec le RGPD, en cas de violation de leurs droits.²²

33. La Cour constitutionnelle estime toutefois, en s'appuyant sur la jurisprudence de la CEDH, qu'il n'est pas nécessaire que la personne concernée soit informée de l'accès à ses données d'identification.²³

34. L'Autorité laisse dès lors **au président du tribunal de première instance** le soin de décider, au cas par cas, s'il est opportun d'informer la personne concernée de l'accès à ses informations spécifiques. L'obligation d'informer la personne concernée peut également être différée dans le contexte de procédures civiles.²⁴

B. Proposition de loi n° 1 : "procédé dans la mesure du possible à la mise en balance"

35. Comme exposé aux points 28 à 30 inclus, l'Autorité estime essentiel que chaque demande d'informations soit au préalable évaluée par une juridiction, en tenant compte de la proportionnalité et de la subsidiarité.

36. La proposition de loi n° 1 qui précise que le président du tribunal de première instance procède, dans la mesure du possible, à la mise en balance doit dès lors être adaptée.

C. Proposition de loi n° 2 : "par leur intermédiaire"

37. Dans le projet d'article XII.20, § 3, premier alinéa du *Code de droit économique* repris dans la proposition de loi n° 2, les termes "par leur intermédiaire" sèment la confusion dans la mesure où ils peuvent donner l'impression que les fournisseurs de services visés seraient obligés de partager avec les

Voir également à cet égard la jurisprudence néerlandaise suivante : Hoge Raad, 25 novembre 2005, ECLI:NL:HR:2005:AU4019, § 4.10 ; Rechtbank Zeeland-West-Brabant, ECLI:NL:RBZWB:2020:6923, § 3-5 ; Gerechtshof Arnhem-Leeuwarden, 2 mai 2023, ECLI:NL:GHARL:2023:3598, § 4.7.

²² CJCE, 21 décembre 2016, C-203/15 et C-15/15, Tele2Sverige AB/ Post-och telestyrelsen ; § 121.

²³ Cour Const., 18 novembre 2021, arrêt n° 158/2021, § B.14.3.

²⁴ Voir le considérant 34 du DSA.

autorités judiciaires et administratives des informations sur les violations qu'ils pourraient avoir commises en tant qu'auteur, coauteur ou complice.

38. La section de législation du Conseil d'État a déjà rappelé à plusieurs reprises que "*Le droit de ne pas s'auto-incriminer, garanti par l'article 6 de la Convention européenne des droits de l'homme, fait toutefois obstacle à ce qu'une personne, "pénalement accusée" au sens de cette disposition, puisse être sanctionnée pour avoir refusé de prêter son concours à l'établissement de sa propre culpabilité*".²⁵

39. Par conséquent, les termes "par leur intermédiaire" doivent être remplacés par une formulation plus adéquate, par exemple par les termes "par un destinataire spécifique de leur service intermédiaire". En outre, cette formulation correspond mieux aux formulations utilisées à l'article 10 du DSA.²⁶

D. Divers

➤ Délai de conservation

40. L'Autorité attire l'attention du demandeur sur la jurisprudence de la Cour constitutionnelle qui affirme que la loi doit *prévoir des mesures contre les abus, parmi lesquelles la garantie que les données ne seront pas conservées plus longtemps que ce qui est nécessaire aux fins de l'investigation menée*.²⁷

41. En vertu de l'article 5.1.e) du RGPD, les données à caractère personnel ne peuvent pas être conservées sous une forme permettant l'identification des personnes concernées pendant une durée excédant celle nécessaire à la réalisation des finalités pour lesquelles elles sont traitées. **Dès lors, il faut prévoir un délai de conservation (maximal) pour les données ou les critères pour déterminer ce délai.**

➤ Identification

²⁵ Conseil d'État, avis 60.619/2 du 25 janvier 2017 sur un avant-projet qui a abouti à la loi du 2 octobre 2017 *réglementant la sécurité privée et particulière*, Doc. Parl. Chambre, 2016-17, n° 2388/001, 159-196. Voir également les avis 63.296/4 du 2 mai 2018 sur un avant-projet qui a abouti à la loi du 7 avril 2019 *établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique*, Doc. Parl. Chambre, 2018-19, n° 3340/001, 75-87. 64.879/4 du 4 février 2019 sur un avant-projet qui a abouti au décret du 2 mai 2019 *modifiant le Code wallon de l'action sociale et de la santé en ce qui concerne la prévention et la promotion de la santé*, Doc. Parl. Parlement wallon 2018-19, n° 1332/1, 25-35 et 69.813/2/V du 30 août 2021 sur un avant-projet de loi qui a abouti à la loi du 20 juillet 2022 *relative à la certification de cybersécurité des technologies de l'information et des communications et portant désignation d'une autorité nationale de certification de cybersécurité*, Doc. Parl. Chambre 2021-22, n° 2963/001, 75-87.

²⁶ Voir également le Conseil d'État du 20 décembre 2023, avis 74.816/VR-4 sur un avant-projet de loi *mettant en œuvre le règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE, portant modifications du livre XII et du livre XV du Code de droit économique et portant modifications de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges*, <http://www.raadvst-consetat.be/dbx/avis/74816.pdf#search=74.816%2FVR-4>, p. 23-24.

²⁷ Cour Const., 18 novembre 2021, arrêt n° 158/2021, § B.29.2.

42. L'Autorité estime également essentiel d'attirer l'attention du demandeur sur le fait que l'identification de l'abonné d'un service intermédiaire ne permet pas nécessairement d'identifier l'utilisateur effectif de ce service.

43. Dans les faits, il n'est en effet pas rare que l'utilisateur d'un service intermédiaire soit différent de la personne ayant souscrit à ce service. Il existe donc un risque réel que l'utilisateur final ne puisse pas être identifié avec certitude et que la qualité des données d'identification de l'utilisateur final puisse être remise en cause. Les incertitudes quant à la qualité des données d'identification seront d'autant plus importantes que l'identification de l'abonné aura lieu par le biais d'une méthode d'identification indirecte. En effet, l'identification de la personne "derrière" une adresse IP, un numéro de téléphone ou la référence d'une transaction bancaire ne permet pas d'identifier avec certitude la personne qui a effectivement utilisé le service intermédiaire. Dans ces circonstances où la qualité de l'identification de l'utilisateur effectif du service intermédiaire apparaît incertaine, l'Autorité insiste pour que le demandeur réfléchisse sur, et justifie, la nécessité de l'ingérence causée dans le droit à la protection des données à caractère personnel des destinataires de services intermédiaires.²⁸

E. DSA

44. L'Autorité attire l'attention du demandeur sur le fait que le DSA s'applique.²⁹

45. Conformément à l'article 8 du DSA, "*les fournisseurs de services intermédiaires ne sont soumis à aucune obligation générale de surveiller les informations qu'ils transmettent ou stockent ou de rechercher activement des faits ou des circonstances révélant des activités illégales*".

46. Toutefois, des obligations de surveillance spécifiques sont prévues, comme les 'injonctions de fournir des informations' (article 10 du DSA). L'Autorité estime nécessaire de préciser qu'une demande d'informations **doit** au moins **remplir les conditions énumérées à l'article 10, paragraphe 2 du DSA**, à savoir que :

"a) ladite injonction comprend les éléments suivants :

- i) une référence à la base juridique au titre du droit de l'Union ou du droit national pour l'injonction ;*
- ii) des informations permettant d'identifier l'autorité d'émission ;*

²⁸ Voir également l'avis n° 66/2022 de l'Autorité du 1^{er} avril 2022 *concernant 18 amendements modifiant le projet de loi relatif 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* : <https://www.autoriteprotectiondonnees.be/publications/avis-n-66-2022.pdf>.

²⁹ Le demandeur le mentionne également lui-même dans les développements des propositions de loi, voir p. 11 de la proposition de loi n° 1 et p. 10 de la proposition de loi n° 2.

- iii) des informations claires permettant au fournisseur de services intermédiaires d'identifier le ou les destinataires spécifiques au sujet desquels des informations sont demandées, telles qu'un ou plusieurs noms de compte ou identifiants uniques ;*
- iv) un exposé des motifs expliquant dans quel but les informations sont requises et pourquoi la demande de fourniture d'informations est nécessaire et proportionnée pour déterminer si les destinataires des services intermédiaires respectent le droit de l'Union ou le droit national conforme au droit de l'Union applicable, à moins qu'un tel exposé ne puisse être fourni pour des raisons liées à la prévention et à la détection des infractions pénales et aux enquêtes et poursuites en la matière ;*
- v) des informations relatives aux mécanismes de recours dont disposent le fournisseur et les destinataires du service concerné ;*
- vi) le cas échéant, des informations relatives à l'autorité qui doit recevoir les informations relatives aux suites données aux injonctions ;*
- b) ladite injonction exige uniquement du fournisseur qu'il communique des informations déjà collectées aux fins de fournir le service et dont il a le contrôle ;*
- c) ladite injonction est transmise dans l'une des langues déclarées par le fournisseur de services intermédiaires en vertu de l'article 11, paragraphe 3, ou dans une autre langue officielle des États membres convenue entre l'autorité qui a émis l'injonction et le fournisseur, et elle est envoyée au point de contact électronique désigné par ce fournisseur, conformément à l'article 11 ; lorsque l'injonction n'est pas rédigée dans la langue déclarée par le fournisseur de services intermédiaires ou dans une autre langue convenue de manière bilatérale, l'injonction peut être transmise dans la langue de l'autorité qui l'a émise, à condition qu'elle soit accompagnée d'une traduction, dans cette langue déclarée ou convenue de manière bilatérale, au minimum des éléments mentionnés aux points a) et b) du présent paragraphe."*

47. L'Autorité constate que conformément à l'article 10, paragraphes 3 et 4 du DSA, le président du tribunal de première instance doit transmettre l'injonction ainsi que toute information reçue du fournisseur de services intermédiaires concernant la suite donnée à cette injonction au coordinateur pour les services numériques de l'État membre de l'autorité d'émission (à savoir l'IBPT). L'IBPT doit ensuite transmettre une copie à tous les coordinateurs pour les services numériques³⁰. L'Autorité souligne le fait que cette obligation peut ne pas s'appliquer mais que cela doit alors être repris en droit national.³¹

³⁰ Voir à cet égard l'avis n° 33/2024 de l'Autorité du 12 avril 2024 *relatif à un projet d'accord de coopération entre l'État fédéral, la Communauté flamande, la Communauté française, la Communauté germanophone, relatif à l'exécution coordonnée du règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques)*, <https://www.autoriteprotectiondonnees.be/publications/avis-n-33-2024.pdf>.

³¹ Voir le considérant 34 du DSA.

**PAR CES MOTIFS,
l'Autorité,**

estime qu'au minimum les modifications suivantes sont nécessaires dans la proposition de loi n° 1 (proposition de loi ouvrant la voie civile aux victimes d'activités supposées illicites exercées de manière anonyme sur Internet et modifiant l'article XII.20 du Code de droit économique) :

- préciser la notion de "fautes commises par des tiers" (notamment les circonstances), voir les points 17-19 ;
- poser des limites aux données qui doivent être traitées (uniquement les données à caractère personnel strictement nécessaires, notamment l'objet), voir les points 20-24 ;
- préciser que toute demande d'informations doit être évaluée au préalable par une juridiction, en tenant compte de la proportionnalité et de la subsidiarité, voir les points 28-30 et 35-36 ;
- prévoir un délai de conservation (maximal) pour les données, ou les critères pour déterminer ce délai, voir les points 40-41 ;
- préciser qu'une demande d'informations doit au moins remplir les conditions énumérées à l'article 10, paragraphe 2 du DSA, voir les points 44-47 ;

estime qu'au minimum les modifications suivantes sont nécessaires dans la proposition de loi n° 2 (proposition de loi modifiant le Code de droit économique en vue d'offrir la possibilité d'agir au civil aux victimes de contenus supposés illicites diffusés de manière anonyme sur Internet) :

- préciser la notion d' "actes supposés illicites commis par des tiers" (notamment les circonstances), voir les points 17-19 ;
- poser des limites aux données qui doivent être traitées (uniquement les données à caractère personnel strictement nécessaires, notamment l'objet), voir les points 20-24 ;
- remplacer les termes "par leur intermédiaire" par "par un destinataire spécifique de leur service intermédiaire", voir les points 37-39 ;
- prévoir un délai de conservation (maximal) pour les données, ou les critères pour déterminer ce délai, voir les points 40-41 ;
- préciser qu'une demande d'informations doit au moins remplir les conditions énumérées à l'article 10, paragraphe 2 du DSA, voir les points 44-47.

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