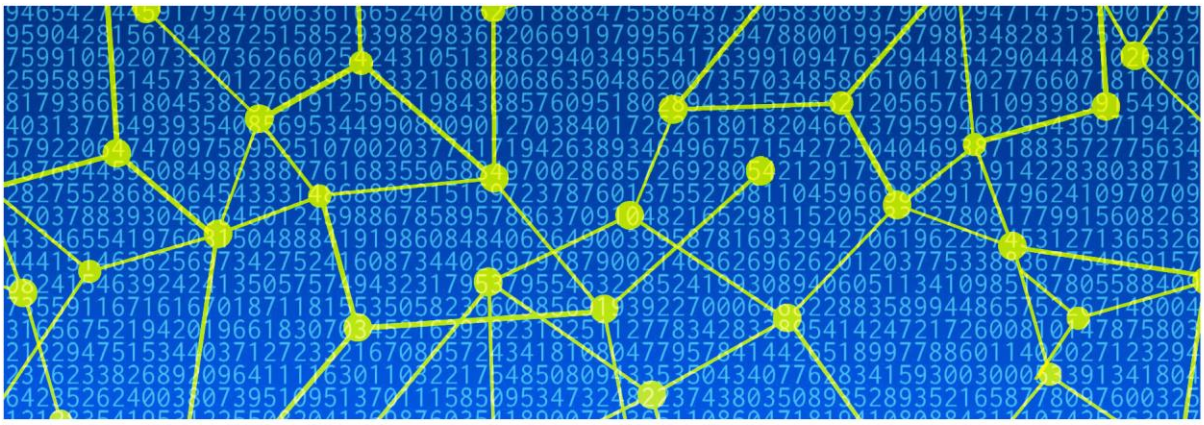

EUROPEAN DATA PROTECTION SUPERVISOR

Avis 7/2020

sur la proposition de dérogations temporaires à la directive 2002/58/CE aux fins de la lutte contre les abus sexuels commis contre des enfants en ligne

EDPS

10 novembre 2020

Le Contrôleur européen de la protection des données (CEPD) est une institution indépendante de l'Union européenne chargée, en vertu de l'article 52, paragraphe 2, du règlement (UE) 2018/1725, «[e]n ce qui concerne le traitement de données à caractère personnel, […] de veiller à ce que les libertés et droits fondamentaux des personnes physiques, notamment le droit à la protection des données, soient respectés par les institutions et organes de l'Union» et, en vertu de l'article 52, paragraphe 3, «de conseiller les institutions et organes de l'Union et les personnes concernées pour toutes les questions concernant le traitement des données à caractère personnel».

Wojciech Wiewiorówski a été nommé Contrôleur le 5 décembre 2019 pour un mandat de cinq ans.

En vertu de l'article 42, paragraphe 1, du règlement (UE) 2018/1725, «[à] la suite de l'adoption de propositions d'acte législatif, de recommandations ou de propositions au Conseil en vertu de l'article 218 du traité sur le fonctionnement de l'Union européenne ou lors de l'élaboration d'actes délégués ou d'actes d'exécution, la Commission consulte le Contrôleur européen de la protection des données en cas d'incidence sur la protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel», et de l'article 57, paragraphe 1, point g), dudit règlement, le CEPD «conseille, de sa propre initiative ou sur demande, l'ensemble des institutions et organes de l'Union sur les mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel».

Le présent avis a été rendu par le CEPD, dans le délai de huit semaines à compter de la réception de la demande de consultation prévu à l'article 42, paragraphe 3, du règlement (UE) 2018/1725, vu l'incidence sur la protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel de la proposition de la Commission relative au règlement du Parlement européen et du Conseil concernant une dérogation temporaire à certaines dispositions de la directive 2002/58/CE du Parlement européen et du Conseil en ce qui concerne l'utilisation de technologies par des fournisseurs de services de communications interpersonnelles non fondés sur la numérotation pour le traitement de données à caractère personnel et d'autres données aux fins de la lutte contre les abus sexuels commis contre des enfants en ligne.

Synthèse

Le 10 septembre 2020, la Commission a publié une proposition de règlement concernant une dérogation temporaire à certaines dispositions de la directive 2002/58/CE «vie privée et communications électroniques» en ce qui concerne l'utilisation de technologies par des fournisseurs de services de communications interpersonnelles non fondés sur la numérotation pour le traitement de données à caractère personnel et d'autres données aux fins de la lutte contre les abus sexuels commis contre des enfants en ligne. La dérogation concerne l'article 5, paragraphe 1, et l'article 6 de la directive «vie privée et communications électroniques» et porte sur le traitement de données à caractère personnel liées à la fourniture de services de communications interpersonnelles non fondés sur la numérotation nécessaire à l'utilisation de technologies dans le seul but de détecter ou signaler aux autorités les abus sexuels commis contre des enfants en ligne.

Dans le présent avis, le CEPD formule ses recommandations relatives à la proposition en réponse à une consultation formelle de la Commission en vertu de l'article 42 du règlement (UE) 2018/1725.

Il fait observer en particulier que les mesures envisagées dans la proposition constitueraient une ingérence dans les droits fondamentaux au respect de la vie privée et à la protection des données de tous les utilisateurs de services de communications électroniques très populaires, tels que les plateformes et applications de messagerie instantanée. **La confidentialité des communications est un élément essentiel des droits fondamentaux au respect de la vie privée et familiale. Même les mesures volontaires prises par des entreprises privées constituent une ingérence dans ces droits** lorsque ces mesures comprennent le suivi et l'analyse du contenu des communications et le traitement des données à caractère personnel.

Le CEPD tient à souligner que les questions en jeu ne sont pas spécifiques à la lutte contre les abus commis contre des enfants, mais à toute initiative visant la collaboration du secteur privé à des fins de répression. Si elle est adoptée, la proposition constituera inévitablement un précédent pour la législation future dans ce domaine. Le CEPD estime donc essentiel que cette proposition ne soit pas adoptée, même sous la forme d'une dérogation temporaire, tant que toutes les garanties nécessaires énoncées dans le présent avis ne sont pas intégrées.

En particulier, dans un souci de sécurité juridique, le CEPD estime qu'il est nécessaire de préciser si la proposition elle-même est destinée à fournir une base juridique au traitement au sens du règlement général sur la protection des données (RGPD). Dans le cas contraire, le CEPD recommande de préciser explicitement dans la proposition quelle base juridique au titre du RGPD serait applicable en l'espèce. À cet égard, le CEPD souligne que **les orientations données par les autorités chargées de la protection des données ne sauraient remplacer le respect de l'exigence de légalité**. Il est insuffisant de disposer que la dérogation temporaire est «sans préjudice» du RGPD et d'exiger la consultation préalable des autorités chargées de la protection des données. Le colégislateur doit assumer sa responsabilité et veiller à ce que la dérogation proposée soit conforme aux exigences de l'article 15, paragraphe 1, tel qu'interprété par la Cour de justice de l'Union européenne (CJUE).

Pour satisfaire à l'exigence de proportionnalité, **une réglementation doit prévoir des règles claires et précises régissant la portée et l'application des mesures en cause et imposant des exigences minimales, de telle sorte que les personnes dont les données à caractère personnel sont concernées disposent de garanties suffisantes permettant de protéger efficacement ces données contre les risques d'abus**.

Enfin, le CEPD est d'avis que la période de cinq ans proposée ne semble pas proportionnée compte tenu de l'absence a) de démonstration préalable de la proportionnalité de la mesure envisagée et b) de l'inclusion de garanties suffisantes dans le texte de la législation. Il estime que la durée de validité de toute mesure transitoire ne devrait pas dépasser deux ans.

TABLE DES MATIÈRES

I. Table des matières

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 16,

vu la charte des droits fondamentaux de l'Union européenne (la «charte»), et notamment ses articles 7 et 8,

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 ou RGPD)[1],

vu le règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données[2], et notamment son article 42, paragraphe 1, son article 57, paragraphe 1, point g), et son article 58, paragraphe 3, point c),

vu la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil[3],

A ADOPTÉ LE PRÉSENT AVIS:

1. INTRODUCTION

1.1 Contexte

1. Le 24 juillet 2020, la Commission a adopté une communication intitulée «*Stratégie de l'UE en faveur d'une lutte plus efficace contre les abus sexuels commis contre des enfants*»[4]. La communication indique qu'à partir de décembre 2020, la directive 2002/58/CE (la «directive "vie privée et communications électroniques"»)[5] aura un champ d'application élargi en raison du code des communications électroniques européen (le «CCEE»)[6], qui a déjà été adopté. Le CCEE élargit le champ d'application de la directive «vie privée et communications électroniques» aux services de communications interpersonnelles par contournement (OTT), tels que les services de messagerie et le courrier électronique. Selon la communication, cela empêcherait certaines entreprises (en l'absence de mesures législatives nationales adoptées en vertu de l'article 15, paragraphe 1, de la directive «vie privée et communications électroniques») de continuer à appliquer leurs propres mesures volontaires concernant la détection, la suppression et le signalement d'abus sexuels commis contre des enfants en ligne[7].

2. Le 10 septembre 2020, la Commission a publié[8] une proposition de règlement provisoire relatif au traitement de données à caractère personnel et d'autres données aux fins de la lutte contre les abus sexuels commis contre des enfants, qui prévoit une dérogation temporaire à l'article 5, paragraphe 1, et à l'article 6 de la directive «vie privée et communications électroniques» (la «proposition»). La Commission estime qu'une telle dérogation est nécessaire pour permettre la poursuite des activités volontaires actuelles après décembre 2020. Cette dérogation concernerait le traitement de données à caractère personnel dans le cadre de la fourniture de «*services de communications interpersonnelles non fondés sur la numérotation*»[9] (par exemple, voix sur IP, services de messagerie et services de courrier électronique web) strictement nécessaire à l'utilisation de technologies dans le seul but de supprimer le matériel pédopornographique et de détecter ou de signaler les abus sexuels commis contre des enfants en ligne aux autorités répressives et aux organismes agissant dans l'intérêt public contre ces abus. La proposition énumère plusieurs conditions pour que la dérogation soit applicable, lesquelles seront analysées ultérieurement dans le présent avis.

3. Le CEPD a été officiellement consulté par la Commission le 16 septembre 2020. Le 30 septembre, la Commission a lancé une consultation publique pour recueillir des avis sur sa proposition.

1.2 Relation avec la directive 2011/93/UE

4. L'UE a déjà adopté un instrument juridique complet pour lutter contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie, à savoir la directive 2011/93/UE (directive relative aux abus sexuels commis contre des enfants)[10].

5. La directive relative aux abus sexuels commis contre des enfants établit des règles minimales relatives à la définition des infractions pénales et des sanctions dans le domaine des abus sexuels et de l'exploitation sexuelle des enfants et de la pédopornographie. Elle impose aux États membres de veiller à ce que les comportements intentionnels suivants, lorsqu'ils sont commis sans droit[11], soient punissables:

   - le fait d'accéder intentionnellement et en connaissance de cause, au moyen des technologies de l'information et de la communication, à de la pédopornographie;

   - la distribution, la diffusion ou la transmission de pédopornographie;

   - le fait d'offrir, de fournir ou de mettre à disposition de la pédopornographie[12].

6. La directive relative aux abus sexuels commis contre des enfants oblige également les États membres à prendre les mesures nécessaires pour que soient punissables certains comportements assimilables à de la sollicitation d'enfants à des fins sexuelles, y compris au moyen des technologies de l'information et de la communication.

7. La directive relative aux abus sexuels commis contre des enfants oblige les États membres à prendre les mesures nécessaires pour faire rapidement *supprimer les pages internet* contenant ou diffusant de la pédopornographie qui sont hébergées sur leur territoire et à s'efforcer d'obtenir la suppression des pages hébergées en dehors de celui-ci, ainsi que de saisir et confisquer les instruments et produits de telles infractions[13]. En outre, les États

membres peuvent prendre des mesures pour *bloquer l'accès par les internautes* sur leur territoire *aux pages internet* contenant ou diffusant de la pédopornographie[14].

8. En 2010, le CEPD a publié de sa propre initiative un avis sur la proposition de directive relative à l'exploitation et aux abus sexuels concernant des enfants et à la pédopornographie[15]. Cet avis contient des considérations et des recommandations qui sont également pertinentes pour la présente proposition de règlement provisoire. Le cas échéant, le CEPD réitère son avis de 2010 et/ou y fait référence.

2. RECOMMANDATIONS PRINCIPALES

9. La confidentialité des communications est un élément essentiel des droits fondamentaux au respect de la vie privée et familiale et à la protection des données à caractère personnel. Même les mesures volontaires prises par des entreprises privées **constituent une ingérence dans ces droits** lorsque ces mesures comprennent le suivi et l'analyse du contenu des communications et le traitement des données à caractère personnel. Les mesures envisagées par la proposition constitueront une ingérence dans les droits au respect de la vie privée et à la protection des données des personnes concernées (utilisateurs, auteurs d'abus présumés et victimes).

10. Il est possible d'enfreindre la confidentialité des communications, mais uniquement sous certaines conditions. Des limitations ne peuvent être apportées que si elles sont **prévues par la loi, respectent le contenu essentiel** des droits à la protection des données et à la vie privée et, dans le respect du principe de proportionnalité, qu'elles sont **nécessaires et répondent effectivement à des objectifs d'intérêt général** reconnus par l'Union ou au besoin de protection des **droits et libertés d'autrui** (article 52, paragraphe 1, de la charte)[16].

11. La Commission maintient que la proposition **vise simplement** à permettre **la poursuite de certaines pratiques volontaires existantes**, et non pas à créer une nouvelle ingérence dans ces droits fondamentaux. Toutefois, la dérogation temporaire est proposée précisément en raison du champ d'application élargi de la directive «vie privée et communications électroniques» résultant de l'entrée en vigueur du CCEE en décembre 2020. Le CEPD tient à souligner que c'est le législateur européen qui a choisi d'élargir la notion de «*service de communications électroniques*» à des services en ligne fonctionnellement équivalents, afin de garantir que les utilisateurs finaux et leurs droits sont effectivement et équitablement protégés lorsqu'ils utilisent ces services[17]. Les limitations à la confidentialité des communications ne sauraient être justifiées au seul motif que certaines mesures ont été précédemment mises en place alors que les services concernés ne constituaient pas, d'un point de vue juridique, des services de communications électroniques. À compter du 21 décembre 2020, les services en question seront considérés comme des services de communications électroniques, avec pour corollaire la protection juridique de la confidentialité. La dérogation proposée doit donc être évaluée conformément aux exigences de l'article 52 de la charte.

12. Le CEPD tient à souligner que les questions en jeu **ne sont pas spécifiques à la lutte contre les abus commis contre des enfants**, mais à toute initiative visant la collaboration du secteur privé à des fins de répression[18]. Les abus commis contre des enfants sont des crimes particulièrement abjects, et l'objectif visant à permettre une action efficace pour lutter

contre les abus sexuels commis contre des enfants en ligne constitue clairement un objectif d'intérêt général reconnu par l'Union et vise à protéger les droits et libertés d'autrui[19]. En ce qui concerne la lutte effective contre les infractions pénales dont sont victimes les mineurs et les autres personnes vulnérables, la CJUE a signalé que des **obligations positives** peuvent résulter de l'article 7 de la charte, imposant aux autorités publiques d'**adopter des mesures juridiques** visant à protéger la vie privée et familiale. De telles obligations sont également susceptibles de découler dudit article 7 en ce qui concerne la protection du domicile et des communications, ainsi que des articles 3 et 4 s'agissant de la protection de l'intégrité physique et psychique des personnes ainsi que de l'interdiction de la torture et des traitements inhumains et dégradants[20].

13. Le CEPD a déjà **remis en cause** auparavant **les mécanismes purement volontaires** pour lutter contre la diffusion de matériel pédopornographique, compte tenu de la nature de l'ingérence et de la nécessité d'assurer une sécurité juridique pour tous les acteurs concernés[21]. En effet, il est nécessaire de veiller à la mise en place de **procédures harmonisées, claires et détaillées** dans le cadre de la lutte contre les contenus illicites, et ce sous la supervision d'autorités publiques indépendantes.

14. Même si la proposition n'*oblige* pas les parties privées à porter atteinte à la confidentialité des communications, elle prévoit néanmoins une restriction de la confidentialité des communications. Compte tenu de la nature de l'ingérence en cause, le CEPD estime que les mesures de détection, de suppression et de signalement des abus sexuels commis contre des enfants en ligne doivent s'accompagner d'**un cadre juridique complet** qui réponde aux exigences des articles 7 et 8 de la charte. Pour satisfaire à l'exigence de proportionnalité, une réglementation doit prévoir des **règles claires et précises régissant la portée et l'application des mesures** en cause et imposant des **exigences minimales**, de telle sorte que les personnes dont les données à caractère personnel sont concernées disposent de garanties suffisantes permettant de protéger efficacement ces données contre les risques d'abus[22]. Cette réglementation doit être légalement contraignante et, en particulier, indiquer **en quelles circonstances et sous quelles conditions** une mesure prévoyant le traitement de telles données peut être prise, garantissant ainsi que l'ingérence soit **limitée au strict nécessaire**[23]. Comme l'a précisé la CJUE, la nécessité de disposer de telles garanties est d'autant plus importante lorsque les données à caractère personnel sont soumises à un traitement automatisé, et lorsqu'est en jeu la protection de cette catégorie particulière de données à caractère personnel que sont les données sensibles[24].

15. Il est d'autant plus nécessaire d'introduire des **garanties appropriées** dans la proposition elle-même qu'elle a trait à un règlement et non à une directive. Le choix d'un instrument juridique directement applicable dans tous les États membres engage la responsabilité du législateur de l'UE, qui doit veiller à ce que les garanties appropriées soient déjà mises en place au niveau de l'UE.

3. RECOMMANDATIONS SPÉCIFIQUES

3.1. Base juridique

16. Le considérant 10 de la proposition indique que le règlement (UE) 2016/679 (RGPD)[25] reste applicable au traitement des données à caractère personnel relevant du champ d'application de la dérogation. Conformément à l'article 6 du RGPD, le traitement de données à caractère personnel n'est licite que si l'une des six conditions énoncées à l'article 6, paragraphe 1, points a) à f), est remplie.

17. La proposition n'indique pas clairement si elle vise ou non à fournir une base juridique au sens de l'article 6 du RGPD. L'exposé des motifs indique simplement que la directive «vie privée et communications électroniques» «*ne contient pas de base juridique explicite*» pour le traitement volontaire de contenus ou de données relatives au trafic aux fins de la détection d'abus sexuels commis contre des enfants en ligne. Il signale également qu'en l'absence de mesures législatives prévoyant une dérogation, les fournisseurs de services de communications interpersonnelles non fondés sur la numérotation «*manqueraient d'une base juridique*» pour continuer à détecter les abus sexuels commis contre des enfants sur leurs services[26].

18. Dans un souci de sécurité juridique, le CEPD estime qu'il est nécessaire de **préciser** si la proposition elle-même est destinée à fournir une **base juridique** au traitement au sens du RGPD. Dans le cas contraire, le CEPD recommande de préciser explicitement dans la proposition quelle base juridique au titre du RGPD serait applicable en l'espèce.

19. À cet égard, le CEPD remarque que la dérogation prévue par la proposition porte sur le traitement *volontaire* de contenus ou de données relatives au trafic aux fins de la détection d'abus sexuels commis contre des enfants en ligne. En d'autres termes, elle n'obligerait pas les fournisseurs de services de communications interpersonnelles non fondés sur la numérotation à effectuer un traitement quelconque. En conséquence, la base juridique du traitement ne repose pas sur l'article 6, paragraphe 1, point c), du RGPD (le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis).

20. Dans son avis de 2014 sur la notion d'intérêt légitime du responsable du traitement, le groupe de travail «article 29» a estimé que les intérêts légitimes poursuivis par le responsable du traitement «*[peuvent comprendre] notamment de[s] situations où le responsable du traitement va plus loin que les obligations légales spécifiques qui lui sont imposées par des lois ou des réglementations afin d'aider les services répressifs ou des acteurs privés dans leur lutte contre des activités illégales, comme la séduction malintentionnée de mineurs. Dans ces situations, cependant, il importe particulièrement de veiller à ce que les limites prévues par l'article 7, point f), soient pleinement respectées*[27].

21. Le CEPD fait observer que la déclaration susmentionnée ne signifie pas que *tout* traitement effectué pour lutter contre des activités illégales puisse automatiquement être considéré comme licite au sens de l'article 6, paragraphe 1, point f), du RGPD. Premièrement, le traitement en question doit remplir trois conditions cumulatives, à savoir, i) la poursuite d'un intérêt légitime par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, ii) la nécessité du traitement des données à caractère

personnel pour la réalisation de l'intérêt légitime poursuivi et, iii) la condition que les droits et les libertés fondamentaux de la personne concernée par la protection des données ne prévalent pas[28]. Deuxièmement, la déclaration du groupe de travail «article 29» est d'ordre général, et ne laisse pas entendre que les responsables du traitement pourraient être autorisés à se fonder sur la base juridique de l'intérêt légitime dans les affaires portant atteinte à la confidentialité des communications.

3.2. Nécessité et proportionnalité

22. En l'absence d'une analyse d'impact accompagnant la proposition, la Commission **n'a pas encore démontré** que les mesures envisagées par cette proposition sont **strictement nécessaires, efficaces et proportionnées** pour atteindre l'objectif visé. Dans un premier temps, le CEPD invite la Commission à fournir des informations supplémentaires pour permettre au colégislateur d'étudier si les mesures envisagées répondent effectivement aux exigences de nécessité, d'efficacité et de proportionnalité[29].

23. Afin de pouvoir évaluer l'incidence d'une mesure sur les droits fondamentaux à la vie privée et à la protection des données à caractère personnel, il est essentiel, en particulier, de déterminer précisément[30]:

- la **portée** de la mesure, y compris le nombre de personnes concernées et le risque éventuel d'«*intrusion collatérale*» (c'est-à-dire d'ingérence dans la vie privée de personnes autres que les personnes concernées par la mesure);
- sa **mesure**, y compris la quantité d'informations collectées; la durée de la collecte; le besoin ou non, dans le cadre de la mesure examinée, de collecter et traiter des catégories particulières de données;
- le **degré d'intrusion**, en s'interrogeant: sur la **nature de l'activité** sur laquelle porte la mesure (si elle affecte des activités soumises à une obligation de confidentialité telles que les relations entre un avocat et son client, les activités médicales); sur le **contexte**; sur le fait qu'il puisse s'agir en réalité de **profilage** des individus concernés; sur le fait que le traitement puisse supposer l'utilisation de systèmes de prise de décision **automatisés** (entièrement ou en partie) comportant un «taux d'erreur»;
- si la mesure concerne des personnes **vulnérables** ou non;
- si la mesure **porte également sur d'autres droits fondamentaux** (par exemple, le droit à la protection de la vie privée et le droit à la libre expression, comme dans les affaires Digital Rights et Tele2).

Dans ce contexte, il est également important de signaler que l'incidence peut être faible pour l'individu concerné, mais n'en être pas moins considérable ou très considérable pour la société dans son ensemble[31].

24. Le CEPD constate que différentes mesures de lutte contre les abus sexuels commis contre des enfants en ligne peuvent comporter **différents degrés d'intrusion**. À titre de question préalable, le CEPD fait observer que l'analyse automatisée d'un discours ou d'un texte en vue d'identifier des cas potentiels de sollicitation d'enfants est susceptible de constituer une ingérence plus importante que la mise en correspondance d'images ou de vidéos sur la base de cas de pédopornographie précédemment confirmés.

25. Le considérant 11 de la proposition dispose que «*[l]es types de technologies déployés devraient être les moins intrusifs dans la vie privée en l'état actuel de la technique dans le secteur, ne devraient pas comporter de filtrage et de contrôle systématiques des communications contenant du texte et devraient n'examiner que des communications spécifiques en cas d'éléments concrets conduisant à soupçonner des abus sexuels contre des enfants*». Bien que le CEPD salue l'intention sous-jacente de délimiter la portée de l'ingérence, il convient de formuler plusieurs observations. Premièrement, toute délimitation ayant une incidence sur la **portée de l'ingérence devrait être clairement reflétée dans le texte** même de la proposition, et non pas seulement dans un considérant. Deuxièmement, il convient d'indiquer clairement si les **communications contenant des données autres que du texte** (par exemple, des images ou des données audio) pourraient faire l'objet d'un filtrage et d'un suivi systématiques. Troisièmement, il est nécessaire de clarifier la **manière dont les «*éléments concrets conduisant à soupçonner des abus*» seront déterminés dans la pratique** et, en particulier, si une telle détermination fait intervenir ou non une autorité compétente.

26. En ce qui concerne la technologie utilisée pour détecter la sollicitation d'enfants, l'article 3, point c), de la proposition dispose que la technologie utilisée doit «*se limite[r] à l'utilisation d'indicateurs clés, tels que des mots-clés et des facteurs de risque déterminés objectivement, tels que la différence d'âge, sans préjudice du droit à un examen humain*». À cet égard, le CEPD estime que **l'analyse générale, indifférenciée et automatisée de toutes les communications textuelles transmises par l'intermédiaire de services de communications interpersonnelles non fondés sur la numérotation en vue de détecter de nouvelles infractions potentielles ne respecte pas les principes de nécessité et de proportionnalité**. Même si la technologie utilisée se limite à l'utilisation d'«*indicateurs clés*», le CEPD estime que le déploiement d'une telle analyse générale et indifférenciée est excessif.

27. En ce qui concerne le «***droit à un examen humain***» mentionné à l'article 3, point c), de la proposition, le CEPD demande instamment au colégislateur de préciser plus clairement quand un tel droit deviendrait applicable et quelle entité serait chargée de procéder à cet examen. Ce point est particulièrement important pour veiller à la mise en place de **mécanismes de recours** appropriés [voir également les sections 6.5 (signalement aux autorités publiques) et 6.6 (transparence et droits des personnes concernées)]. Enfin, l'utilisation du terme «*droit*» laisse entendre que l'examen humain ne serait pas mis en œuvre par défaut. Le CEPD demande instamment au législateur de préciser dans quelles circonstances un examen humain sera assuré et par qui. Cette précision est d'autant plus nécessaire pour clarifier dans quelles circonstances l'utilisation de la technologie **pourrait constituer une prise de décision automatisée** au sens de l'article 22 du RGPD (compte tenu notamment des conséquences possibles du signalement et du blocage des utilisateurs envisagés par la proposition).

3.3. Champ d'application et étendue de la dérogation

28. La proposition porte sur les «*services de communications interpersonnelles non fondés sur la numérotation*», qui comprennent un large éventail de services, tels que la voix sur IP, les services de messagerie et les services de courrier électronique web. Des précisions devraient être apportées quant aux **types de services** qui seraient concernés par la dérogation. Par exemple, il convient de préciser sans ambiguïté si la dérogation concerne

les mesures visant à détecter les contenus pédopornographiques sous forme de vidéos et d'images, ou également de messages textuels et d'appels vocaux. Ce point est nécessaire pour satisfaire à l'exigence selon laquelle la réglementation doit établir des règles *claires et précises* régissant la portée et l'application de la mesure.

29. Dans le même ordre d'idées, il convient de clarifier davantage les **types de mesures de détection** qui relèveraient du champ d'application de la dérogation. L'article 3 de la proposition énonce plusieurs conditions pour que la dérogation soit applicable, mais ne fournit pas de description claire des types de mesures envisagées[32]. L'article 3, point c), indique que des «*indicateurs clés, tels que des mots-clés et des facteurs de risque déterminés objectivement, tels que la différence d'âge*», seraient utilisés pour détecter la sollicitation d'enfants, tandis que l'article 3, point e), sous-entend in fine que la détection de pédopornographie peut supposer «*l'utilisation d'une signature numérique non reconvertible ("hachage")*». Une compréhension claire de la nature précise des mesures limitant la confidentialité des communications est nécessaire non seulement pour garantir la clarté et la sécurité juridique, mais également pour déterminer si les mesures sont effectivement limitées au strict nécessaire.

30. Troisièmement, il est nécessaire de clarifier davantage l'**étendue** des communications auxquelles les «*technologies bien établies*» seraient appliquées. En particulier, il convient de préciser ce qu'il faut entendre exactement par «*technologies bien établies*» et si ces technologies seraient appliquées à toutes les communications échangées par tous les utilisateurs ou à un sous-ensemble de celles-ci. Dans ce dernier cas, il serait nécessaire de préciser les critères selon lesquels ces technologies seraient appliquées à un sous-ensemble spécifique de communications.

31. Le CEPD se demande si l'**étendue de la dérogation proposée** est strictement nécessaire pour atteindre les objectifs fixés par la proposition. Plus précisément, le CEPD se demande si la dérogation à l'intégralité de l'article 6 de la directive «vie privée et communications électroniques» est justifiée, étant donné que cet article concerne principalement des activités de traitement qui n'ont aucun rapport avec le traitement envisagé par la proposition. En outre, l'article 6, paragraphe 1, dispose explicitement qu'il est sans préjudice de l'article 15, paragraphe 1, de la directive «vie privée et communications électroniques». Enfin, l'article 5, paragraphe 1, fait également référence aux «*données relatives au trafic [...] afférentes [aux communications]*», ce qui semble plus directement en lien avec les objectifs sous-jacents de la proposition.

3.4. Limitation de la finalité et limitation du stockage

32. La proposition prévoit parmi les conditions à la dérogation que le traitement soit «*limité à ce qui est strictement nécessaire pour détecter et signaler les abus sexuels commis contre des enfants en ligne et pour supprimer le matériel pédopornographique et que, sauf si un abus sexuel contre des enfants en ligne a été détecté et confirmé, les données soient effacées immédiatement*». Le CEPD comprend que l'obligation d'effacer les données fait référence à toutes les «***données à caractère personnel et autres données***» couvertes par le champ d'application de la dérogation. Le CEPD demande instamment au colégislateur d'être **plus explicite** à cet égard, en précisant également les catégories spécifiques de données qui peuvent être conservées.

33. La proposition dispose également qu'en ce qui concerne le point d), lorsque des abus sexuels commis contre des enfants en ligne ont été détectés et confirmés, les *données y afférentes* peuvent être conservées uniquement aux fins suivantes et pendant la période nécessaire: i) pour établir un rapport et répondre à des demandes proportionnées des services répressifs et d'autres autorités publiques compétentes; ii) pour bloquer le compte de l'utilisateur concerné; et iii) en relation avec des données identifiées de manière fiable comme pédopornographiques, aux fins de la création d'une signature numérique unique non reconvertible («hachage»). Là encore, le CEPD encourage le colégislateur à préciser, dans le texte de la proposition, **quelles catégories de données constitueraient des «*données […] afférentes*»** pour chacune de ces finalités et **quels destinataires constituent de fait d'«*autres autorités publiques concernées*»**.

34. Le CEPD se demande si le signalement des personnes et le blocage du compte des utilisateurs concernés seront strictement nécessaires et proportionnés dans tous les cas, compte tenu également de l'absence d'informations complémentaires sur **ce qui constitue un cas «*détecté et confirmé*»** d'abus sexuels commis contre des enfants en ligne. La réception non sollicitée de matériel pédopornographique justifierait-elle le signalement et/ou le blocage? Le processus de confirmation comporte-t-il, par définition, un examen humain[33]? Qui procède à la confirmation et qui détermine si le titulaire du compte est effectivement coupable des actes décrits à l'article 2, paragraphe 2, de la proposition? Si le CEPD soutient l'objectif visant à neutraliser rapidement les moyens utilisés pour commettre des abus sexuels contre des enfants en ligne, le cadre juridique devrait être suffisamment clair et précis pour ce qui est des **circonstances dans lesquelles les mesures décrites peuvent être prises**.

35. Enfin, si la proposition prévoit que les «*données […] afférentes*» ne devraient être conservées que dans la mesure nécessaire pour atteindre les fins énumérées, il n'y aucune clarté quant à la **durée de conservation des données** en vue de «*répondre à des demandes proportionnées des services répressifs et d'autres autorités publiques compétentes*»[34]. La proposition ne fournit pas d'indication claire de durée effective à cet égard. Elle ne précise pas non plus expressément quelles entités seraient autorisées à poursuivre le traitement des données pertinentes de manière à permettre l'identification des personnes concernées (auteurs présumés et victimes)[35].

3.5. Signalement aux autorités compétentes

36. En ce qui concerne le signalement, le CEPD a déjà indiqué précédemment qu'il était nécessaire de **définir précisément** dans le texte de la réglementation **les personnes habilitées à collecter et conserver des informations**, ainsi que les conditions dans lesquelles elles y sont autorisées[36]. Cela est particulièrement important compte tenu des conséquences d'un signalement: les données à caractère personnel en jeu sont non seulement celles des enfants, mais aussi celles de l'ensemble des personnes liées d'une manière ou d'une autre aux informations circulant sur le réseau, par exemple les informations concernant une personne soupçonnée de comportement préjudiciable, qu'il s'agisse d'un internaute ou d'un fournisseur de contenus, mais aussi celles concernant une personne signalant un contenu suspect ou la victime de l'abus[37].

37. À cet égard, le CEPD s'inquiète particulièrement du fait que la proposition n'explique pas le modèle de gouvernance des fournisseurs de services électroniques ayant recours à cette

dérogation. La manière dont les fournisseurs de services électroniques effectueront le signalement, et à qui, n'est pas claire. Il n'est pas non plus précisé qui sera chargé de la maintenance et de la mise à jour des bases de données pertinentes pour détecter les futurs cas d'abus sexuels commis contre des enfants en ligne.

38. S'agissant des exigences de **qualité** et d'**intégrité**, il conviendrait de mettre en œuvre des mesures supplémentaires afin de garantir que ces informations, considérées comme des preuves numériques, ont été dûment recueillies et conservées et qu'elles seront donc recevables en justice. Les garanties liées à la supervision du système et à son utilisation, qui doit en principe être assurée par les autorités répressives, sont des éléments incontournables. La transparence et la mise à disposition de possibilités de recours devant une instance indépendante sont d'autres éléments essentiels à intégrer dans un tel mécanisme[38].

3.6. Transparence et droits des personnes concernées

39. La proposition ne contient aucune disposition concernant **la transparence et l'exercice des droits des personnes concernées**. Dans la mesure où la proposition est destinée à être «*sans préjudice*» du RGPD, les obligations du fournisseur d'informer les personnes et de tenir compte des droits des personnes concernées restent en principe inchangées. Néanmoins, le CEPD recommande au colégislateur d'introduire des mesures supplémentaires pour garantir la transparence et l'exercice des droits des personnes concernées, sous réserve, lorsque cela est strictement nécessaire, de restrictions précisément définies (par exemple, pour protéger la confidentialité d'une enquête en cours). Ces restrictions doivent, en tout état de cause, être conformes aux exigences énoncées à l'article 23, paragraphes 1 et 2, du RGPD.

40. En ce qui concerne les utilisateurs, la proposition de règlement relatif à la prévention de la diffusion de contenus à caractère terroriste en ligne offre un exemple de mesures possibles pour garantir la transparence et mettre en place des dispositifs de réclamation[39]. Outre des obligations générales en matière de transparence (article 8) et des dispositifs de réclamation (article 9), elle prévoit également la mise à disposition d'informations à l'intention du fournisseur de contenus (sous réserve d'une dérogation lorsque les autorités compétentes décident que, pour des raisons de sécurité publique, notamment dans le cadre d'une enquête, il est jugé inapproprié ou contre-productif de notifier directement au fournisseur de contenus la suppression de contenus ou le blocage de l'accès à ceux-ci) (article 11). Même s'il est probable que des adaptations supplémentaires seront nécessaires, il peut être utile de prendre ces exemples en considération, étant donné que le colégislateur de l'UE cherche à intégrer des garanties supplémentaires dans le texte du règlement.

3.7. Suivi des évolutions de l'état de la technique

41. L'article 3, point a), de la proposition limite le champ d'application de la dérogation aux «*[…] technologies bien établies régulièrement utilisées à cette fin par les fournisseurs de services de communications interpersonnelles non fondés sur la numérotation avant l'entrée en vigueur du présent règlement […]*». Le CEPD souligne que ces «*technologies bien établies*» ne sont pas décrites dans la proposition. Cette absence de définition précise des mesures faisant l'objet de la dérogation est susceptible de porter atteinte à la sécurité juridique.

42. Le fait de limiter les mesures à celles régulièrement utilisées avant la future entrée en vigueur de la proposition empêcherait l'évolution future vers des mesures techniques et organisationnelles moins intrusives. Le considérant 11 de la proposition indique que le règlement n'exclut pas que «*cette technologie puisse encore évoluer dans le respect de la vie privée*», mais cette affirmation n'est pas étayée par le texte même de la proposition.

43. Le CEPD recommande donc de préciser dans le texte de la proposition que la **référence aux technologies régulièrement utilisées** avant la future entrée en vigueur de la proposition **n'empêche pas le déploiement de technologies ayant une finalité similaire** qui sont moins intrusives dans la vie privée, conformément aux exigences de minimisation des données, de protection des données dès la conception et de protection des données par défaut.

3.8. Analyse d'impact relative à la protection des données (AIPD) et consultation préalable

44. Le considérant 10 de la proposition précise que l'obligation de procéder, avant le déploiement des technologies concernées, à une analyse d'impact des opérations de traitement envisagées en application de l'article 35 du RGPD («AIPD») s'applique «*lorsque cela est approprié*».

45. Le CEPD fait observer, conformément à l'article 35, paragraphe 1, du RGPD, que la réalisation d'une AIPD est requise lorsque le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, compte tenu de la nature, de la portée, du contexte et des finalités du traitement. Compte tenu des orientations pertinentes, il est très probable que le traitement envisagé par la proposition atteigne ce seuil (étant donné que le traitement est susceptible d'être de grande ampleur par nature, de comprendre le traitement de données sensibles ou de données à caractère hautement personnel, etc.)[40].

46. Le CEPD recommande l'introduction, également en vue de fournir une sécurité juridique, d'une exigence explicite de réalisation d'une AIPD au sens de l'article 35 du RGPD pour tout traitement relevant du champ d'application de la dérogation proposée. Bien que la réalisation d'une AIPD ne soit pas toujours nécessaire pour les opérations de traitement qui étaient déjà effectuées au 25 mai 2018[41], les responsables du traitement sont tenus de procéder à une AIPD, le moment venu, dans le cadre de leurs obligations générales en matière de responsabilité[42]. L'ajout d'une exigence explicite à cet égard apporterait une plus grande clarté et une assurance que le traitement sera effectué conformément au RGPD.

47. En ce qui concerne l'exigence de consultation préalable conformément à l'article 36 du RGPD, le CEPD prend note de l'exigence proposée par le Conseil[43] selon laquelle la procédure de consultation préalable prévue à l'article 36 du RGPD s'applique à toute technologie qui n'a pas été utilisée avant l'entrée en vigueur de la proposition. Le CEPD tient toutefois à souligner qu'une telle obligation continue d'être applicable dans toute situation où une AIPD révèle des risques résiduels élevés[44].

48. Enfin, le CEPD souhaite souligner que **les orientations des autorités chargées de la protection des données ne sauraient remplacer le respect de l'exigence de légalité**. Étant donné que la proposition prévoit une dérogation à la confidentialité des

communications, il est **insuffisant** de disposer que la dérogation temporaire est **«*sans préjudice*» du RGPD** et d'exiger la consultation préalable des autorités chargées de la protection des données et/ou d'inviter le comité européen de la protection des données à émettre des orientations. Le colégislateur doit assumer sa responsabilité et veiller à ce que la dérogation proposée soit conforme aux exigences de l'article 15, paragraphe 1, tel qu'interprété par la CJUE.

3.9. Durée de la dérogation temporaire

49. L'article 4 de la proposition précise que le règlement s'applique du 21 décembre 2020 au 31 décembre 2025, c'est-à-dire pour une période de cinq ans. Le considérant 16 précise que la période d'application de ce règlement a été choisie comme étant «*la période raisonnablement nécessaire à l'adoption d'un nouveau cadre juridique à long terme*». Si la législation à long terme annoncée était adoptée et entrait en vigueur avant cette date, cette législation devrait abroger le présent règlement.

50. Le CEPD est d'avis que la période de cinq ans proposée est trop longue et ne semble pas proportionnée compte tenu de l'absence a) de démonstration préalable de la proportionnalité de la mesure envisagée et b) de l'inclusion de garanties suffisantes dans le texte de la législation. **Il recommande que la durée de validité de toute mesure transitoire ne dépasse pas deux ans.**

51. Si elle est adoptée, la proposition constituera inévitablement un précédent pour la future réglementation relative à la lutte contre la diffusion de contenus illicites en ligne, en particulier en ce qui concerne les communications confidentielles. **Le CEPD estime donc essentiel que le règlement ne soit pas adopté, même sous la forme d'une dérogation temporaire, tant que les garanties nécessaires et tous les éléments manquants recensés dans les présentes recommandations spécifiques ne sont pas intégrés.**

4. CONCLUSIONS

52. Les mesures envisagées dans la proposition constitueraient une ingérence dans les droits fondamentaux au respect de la vie privée et à la protection des données de tous les utilisateurs de services de communications électroniques très populaires, tels que les plateformes et applications de messagerie instantanée. Même les mesures volontaires prises par des entreprises privées constituent une ingérence dans ces droits lorsque ces mesures comprennent le suivi et l'analyse du contenu des communications et le traitement des données à caractère personnel.

53. Les questions en jeu ne sont pas spécifiques à la lutte contre les abus commis contre des enfants, mais à toute initiative visant la collaboration du secteur privé à des fins de répression. Si elle est adoptée, la proposition constituera inévitablement un précédent pour la législation future dans ce domaine. Le CEPD estime donc essentiel que cette proposition ne soit pas adoptée, même sous la forme d'une dérogation temporaire, tant que toutes les garanties nécessaires énoncées dans le présent avis ne sont pas intégrées.

54. Dans un souci de sécurité juridique, le CEPD estime qu'il est nécessaire de préciser si la proposition elle-même est destinée à fournir une base juridique au traitement au sens du RGPD. Dans le cas contraire, le CEPD recommande de préciser explicitement dans la proposition quelle base juridique au titre du RGPD serait applicable en l'espèce. À cet égard, le CEPD souligne que les orientations données par les autorités chargées de la protection des données ne sauraient remplacer le respect de l'exigence de légalité. Il est insuffisant de disposer que la dérogation temporaire est «*sans préjudice*» du RGPD et d'exiger la consultation préalable des autorités chargées de la protection des données. Le colégislateur doit assumer sa responsabilité et veiller à ce que la dérogation proposée soit conforme aux exigences de l'article 15, paragraphe 1, tel qu'interprété par la CJUE.

55. Pour satisfaire à l'exigence de proportionnalité, une réglementation doit prévoir des règles claires et précises régissant la portée et l'application des mesures en cause et imposant des exigences minimales, de telle sorte que les personnes dont les données à caractère personnel sont concernées disposent de garanties suffisantes permettant de protéger efficacement ces données contre les risques d'abus.

56. L'absence de définition précise des mesures faisant l'objet de la dérogation est susceptible de porter atteinte à la sécurité juridique.

57. Enfin, le CEPD est d'avis que la période de cinq ans proposée ne semble pas proportionnée compte tenu de l'absence a) de démonstration préalable de la proportionnalité de la mesure envisagée et b) de l'inclusion de garanties suffisantes dans le texte de la législation. Il estime que la durée de validité de toute mesure transitoire ne devrait pas dépasser deux ans.

Fait à Bruxelles, le 10 novembre 2020

Wojciech Wiewiorowski

(signature électronique)

Notes

[1] JO L 119 du 4.5.2016, p. 1.
[2] JO L 295 du 21.11.2018, p. 39.
[3] JO L 119 du 4.5.2016, p. 89.
[4] COM(2020) 607 final, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20200724_com-2020-607-commission-communication_fr.pdf.
[5] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive «vie privée et communications électroniques»), JO L 201 du 31.7.2002, p. 37.
[6] Directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen, JO L 321 du 17.12.2018, p. 36.
[7] COM(2020) 607 final, p. 4. La communication fait observer qu'étant donné que la directive «vie privée et communications électroniques» ne contient pas de base juridique pour le traitement *volontaire* du contenu et des données de trafic aux fins de la détection des abus sexuels commis contre des enfants, les fournisseurs peuvent uniquement appliquer de telles mesures sur la base d'une mesure législative nationale, qui répond aux exigences de l'article 15 de la directive «vie privée et communications électroniques» restreignant le droit à la confidentialité. En l'absence de pareilles mesures législatives, les mesures volontaires destinées à détecter les abus sexuels commis contre des enfants adoptées par ces fournisseurs, qui traitent du contenu ou des données de trafic, seraient dépourvues de base juridique.
[8] COM(2020) 568 final, 2020/0259 (COD), proposition de règlement du Parlement européen et du Conseil concernant une dérogation temporaire à certaines dispositions de la directive 2002/58/CE du Parlement européen et du Conseil en ce qui concerne l'utilisation de technologies par des fournisseurs de services de communications interpersonnelles non fondés sur la numérotation pour le traitement de données à caractère personnel et d'autres données aux fins de la lutte contre les abus sexuels commis contre des enfants en ligne, https://ec.europa.eu/digital-single-market/en/news/interim-regulation-processing-personal-and-other-data-purpose-combatting-child-sexual-abuse.
[9] Selon l'article 2, paragraphe 5, du CCEE, un «*service de communications interpersonnelles*» est «*un service normalement fourni contre rémunération qui permet l'échange interpersonnel et interactif direct d'informations via des réseaux de communications électroniques entre un nombre fini de personnes, par lequel les personnes qui amorcent la communication ou y participent en déterminent le ou les destinataires et qui ne comprend pas les services qui rendent possible une communication interpersonnelle et interactive uniquement en tant que fonction mineure accessoire intrinsèquement liée à un autre service*». Un «*service de communications interpersonnelles non fondé sur la numérotation*» est un service de communications interpersonnelles qui n'établit pas de connexion à des ressources de numérotation attribuées publiquement, c'est-à-dire un numéro ou des numéros figurant dans des plans nationaux ou internationaux de numérotation, ou qui ne permet pas la communication avec un numéro ou des numéros figurant dans des plans nationaux ou internationaux de numérotation (article 2, paragraphe 7, du CCEE).
[10] Directive 2011/93/UE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil, JO L 335 du 17.12.2011, p. 1.
[11] Les termes «sans droit» permettent aux États membres de prévoir une défense pour les actes relatifs au matériel pornographique ayant, par exemple, un objectif médical, scientifique ou similaire. Ils permettent également de mener des activités en vertu de compétences légales nationales, telles que la détention légitime de pédopornographie par les autorités à des fins de poursuites pénales ou de prévention, de détection ou d'enquête pénale. En outre, ils n'excluent pas les défenses légales ou les principes similaires applicables qui exemptent une personne de sa responsabilité dans certaines circonstances, par exemple dans le contexte d'activités de signalement de tels cas via des lignes d'urgence, téléphoniques ou via l'internet. Considérant 25 de la directive 2011/93/UE.
[12] Article 5, paragraphes 3, 4 et 5, de la directive 2011/93/UE.
[13] Articles 11 et 25, paragraphe 1, de la directive 2011/93/UE.
[14] Article 25, paragraphe 2, de la directive 2011/93/UE.
[15] Avis du Contrôleur européen de la protection des données sur la proposition de directive du Parlement européen et du Conseil relative à l'exploitation et aux abus sexuels concernant des enfants et à la pédopornographie, abrogeant la décision-cadre 2004/68/JAI, 10 mai 2010, https://edps.europa.eu/sites/edp/files/publication/10-05-10_child_abuse_fr.pdf.
[16] Cour de justice de l'Union européenne, La Quadrature du Net e.a., affaires jointes C-511/18, C-512/18 et C-520/18, 6 octobre 2020, EU:C:2020:791, point 121.

[17] Considérant 15 de la directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen (refonte), JO L 321/36 du 17.12.2018.
[18] CEPD, Avis du Contrôleur européen de la protection des données sur la proposition de directive du Parlement européen et du Conseil relative à l'exploitation et aux abus sexuels concernant des enfants et à la pédopornographie, abrogeant la décision-cadre 2004/68/JAI, paragraphe 5.
[19] Cour de justice de l'Union européenne, La Quadrature du Net e.a., affaires jointes C-511/18, C-512/18 et C-520/18, 6 octobre 2020, EU:C:2020:791, point 128.
[20] Arrêt de la Cour de justice de l'Union européenne, La Quadrature du Net e.a., affaires jointes C-511/18, C-512/18 et C-520/18, 6 octobre 2020, EU:C:2020:791, point 126.
[21] Avis du Contrôleur européen de la protection des données sur la proposition de directive du Parlement européen et du Conseil relative à l'exploitation et aux abus sexuels concernant des enfants et à la pédopornographie, abrogeant la décision-cadre 2004/68/JAI, 10 mai 2010, paragraphe 7, disponible à l'adresse suivante: https://edps.europa.eu/sites/edp/files/publication/10-05-10_child_abuse_fr.pdf.
[22] Arrêt de la Cour de justice de l'Union européenne, La Quadrature du Net e.a., affaires jointes C-511/18, C-512/18 et C-520/18, 6 octobre 2020, EU:C:2020:791, point 132.
[23] Idem.
[24] Idem.
[25] 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), JO L 119 du 4.5.2016, p. 1.
[26] Exposé des motifs de la proposition de règlement provisoire, p. 2.
[27] Groupe de travail «article 29» sur la protection des données, «*avis 06/2014 sur la notion d'intérêt légitime du responsable du traitement au titre de l'article 7 de la directive 95/46/CE*», WP 217, 9 avril 2014, p. 29.
[28] Arrêt de la Cour de justice de l'Union européenne dans l'affaire Fashion ID, 29 juillet 2019, C-40/17, EU:C:2019:629, point 95.
[29] Voir également: Contrôleur européen de la protection des données, *Guide pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel*, 11 avril 2017, p. 9. La première étape de la liste des points à vérifier pour évaluer la nécessité de toute nouvelle mesure législative exige «***une description factuelle détaillée*** *de la mesure proposée et de sa finalité, préalablement à toute [autre] évaluation*».
[30] Lignes directrices du CEPD portant sur l'évaluation du caractère proportionné des mesures limitant les droits fondamentaux à la vie privée et à la protection des données à caractère personnel, 19 décembre 2019, p. 24, disponible à l'adresse suivante: https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_fr.pdf.
[31] Lignes directrices du CEPD portant sur l'évaluation du caractère proportionné des mesures limitant les droits fondamentaux à la vie privée et à la protection des données à caractère personnel, 19 décembre 2019, p. 22, disponible à l'adresse suivante: https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_fr.pdf.
[32] Bien que l'article 3 de la proposition limite les mesures proposées aux «*[…] technologies bien établies régulièrement utilisées à cette fin par les fournisseurs de services de communications interpersonnelles non fondés sur la numérotation avant l'entrée en vigueur du présent règlement […]*», la proposition ne décrit pas plus en détail quelles sont ces «*technologies bien établies*», ce qui pourrait apporter une sécurité juridique à la définition des mesures autorisées.
[33] Le considérant 11 de la proposition précise que «*[l]a référence à la technologie inclut, si nécessaire, tout examen humain directement lié à l'utilisation de la technologie et la supervisant*». Cette précision ne clarifie pas dans quelles circonstances un examen humain sera effectué, mais indique seulement qu'il n'est pas toujours effectué.
[34] Comparer, par exemple, avec l'article 7 (Conservation des contenus et des données connexes) de la proposition de règlement du Parlement européen et du Conseil relatif à la prévention de la diffusion de contenus à caractère terroriste en ligne, Bruxelles, 12.9.2018, COM(2018) 640 final.
[35] Bien que la proposition indique qu'en relation avec des données identifiées de manière fiable comme pédopornographiques, les données ne peuvent être conservées qu'aux fins de la création d'une signature numérique unique non reconvertible («hachage»), elle ne précise pas explicitement quelles entités seraient autorisées à conserver une copie des données originales identifiées comme pédopornographiques ni à quel moment le fournisseur serait tenu d'effacer les données identifiées de manière fiable comme pédopornographiques.
[36] Avis du Contrôleur européen de la protection des données sur la proposition de directive du Parlement européen et du Conseil relative à l'exploitation et aux abus sexuels concernant des enfants et à la pédopornographie,

abrogeant la décision-cadre 2004/68/JAI, 10 mai 2010, paragraphe 12, disponible à l'adresse suivante: https://edps.europa.eu/sites/edp/files/publication/10-05-10_child_abuse_fr.pdf.

[37] Avis du Contrôleur européen de la protection des données sur la proposition de directive du Parlement européen et du Conseil relative à l'exploitation et aux abus sexuels concernant des enfants et à la pédopornographie, abrogeant la décision-cadre 2004/68/JAI, paragraphe 13.

[38] Avis du Contrôleur européen de la protection des données sur la proposition de directive du Parlement européen et du Conseil relative à l'exploitation et aux abus sexuels concernant des enfants et à la pédopornographie, abrogeant la décision-cadre 2004/68/JAI, paragraphe 15.

[39] Proposition de règlement du Parlement européen et du Conseil relatif à la prévention de la diffusion de contenus à caractère terroriste en ligne, Bruxelles, 12.9.2018, COM(2018) 640 final.

[40] Voir Groupe de travail «article 29» sur la protection des données, Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «*susceptible d'engendrer un risque élevé*» aux fins du règlement (UE) 2016/679, WP 248 rév. 01, 4 octobre 2017.

[41] Traitement ayant reçu un avis positif de la part d'une autorité chargée de la protection des données à la suite d'une consultation.

[42] Ibid., p. 16.

[43] Proposition de règlement du Parlement européen et du Conseil concernant une dérogation temporaire à certaines dispositions de la directive 2002/58/CE du Parlement européen et du Conseil en ce qui concerne l'utilisation de technologies par des fournisseurs de services de communications interpersonnelles non fondés sur la numérotation pour le traitement de données à caractère personnel et d'autres données aux fins de la lutte contre les abus sexuels commis contre des enfants en ligne, mandat de négociation avec le Parlement européen, 23 octobre 2020, 2020/0259 (COD).

[44] Ibid., p. 21.