Autorité de protection des données
Gegevensbeschermingsautoriteit

Avis n° 16/2025 du 27 mars 2025

Objet: Avis d'initiative *relatif à la Convention des Nations-Unies contre la cybercriminalité* (CO-A-2025-019)

Version originale

Introduction

Dans le cadre du processus d'adoption de la convention des Nations-Unies contre la cybercriminalité, l'EDPB a été invité à rappeler sa position concernant l'importance du chiffrement des données de communication. L'Autorité en profite pour émettre un avis d'initiative sur cette question et préconise, sinon de s'abstenir de donner l'assentiment de la Chambre au texte de cette Convention, à tout le moins, d'interroger la Cour de justice au sujet de la compatibilité de cette dernière avec la Charte des droits fondamentaux.

Le Service d'Autorisation et d'Avis de l'Autorité de protection des données (ci-après « l'Autorité »),
Présent.e.s : Mesdames Cédrine Morlière, Nathalie Ragheno et Griet Verhenneman et Messieurs Yves-Alexandre de Montjoye, Bart Preneel et Gert Vermeulen;

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

Vu l'article 43 du règlement d'ordre intérieur selon lequel les décisions du Service d'Autorisation et d'Avis sont adoptées à la majorité des voix;

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 »);

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 collégialement.

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 »);

Émet, le 27 mars 2025, l'avis d'initiative suivant :

I. CONTEXTE ET PORTEE DE L'AVIS

1. La Convention des Nations-Unies sur la cybercriminalité (ci-après « la Convention » ou « le Traité ») a été adoptée par l'Assemblée générale des Nations-Unies, le 24 décembre 2024 par la résolution 79/243[1].

2. La Convention sera ouverte à la signature des Etats lors d'une cérémonie qui se tiendra mi-2025[2] dans la ville d'Hanoi, au Vietnam. Elle pourra alors être ratifiée par les Etats Parties et elle entrera en vigueur dès que 40 Etats seront formellement Parties à la Convention[3].

3. Cette Convention comporte un préambule et neuf chapitres : Dispositions générales, Incrimination, Compétence, Mesures procédurales, détection et répression, Coopération internationale, Mesures préventives, Assistance technique et échange d'informations, Mécanismes d'application et Dispositions finales.

4. Plusieurs de ses dispositions ont fait l'objet de critiques sur de très nombreux points[4].

5. Plusieurs dispositions concernant la protection des données sont également problématiques[5] (telles que par exemple les dispositions relatives à la rétention des données de communication[6] et à la collaboration entre autorités au niveau international, dont le libellé risque d'ouvrir la voie à un

---

[1] Sans qu'il soit procédé à un vote (voy. https://unis.unvienna.org/unis/pressrels/2024/uniscp1184.html) et sur base du rapport de la Troisième Commission (A/79/460 , §15).

[2] La date exacte n'a pas encore été communiquée (voy. https://www.unodc.org/unodc/en/cybercrime/convention/home.html).

[3] Voy. https://www.unodc.org/unodc/en/cybercrime/convention/home.html

[4] Voy. notamment

https://www.hrw.org/sites/default/files/media_2023/08/ARTICLE%2019%20and%20Human%20Rights%20Watch%E2%80%99s%20Comments%20on%20the%20Draft%20Text%20of%20the%20UN%20Cybercrime%20Convention_1.pdf ; https://www.eff.org/deeplinks/2024/01/joint-statement-proposed-cybercrime-treaty-ahead-concluding-session; https://epicenter.works/fileadmin/user_upload/Open_Letter_of_the_Multistakeholder_Community_to_the_Chair_of_AHC.pdf; https://www.gp-digital.org/news/civil-society-sends-joint-letter-urging-eu-and-member-states-to-withdraw-support-from-rights-harming-un-cybercrime-convention/ et G. Vermeulen, "The growing human rights cost of tackling cybercrime at UN, CoE and EU levels : from unlimiting state control and surveillance to limiting the freedom of information, privacy and procedural rights in criminal matters," in Conferência Internacional Sobre o Crime Organizado, Rio de Janeiro, 2023 (https://biblio.ugent.be/publication/01HJJZDJ41NSTF8SX765MB7W61)

[5] Voy. l'avis 9/2022 donné par l'EDPS le 18 mai 2022.

[6] Sur cette question, l'Autorité renvoie à ses avis 108/2021 (https://www.autoriteprotectiondonnees.be/publications/avis-n-108-2021.pdf) et 66/2022 (https://www.autoriteprotectiondonnees.be/publications/avis-n-66-2022.pdf) pour tout ce qui n'est pas expressément mentionné dans le présent avis.

contournement des garanties européennes en matière de transferts de données[7]). En outre, comme l'ont relevé plusieurs ONG, le libellé de l'art. 28.4 de la Convention – similaire[8] à celui de l'art. 19.4. de la Convention de Budapest (adoptée en 2001 par les Etats membres du Conseil de l'Europe) - est susceptible de conduire à un affaiblissement de la technique du chiffrement de bout en bout des communications. L'Autorité partage cette préoccupation.

II. EXAMEN DE L'ART. 28.4 DE LA CONVENTION

6. L'art. 28.4 de la Convention dispose que « *chaque État partie adopte les mesures législatives et autres nécessaires* ***pour habiliter ses autorités compétentes à ordonner à toute personne connaissant*** *le fonctionnement du système d'information et de communication en question, du réseau d'information et de télécommunications, ou de leurs éléments constitutifs, ou* ***des mesures appliquées pour protéger les données électroniques qu'ils contiennent, de fournir, dans la mesure du raisonnable, toutes les informations nécessaires*** (…) ».

7. Comme l'ont relevé plusieurs ONG, ce libellé est susceptible de conduire à un affaiblissement de la technique du chiffrement de bout en bout des communications. La 22ème recommandation du groupe d'experts de haut niveau sur l'accès aux données pour une effectivité du travail policier[9], mentionne d'ailleurs la demande des services de police visant à obtenir un accès licite préétabli aux données *en clair*, « *conforme aux instruments internationaux* »[10].

8. La position de l'EDPB concernant l'importance de la préservation du chiffrement est rappelée au point 3 de sa déclaration 5/2024[11]. L'Autorité se rallie sans réserve à cette déclaration, mais souhaite apporter quelques précisions dans la perspective d'un éventuel assentiment parlementaire à ce Traité.

1.Risque de détournement de finalité

9. Tout d'abord, l'Autorité souligne qu'avant d'autoriser une mesure de surveillance, le législateur doit avoir à l'esprit que, même en étant conscient des risques, les détournements de finalités sont inhérents

---

[7] Voy. l'art. 36.1.c de la Convention qui encourage les Etats Parties à « *conclure des accords bilatéraux ou multilatéraux pour faciliter le transfert de données personnelles* », comme le relevait G. Vermeulen, *op. cit.*, slides 6 et 7 ; voy. également la Civil society's joint letter urging EU and member states to withdraw support from rights-harming UN Cybercrime Convention.

[8] La Convention de Budapest vise les « systèmes informatiques « et les « *mesures appliquées pour protéger les données informatiques* » alors que la convention ONU à l'examen vise les « *systèmes d'information et de communication* ».

[9] Voy. le *Step 3* de la version révisée de ce rapport présentée aux délégations par le Conseil, le 13 mars 2025 (p. 75) https://data.consilium.europa.eu/doc/document/ST-15941-2024-REV-2/en/pdf

[10] Pp. 14 et 20

[11] Statement on the recommendations of the High-Level Group on Access to Data for Effective Law Enforcement

à nos sociétés technologiques. De tels détournements se produisent en effet dès que la tentation existe, c'est-à-dire dès qu'une évolution technologique rend possible l'enregistrement et la conservation de données[12]. En d'autres termes, bien que l'Autorité reconnaisse que certaines mesures peuvent se justifier, il convient d'être conscient du fait que **seule une interdiction pure et simple de la mesure de surveillance est véritablement efficace pour prévenir les extensions de finalités confinant au détournement**. L'exemple habituellement cité est celui de la croissance exponentielle des écoutes téléphoniques, aux Etats-Unis, suite à l'adoption du Wiretap Act de 1968, qui limitait pourtant les écoutes au cas les plus graves et dont les garanties légales qui y étaient prévues ont fait l'objet d'une érosion constante depuis son adoption[13].

10. Le chiffrement est quant à lui dans le viseur des autorités policières depuis le milieu des années 1990[14]. En 1995, les téléphones et autres moyens de communication allaient être utilisés par les cartels de la drogue, les terroristes et les kidnappeurs[15]. En 2014, le directeur du FBI américain faisait état d'un risque de « *travailler à l'aveugle* » face aux « *prédateurs qui exploitent les plus vulnérables parmi nous* [,] *... des criminels violents qui ciblent nos communautés*[,] *... une cellule terroriste utilisant les réseaux sociaux pour recruter, planifier et exécuter une attaque* »[16] et dans les années 2020, c'est la prévention de la diffusion en ligne de matériel d'abus sexuel sur enfants (CSAM) que la Commission européenne, invoque pour s'en prendre au chiffrement de bout en bout[17]. A noter que cette dernière initiative a entrainé des réactions extrêmement vives de la part du monde scientifique ainsi que de l'EDPS et a conduit le Médiateur européen à conclure à une mauvaise administration dans le chef de la Commission européenne[18].

2. Typologie de l'affaiblissement du chiffrement

11. Comme l'indique l'EDPB, l'affaiblissement de la protection fournie par le chiffrement peut résulter de différentes mesures techniques, qui ne se limitent pas à l'introduction d'une "backdoor" au sein du

---

[12] Voy. Le mémoire de M. Jacobs, Function Creep in Surveillance Situations - Identifying control paradoxes through agency and power relations using ANT, 2016 (https://avpn.asia/wp-content/uploads/2020/12/06.pdf)

[13] Sur cette question, voy. Jennifer S. Granick et al., Mission Creep and Wiretap Act 'Super Warrants': A Cautionary Tale, 52 Loy. L.A. L. Rev. 431 (2019) (https://digitalcommons.lmu.edu/cgi/viewcontent.cgi?article=3061&context=llr); A noter qu'une étude relative à la vidéosurveillance depuis 2007 (date de l'entrée en vigueur de la loi caméras) en Belgique arriverait vraisemblablement à une conclusion identique.

[14] Pour une analyse détaillé de qui est qualifié de « crypto war », voy. Bart Preneel (2024), The Encryption Debate: An Enduring Struggle. *In* Proceedings of the Fourteenth ACM Conference on Data and Application Security and Privacy (CODASPY '24). Association for Computing Machinery, New York, NY, USA, 1–3. https://doi.org/10.1145/3626232.3655998

[15] Voy. https://archive.epic.org/crypto/ban/freeh.html; Voy. également la Résolution du Conseil du 17 janvier 1995 relative à l'interception légale des télécommunications (JOUE n° C 329 du 04/11/1996 p. 0001 – 0006)

[16] https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course

[17] Voy. https://netzpolitik.org/2022/dude-wheres-my-privacy-how-a-hollywood-star-lobbies-the-eu-for-more-surveillance/; L'Autorité est d'ailleurs particulièrement préoccupée lorsqu'elle lit dans l'exposé d'orientation politique de la Ministre en charge du Numérique, que la Belgique poursuivra son engagement au niveau européen l'adoption du Règlement CSAM (https://www.lachambre.be/flwb/pdf/56/0767/56K0767030.pdf, p.13)

[18] Voy. la décision du 12 juillet 2024 dans l'affaire 1945/2023/MIG (https://www.ombudsman.europa.eu/fr/decision/fr/189484

processus de chiffrement lui-même, mais également de l'introduction de mesures rendant les garanties offertes par le chiffrement caduques ou les affaiblissant considérablement (p.ex. un « *processus côté client* » permettant un accès à distance aux données avant qu'elles ne soient chiffrées ou après qu'elles aient été déchiffrées au niveau du destinataire).

12. En outre, afin de répondre aux ordonnances d'interception ou d'accès légitimes, les fournisseurs pourraient être **contraints techniquement d'appliquer des mesures affaiblissant le chiffrement de manière indiscriminée pour tous les utilisateurs** afin de se conformer à cette ordonnance, même dans les cas où l'ordonnance initiale d'interception ou d'accès était limitée à un individu spécifique ou à un groupe d'individus spécifique (voy. l'affaire de la CEDH PODCHASOV c. RUSSIE).

13. Plus généralement, l'Autorité rappelle[19] que :

a) chaque nouvelle voie d'accès à l'information (même si c'est pour les forces de l'ordre) augmente la complexité du système, ce qui implique un accroissement du périmètre exposé aux attaques et, par voie de conséquence, le risque de failles ;
b) la probabilité qu'une telle voie d'accès soit exploitée par des cybercriminels (étatiques ou appartenant à une organisation criminelle) est très élevée ;
c) le grand nombre d'autorités (répressives) devant pouvoir bénéficier d'un accès engendre encore des problèmes techniques et juridiques supplémentaires.

3. Effets collatéraux indésirables

14. L'Autorité ajoute que, paradoxalement, l'affaiblissement du chiffrement de bout en bout est de nature à impacter la **sécurité nationale**. À titre d'exemple, c'est précisément parce que le chiffrement de bout en bout n'était pas utilisé que le groupe chinois APT (Advanced Persistent Threat) *Salt Typhoon* a pu infiltrer 9 fournisseurs de services de télécommunications américains[20] et est parvenu à espionner des communications potentiellement très sensibles du gouvernement américain.

15. De plus, dans sa déclaration 5/2024, l'EDPB indique qu'empêcher l'utilisation du chiffrement ou affaiblir l'efficacité de la protection qu'il procure aurait un **impact grave sur le respect de la vie privée et de la confidentialité des utilisateurs, sur leur liberté d'expression, ainsi que sur**

---

[19] En ce sens, voy. Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael A. Specter, Daniel J. Weitzner, Keys under doormats: mandating insecurity by requiring government access to all data and communications , *Journal of Cybersecurity*, Volume 1, Issue 1, September 2015, Pages 69–79, https://doi.org/10.1093/cybsec/tyv009

[20] https://en.wikipedia.org/wiki/2024_United_States_telecommunications_hack

l'innovation et la croissance de l'économie numérique, qui repose sur le haut niveau de confiance et de sécurité que ces technologies fournissent.

16. L'Autorité observe à cet égard que le Traité ne contient aucune **exception pour les journalistes, les défenseurs des droits humains et les chercheurs** en cybersécurité[21]. Bien entendu, la loi nationale peut le prévoir, mais certains Etats y seront plus attentifs que d'autres et **il serait regrettable que l'Etat belge cautionne l'entrée en vigueur d'un traité dont il est craint qu'il soit instrumentalisé** pour restreindre la liberté d'expression des journalistes et des défenseurs des droits humains[22].

17. En ce qui concerne les chercheurs (tant en Belgique qu'à l'étranger), il est également essentiel que ces derniers puissent étudier les systèmes électroniques et identifier les faiblesses de manière responsable et sans être criminalisés. De plus, il est crucial que les chercheurs ne soient pas contraints de communiquer les vulnérabilités prématurément et que les faiblesses soient signalées dans le cadre d'une politique de divulgation coordonnée des vulnérabilités[23]. L'Autorité estime que les intervenants devraient être en premier lieu les chercheurs eux-mêmes ainsi que les organisations responsables des systèmes – les gouvernements ne devraient être informés que lorsque les risques ont été bien étudiés et qu'une première mesure d'endiguement a pu intervenir[24].

4. Nécessité et proportionnalité de la mesure

18. L'Autorité estime que la Belgique ne peut s'engager à imposer aux opérateurs un affaiblissement du chiffrement, que « *sous réserve et dans la mesure où le caractère nécessaire et proportionné de la mesure serait démontré* »[25]. En effet, comme le rappelle un rapport au Haut-Commissaire des Nations-Unies aux Droits humains, s'inquiétant des menaces que la surveillance fait peser sur les démocraties : « *les Etats négligent trop souvent de démontrer l'efficacité des systèmes de surveillance qu'ils mettent en œuvre* »[26]. Il convient donc que le législateur national soit mis en possession d'éléments objectifs[27], en ce compris, le cas échéant, des statistiques, à cet effet. Le cas échéant, ceci devrait conduire à **distinguer le contexte dans lequel un accès aux données est envisagé**

---

[21] Sur cette question, voy. https://cyberscoop.com/un-cybercrime-treaty-threatens-security-research-ilona-cohen-op-ed/

[22] Voy. notamment le courrier mentionné *supra*.

[23] Voy. https://ccb.belgium.be/sites/default/files/Brochure_CVDP_FR_1.pdf

[24] Voy. la norme ISO/IEC 29147:2018 **;** A noter que Cyber Resilience Act est également problématique de ce point de vue. En effet une notification immédiate des gouvernements comporte un risque d'abus.

[25] Conformément à l'art. 52(1) de la Charte des droits fondamentaux de l'UE

[26] Rapport du 4 août 2022, The right to privacy in the digital age, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G22/442/29/PDF/G2244229.pdf?OpenElement, point 54

[27] Voy. également en ce sens B. Preneel (2024), *op. cit.*, point 5 : "(…) *there is a lack of verifiable data from the law enforcement side to substantiate their claimed needs for the interception of encrypted communications and the real-time access to data on client devices*".

(données contenues sur l'appareil de l'utilisateur ou sur les serveurs du provider, avant ou après une confiscation, besoin ou non d'un export de données ou accès en temps réel aux données de communication) et donc de **déterminer l'étendue admissible de l'ingérence**. Ceci devrait également permettre de déterminer les **limites** territoriales et temporelles d'une telle mesure.

19. L'Autorité regrette par ailleurs que le Traité n'impose pas que des statistiques soient réalisées par les Etats Parties aux fins de la **publication de rapports d'évaluation nationaux**. L'Autorité estime qu'il convient d'y remédier afin d'éviter qu'il puisse être reproché aux Etats Parties de ne pas démontrer l'efficacité des mesures qu'ils mettent en œuvre.

5. S'abstenir de rejeter la responsabilité sur les fournisseurs

20. Enfin, dans sa déclaration précitée, l'EDPB met également en garde contre « *la **tentation d'imposer des exigences contradictoires aux fournisseurs** (à la fois permettre l'interception de communications spécifiques et ne pas affaiblir le chiffrement de manière indiscriminée) et les "obliger* […] *à trouver le moyen" de s'y conformer.* (…) *L'EDPB conseille ainsi de **déterminer et d'évaluer les types de mesures** à mettre en place par les fournisseurs, qui devraient servir de base pour juger si elles affaiblissent effectivement ou non le chiffrement ainsi que la sécurité des données personnelles et des communications en général. Plus généralement, il est crucial d'appuyer toute recommandation impliquant l'utilisation d'une solution technique avec une évaluation de la faisabilité pratique et de la conformité de cette solution avec les obligations de protection de la vie privée dès la conception et par défaut.* (…) ».

6. Possibilités offertes à la Chambre des représentants

21. La décision du Conseil de l'Union européenne autorisant la Commission européenne (en 2022)[28] à ouvrir les négociations relatives à cette convention pour l'Union européenne, précisait que l'Union avait déjà adopté des règles qui couvrent « *certains[29], mais pas tous, les éléments susceptibles d'être envisagés pour inclusion dans la convention* »[30]. Le Conseil justifie l'autorisation par la nécessité de « *protéger l'intégrité du droit de l'Union et de garantir que les règles du droit international et du droit de l'Union restent cohérentes* »[31]. Le Conseil rappelle toutefois que sa décision d'autoriser la négociation par la Commission européenne s'entendait « *sans préjudice* (…) *de la participation des*

[28] Conformément à l'art. 218(3) du Traité sur le fonctionnement de l'Union européenne (ci-après « TFUE »).

[29] Sont visées certaines directives en matière pénale, dont la directive CSAM (Directive 2011/93/EU), les instruments adoptés en matière de coopération policière et judiciaire en matière pénale, en matière de garanties procédurales minimales et en matière de protection des données (RGPD, directive 2016/680 dite « police-justice » et e-Evidence)

[30] 2ème considérant ; voy. également les art. 82(1) et (2) ainsi que l'art. 83(1) TFUE.

[31] 4ème considérant

États membres aux négociations (…), *ainsi que de toute décision ultérieure de conclure, signer ou ratifier une telle convention* »[32].

22. En Belgique, en vertu de l'art. 167, §§2 et 3 de la Constitution, les traités n'ont d'effet sur le plan interne qu'après avoir reçu l'**assentiment de l'assemblée parlementaire** compétente (la Chambre des représentants pour ce qui concerne le niveau fédéral). La Constitution n'impose pas que l'assentiment précède la ratification[33], mais la doctrine considère généralement qu'il est préférable de procéder à l'assentiment AVANT la ratification[34].

23. Par ailleurs, en vertu de l'art. 218.11 TFUE, « ***un État membre, le Parlement européen***, *le Conseil ou la Commission* ***peut recueillir l'avis de la Cour de justice sur la compatibilité d'un accord envisagé avec les traités***. *En cas d'avis négatif de la Cour, l'accord envisagé ne peut entrer en vigueur, sauf modification de celui-ci ou révision des traités* ». C'est ce que l'Autorité préconise de faire[35] (étant entendu que l'avis de la Cour affectera également l'art. 19.4 de la Convention de Budapest).

24. Toutefois, comme indiqué *supra*, de nombreuses dispositions de la Convention, étrangères à la protection des données, ont fait l'objet de critiques. Par conséquent, si le gouvernement devait envisager de déposer un projet de loi d'assentiment à cette Convention, l'Autorité recommande d'en **soumettre le texte**, préalablement au dépôt du projet de loi d'assentiment à la Chambre, à l'**Institut fédéral des droits humains**, pour avis.

---

[32] 6ème considérant

[33] Contrairement à l'art. 12 de l'accord de coopération du 8 mars 1994 entre l'Etat fédéral les Communautés et les Régions relatif aux modalités de conclusion des traités mixtes (MB 6.03.1996)

[34] Voy. Ch. Behrendt, La ratification des traités internationaux, une perspective de droit comparé (Belgique), Service de recherche du Parlement européen, p. 27

(https://www.europarl.europa.eu/RegData/etudes/STUD/2020/646197/EPRS_STU(2020)646197_FR.pdf); voy. également M. UYTTENDAELE, Précis de droit constitutionnel belge, Bruxelles, Bruylant, 2001, p. 880, qui précise qu'il en est ainsi « *afin d'éviter un conflit entre les pouvoirs législatif et exécutif et que ne surgisse une différence entre l'effet obligatoire du traité dans l'ordre international et dans l'ordre interne* ».

[35] Comme cela aurait d'ailleurs également dû être fait préalablement à l'adoption du Deuxième Protocole additionnel à la Convention du Conseil de l'Europe sur la cybercriminalité, adopté dans une certaine précipitation, précisément pour ne pas perdre la course contre le projet onusien de convention russo-chinoise et qu'il avait été indiqué au parlement européen qu'il s'agissait d'un projet « *bénéfique pour la préparation de dossiers législatifs prioritaires pour l'Espagne, tels que « CSAM »* » (voy. l'explication du vote de Juan Fernando López Aguilar en commission LIBE du Parlement européen (A9-0002/2023)) ; sur la comparaison entre la Convention de Budapest et la convention onusienne relative à la cybercriminalité, voy. https://dig.watch/updates/comparative-analysis-the-budapest-convention-vs-the-un-convention-against-cybercrime

PAR CES MOTIFS,

L'Autorité estime que,

- **à titre principal**, il convient de s'abstenir de donner son assentiment à la Convention des Nations Unies contre la cybercriminalité ;
- **à titre subsidiaire**, comme prévu à l'art. 218.11 TFUE, la Chambre des représentants devrait interroger la Cour de justice de l'Union européenne et/ou inviter ses homologues du Parlement européen à interroger ladite Cour sur la compatibilité de la Convention (et en particulier de l'art. 28.4 de celle-ci) avec les traités et en particulier avec les articles 7, 8, 11 et 52 de la Charte des droits fondamentaux de l'Union européenne et surseoir à donner son assentiment à ladite Convention dans l'attente de l'avis de la Cour.

Pour le Service d'Autorisation et d'Avis,
(sé) Cédrine Morlière - Directrice