Avis conjoint 4/2022

de l'EDPB et du CEPD sur la proposition de règlement du Parlement européen et du Conseil établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfants

adopté le 28 juillet 2022

Translations proofread by EDPB Members.

This language version has not yet been proofread.

TABLE DES MATIÈRES

Synthèse

Le 11 mai 2022, la Commission européenne a publié une proposition de règlement du Parlement européen et du Conseil établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfants.

La proposition imposerait des obligations qualifiées aux fournisseurs de services d'hébergement, de services de communications interpersonnelles et d'autres services en matière de détection, de signalement, de retrait et de blocage du matériel en ligne connu et nouveau relatif à des abus sexuels sur enfants, ainsi que de la sollicitation d'enfants. La proposition prévoit également la création d'une nouvelle agence décentralisée de l'UE (ci-après le «centre de l'UE») et d'un réseau d'autorités nationales de coordination des questions liées aux abus sexuels sur enfants afin de permettre l'application du règlement proposé. Ainsi qu'il est reconnu dans l'exposé des motifs de la proposition, les mesures contenues dans la proposition affecteraient l'exercice des droits fondamentaux des utilisateurs des services concernés.

Les abus sexuels commis contre des enfants constituent un crime particulièrement grave et odieux et l'objectif visant à permettre une action efficace pour lutter contre ces abus constitue un objectif d'intérêt général reconnu par l'Union et vise à protéger les droits et libertés des victimes. Dans le même temps, l'EDPB et le CEPD rappellent que toute limitation des droits fondamentaux, telle que celles envisagées dans la proposition, doit être conforme aux exigences énoncées à l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne.

L'EDPB et le CEPD soulignent que la proposition soulève de graves préoccupations quant à la proportionnalité de l'ingérence envisagée et des limitations à la protection des droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel. À cet égard, l'EDPB et le CEPD soulignent que les garanties procédurales ne peuvent jamais remplacer complètement les garanties substantielles. Un système complexe d'escalade des mesures d'évaluation et d'atténuation des risques à une injonction de détection ne saurait remplacer la clarté requise des obligations de fond.

L'EDPB et le CEPD estiment que la proposition manque de clarté sur des éléments clés, tels que les notions de «risque important». En outre, les entités chargées d'appliquer ces garanties, en commençant par les opérateurs privés et en terminant par les autorités administratives et/ou judiciaires, jouissent d'une très large marge d'appréciation, ce qui entraîne une insécurité juridique quant à la manière d'équilibrer les droits en jeu dans chaque cas individuel. L'EDPB et le CEPD soulignent que le législateur doit, lorsqu'il autorise des ingérences particulièrement graves dans les droits fondamentaux, apporter une clarté juridique quant au moment et aux endroits où les ingérences sont autorisées. Tout en reconnaissant que la législation ne peut être trop prescriptive et doit laisser une certaine souplesse dans son application pratique, l'EDPB et le CEPD estiment que la proposition laisse trop de place à d'éventuels abus en raison de l'absence de règles matérielles claires.

En ce qui concerne la nécessité et la proportionnalité des mesures de détection envisagées, l'EDPB et le CEPD sont particulièrement préoccupés en ce qui concerne les mesures envisagées pour la détection de matériel inconnu relatif à des abus sexuels sur enfants (ci-après le «matériel») et la sollicitation d'enfants (pédopiégeage) dans les services de communications interpersonnelles. En raison de leur caractère intrusif, de leur nature probabiliste et des taux d'erreur associés à ces technologies, l'EDPB et le CEPD considèrent que l'ingérence créée par ces mesures va au-delà de ce qui est nécessaire et proportionné. En outre, les mesures permettant aux autorités publiques d'avoir accès de manière généralisée au contenu d'une communication afin de détecter la sollicitation d'enfants sont davantage susceptibles de porter atteinte au

contenu essentiel des droits garantis par les articles 7 et 8 de la Charte. Par conséquent, les dispositions pertinentes relatives au pédopiégeage devraient être supprimées de la proposition. En outre, la proposition n'exclut pas de son champ d'application l'examen des communications audio. L'EDPB et le CEPD estiment que l'examen des communications audio est particulièrement intrusif et, en tant que tel, doit rester en dehors du champ d'application des obligations de détection énoncées dans la proposition de règlement, tant en ce qui concerne les messages vocaux que les communications en direct.

L'EDPB et le CEPD expriment également des doutes quant à l'efficacité des mesures de blocage et estiment qu'il serait disproportionné d'exiger des fournisseurs de services internet qu'ils déchiffrent les communications en ligne afin de bloquer celles concernant le matériel.

En outre, l'EDPB et le CEPD soulignent que les technologies de chiffrement contribuent de manière fondamentale au respect de la vie privée et de la confidentialité des communications, à la liberté d'expression ainsi qu'à l'innovation et à la croissance de l'économie numérique, qui repose sur le niveau élevé de confiance que ces technologies offrent. Le considérant 26 de la proposition soumet le choix non seulement des technologies de détection, mais aussi des mesures techniques de protection de la confidentialité des communications, telles que le chiffrement, à une réserve selon laquelle ce choix technologique doit répondre aux exigences du règlement proposé, c'est-à-dire qu'il doit permettre la détection. Cela corrobore l'idée tirée de l'article 8, paragraphe 3, et de l'article 10, paragraphe 2, de la proposition selon laquelle un fournisseur ne peut refuser l'exécution d'une injonction de détection sur la base d'une impossibilité technique. L'EDPB et le CEPD estiment qu'il devrait y avoir un meilleur équilibre entre la nécessité sociétale de disposer de canaux de communication sûrs et privés et de lutter contre leurs abus. Il convient d'indiquer clairement dans la proposition qu'aucune disposition du règlement proposé ne devrait être interprétée comme interdisant ou affaiblissant le chiffrement.

Si l'EDPB et le CEPD se félicitent de la déclaration figurant dans la proposition selon laquelle elle ne porte pas atteinte aux pouvoirs et compétences des autorités chargées de la protection des données en vertu du RGPD, l'EDPB et le CEPD sont d'avis que la relation entre les tâches des autorités de coordination et celles des autorités chargées de la protection des données devrait néanmoins être mieux réglementée. À cet égard, l'EDPB et le CEPD apprécient le rôle que la proposition assigne à l'EDPB en exigeant sa participation à la mise en œuvre pratique de la proposition, en particulier la nécessité pour l'EDPB d'émettre un avis sur les technologies que le centre de l'UE mettrait à disposition pour exécuter les injonctions de détection. Il convient toutefois de préciser quel serait l'objectif de l'avis dans le cadre du processus et comment le centre de l'UE agirait après avoir reçu un avis de l'EDPB.

Enfin, l'EDPB et le CEPD notent que la proposition prévoit une coopération étroite entre le centre de l'UE et Europol, qui devraient se fournir «un accès le plus large possible aux systèmes d'information pertinents». Si l'EDPB et le CEPD soutiennent, en principe, la coopération entre les deux agences, étant donné que le centre de l'UE n'est pas une autorité répressive, l'EDPB et le CEPD formulent toutefois plusieurs recommandations en vue d'améliorer les dispositions pertinentes, notamment le fait que la transmission de données à caractère personnel entre le centre de l'UE et Europol n'a lieu qu'au cas par cas, à la suite d'une demande dûment évaluée, au moyen d'un outil de communication d'échange sécurisé, tel que le réseau SIENA.

Le comité européen de la protection des données et le Contrôleur européen de la protection des données

vu l'article 42, paragraphe 2, du règlement (UE) 2018/1725 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, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE (ci-après le «RPDUE»)[1],

vu l'accord EEE et, en particulier, son annexe XI et son protocole 37, tels que modifiés par la décision du comité mixte de l'EEE nº 154/2018 du 6 juillet 2018[2],

vu la demande d'avis conjoint du comité européen de la protection des données et du Contrôleur européen de la protection des données présentée par la Commission européenne le 12 mai 2022 sur la proposition de règlement du Parlement européen et du Conseil établissant des règles visant à prévenir et à combattre les abus sexuels commis contre des enfants[3],

ONT ADOPTÉ L'AVIS CONJOINT SUIVANT

1. CONTEXTE

1. Le 11 mai 2022, la Commission européenne (ci-après la «Commission») a publié une proposition de règlement du Parlement européen et du Conseil établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfants (ci-après la «proposition» ou le «règlement proposé»)[4].

2. La proposition a été présentée à la suite de l'adoption du règlement (UE) 2021/1232 relatif à une dérogation temporaire à certaines dispositions de la directive 2002/58/CE en ce qui concerne l'utilisation de technologies par les 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 (ci-après le «règlement provisoire»)[5]. Le règlement provisoire n'exige pas des fournisseurs de services concernés qu'ils mettent en place des mesures pour détecter le matériel inconnu relatif à des abus sexuels sur enfants (ci-après le «matériel») (par exemple, images, vidéos, etc.) ou la sollicitation d'enfants (également

[1] JO L 295 du 21.11.2018, p. 39.
[2] Dans le présent document, on entend par «États membres» les «États membres de l'EEE».
[3] Proposition de règlement du Parlement européen et du Conseil établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfants, COM(2022) 209 final.
[4] Ibidem.
[5] Règlement (UE) 2021/1232 du Parlement européen et du Conseil du 14 juillet 2021 relatif à une dérogation temporaire à certaines dispositions de la directive 2002/58/CE en ce qui concerne l'utilisation de technologies par les 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 (JO [2021] L 274/41).

appelée pédopiégeage) sur leurs services, mais autorise ces fournisseurs à le faire sur une base volontaire, conformément aux conditions énoncées dans ledit règlement[6].

3. La proposition se compose de deux éléments essentiels. Premièrement, elle impose des obligations qualifiées aux fournisseurs de services d'hébergement, de services de communications interpersonnelles et d'autres services en matière de détection, de signalement, de retrait et de blocage du matériel en ligne connu et nouveau relatif à des abus sexuels sur enfants, ainsi que de la sollicitation d'enfants. Deuxièmement, la proposition prévoit la création d'une nouvelle agence décentralisée de l'UE (ci-après le «centre de l'UE chargé de prévenir et de combattre les abus sexuels sur enfants» ou le «centre de l'UE») et d'un réseau d'autorités nationales de coordination pour les questions relatives aux abus sexuels commis contre des enfants, afin de permettre la mise en œuvre du règlement proposé[7].

4. Ainsi qu'il est reconnu dans l'exposé des motifs de la proposition, les mesures contenues dans la proposition affecteraient l'exercice des droits fondamentaux des utilisateurs des services concernés. Ces droits incluent notamment les droits fondamentaux au respect de la vie privée (y compris au respect de la confidentialité des communications, dans le cadre du droit plus large du respect de la vie privée et familiale), à la protection des données à caractère personnel et à la liberté d'expression et d'information[8].

5. En outre, les mesures proposées visent à s'appuyer sur la législation européenne existante en matière de protection des données et de respect de la vie privée, et, dans une certaine mesure, à la compléter. À cet égard, l'exposé des motifs indique ce qui suit:

> «La proposition s'appuie sur le règlement général sur la protection des données (RGPD). Dans la pratique, les fournisseurs invoquent souvent différents motifs de traitement prévus dans le RGPD pour procéder au traitement de données à caractère personnel nécessaire à la détection et au signalement volontaires des abus sexuels sur enfants en ligne. La proposition établit un système d'injonctions de détection ciblées et précise les conditions de détection, apportant ainsi davantage de sécurité juridique à ces activités. En ce qui concerne les activités de détection obligatoires impliquant le traitement de données à caractère personnel, la proposition, en particulier avec les injonctions de détection prises sur son fondement, établit ainsi le motif de traitement visé à l'article 6, paragraphe 1, point c), du RGPD, qui prévoit le traitement des données à caractère personnel nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis en vertu du droit de l'Union ou du droit national.
>
> La proposition s'applique notamment aux fournisseurs de services de communications électroniques interpersonnelles, qui sont soumis aux dispositions nationales mettant en œuvre la directive vie privée et communications électroniques, dont la révision proposée est actuellement en cours de négociation. Les mesures énoncées dans la proposition limitent, à certains égards, la portée des droits et obligations prévus par les dispositions pertinentes de ladite directive, en ce qui concerne des activités qui sont strictement nécessaires à l'exécution

[6] Voir également avis du CEPD 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 (10 novembre 2020).
[7] COM(2022) 209 final, p. 17.
[8] COM(2022) 209 final, p. 12.

des injonctions de détection. À cet égard, la proposition implique l'application, par analogie, de l'article 15, paragraphe 1, de ladite directive»[9].

6. Compte tenu de la gravité des ingérences envisagées dans les droits fondamentaux, la proposition revêt une importance particulière pour la protection des droits et libertés des personnes à l'égard du traitement des données à caractère personnel. Ainsi, le 12 mai 2022, la Commission a décidé de consulter le comité européen de la protection des données (ci-après l'«EDPB») et le Contrôleur européen de la protection des données (ci-après le «CEPD») conformément à l'article 42, paragraphe 2, du RPDUE.

2. PORTÉE DE L'AVIS

7. Le présent avis conjoint expose les points de vue communs de l'EDPB et du CEPD sur la proposition. Il se limite aux aspects de la proposition relatifs à la protection du respect de la vie privée et des données à caractère personnel. En particulier, l'avis conjoint souligne les domaines dans lesquels la proposition ne garantit pas une protection suffisante des droits fondamentaux au respect de la vie privée et à la protection des données ou exige un alignement plus poussé sur le cadre juridique de l'UE en matière de protection de la vie privée et des données à caractère personnel.

8. Comme expliqué plus en détail dans le présent avis commun, la proposition soulève de graves préoccupations quant à la nécessité et à la proportionnalité des ingérences envisagées et des limitations à la protection des droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel. Toutefois, l'objectif du présent avis conjoint n'est ni de fournir une liste exhaustive de toutes les questions relatives à la protection de la vie privée et des données soulevées par la proposition, ni de formuler des suggestions spécifiques pour améliorer la formulation de la proposition. Au lieu de cela, le présent avis conjoint formule des observations de haut niveau sur les principales questions soulevées par la proposition recensées par l'EDPB et le CEPD. Néanmoins, l'EDPB et le CEPD restent disponibles pour formuler d'autres observations et recommandations aux colégislateurs au cours du processus législatif sur la proposition.

3. OBSERVATIONS GÉNÉRALES SUR LES DROITS À LA CONFIDENTIALITÉ DES COMMUNICATIONS ET À LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

9. La confidentialité des communications est un élément essentiel du droit fondamental au respect de la vie privée et familiale, consacré à l'article 7 de la charte des droits fondamentaux de l'Union européenne (ci-après la «Charte»)[10]. En outre, l'article 8 de la Charte reconnaît le droit fondamental à la protection des données à caractère personnel. Le droit à la confidentialité des communications et le droit à la vie privée et familiale sont également garantis à l'article 8 de la Convention européenne

[9] COM(2022) 209 final, p. 4 et 5.
[10] Voir, par exemple; déclaration de l'EDPB sur la révision de la directive ePrivacy et son incidence sur la protection du respect de la vie privée et la confidentialité des communications électroniques (25 mai 2018).

des droits de l'homme (ci-après la «CEDH») et font partie des traditions constitutionnelles communes aux États membres[11].

10. L'EDPB et le CEPD rappellent que les droits consacrés aux articles 7 et 8 de la Charte ne sont pas des droits absolus, mais doivent être pris en considération par rapport à leur fonction dans la société[12]. Les abus commis contre des enfants sont des crimes particulièrement graves et abjects, et l'objectif visant à permettre une action efficace pour lutter contre ces abus constitue clairement un objectif d'intérêt général reconnu par l'Union et vise à protéger les droits et libertés des victimes. En ce qui concerne la lutte effective contre les infractions pénales dont sont victimes les mineurs et les autres personnes vulnérables, la Cour de justice de l'Union européenne (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, le domicile et les communications. De telles obligations sont également susceptibles de découler des articles 3 et 4 de la Charte, 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[13].

11. Dans le même temps, toute limitation des droits garantis par la Charte, telle que celles envisagées dans la proposition[14], doit être conforme aux exigences énoncées à l'article 52, paragraphe 1, de la Charte. Toute mesure portant atteinte au droit à la confidentialité des communications et au droit à la vie privée et familiale doit avant tout respecter le contenu essentiel des droits en cause[15]. Le contenu essentiel d'un droit est affecté si ce droit est vidé de son contenu de base et si le particulier ne peut l'exercer[16]. L'ingérence ne peut constituer, au regard du but poursuivi, une intervention démesurée et intolérable qui porterait atteinte à la substance même du droit ainsi garanti[17]. Cela signifie que même un droit fondamental qui n'est pas absolu par nature, tel que le droit à la confidentialité des communications et le droit à la protection des données à caractère personnel, comporte certains éléments essentiels qui peuvent ne pas être limités.

12. La CJUE a appliqué à plusieurs reprises le critère du «contenu essentiel d'un droit» dans le domaine du respect de la vie privée des communications électroniques. Dans l'arrêt *Tele2 Sverige et Watson*, la Cour a jugé qu'une réglementation qui ne permet pas la conservation du contenu d'une communication n'est pas de nature à porter atteinte au contenu essentiel des droits à la vie privée et à la protection des données à caractère personnel[18]. Dans l'arrêt *Schrems*, la Cour a jugé qu'une

---

[11] Presque toutes les constitutions européennes incluent un droit protégeant la confidentialité des communications. Voir, par exemple, article 15 de la Constitution de la République italienne; article 10 de la loi fondamentale pour la République fédérale d'Allemagne; article 22 de la Constitution belge; et article 13 de la Constitution du Royaume des Pays-Bas.

[12] Voir, notamment, arrêt de la CJUE, affaire C-311/18, *Facebook Ireland et Schrems*, point 172 et jurisprudence citée. Voir aussi le considérant 4 du RGPD.

[13] Affaires jointes C-511/18, C-512/18 et C-520/18, La Quadrature du Net e.a., points 126 à 128. Voir également avis 7/2020 du CEPD 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 (10 novembre 2020), point 12.

[14] Voir COM(2022) 209 final, p. 12 et 13.

[15] Article 52, paragraphe 1, de la Charte.

[16] Voir lignes directrices du CEPD sur l'évaluation de la proportionnalité des mesures limitant les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel (19 décembre 2019), p. 8, disponible à l'adresse: https://edps.europa.eu/sites/default/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf.

[17] Arrêt de la CJUE dans l'affaire C-393/19, *OM*, point 53.

[18] Arrêt de la CJUE dans les affaires jointes C-203/15 et C-698/15, *Tele2 Sverige et Watson*, point 101.

réglementation permettant aux autorités publiques d'accéder de manière généralisée au contenu de communications électroniques doit être considérée comme portant atteinte au contenu essentiel du droit fondamental au respect de la vie privée, tel que garanti par l'article 7 de la Charte[19]. Dans l'arrêt *Digital Rights Ireland et Seitlinger e.a.*, la Cour a jugé que, même si la conservation des données exigée par la directive 2006/24 constituait une ingérence particulièrement grave dans le droit fondamental au respect de la vie privée et les autres droits énoncés à l'article 7 de la Charte, elle n'était pas de nature à porter atteinte au contenu essentiel de ces droits, étant donné que cette directive ne permettait pas d'acquérir la connaissance du contenu des communications électroniques en tant que tel[20]. On peut déduire de cette jurisprudence que les mesures permettant aux autorités publiques d'avoir accès de manière généralisée au contenu d'une communication sont davantage susceptibles d'affecter le contenu essentiel des droits garantis par les articles 7 et 8 de la Charte. Ces considérations sont également pertinentes en ce qui concerne les mesures de détection matériel et de sollicitation d'enfants, telles que celles envisagées dans la proposition.

13. En outre, la CJUE a estimé que les mesures de sécurité des données jouent un rôle essentiel pour garantir que le contenu essentiel du droit fondamental à la protection des données à caractère personnel énoncé à l'article 8 de la Charte n'est pas affecté[21]. À l'ère numérique, des solutions techniques pour sécuriser et protéger la confidentialité des communications électroniques, y compris les mesures de chiffrement, sont essentielles pour garantir l'exercice de tous les droits fondamentaux[22]. Il convient d'en tenir dûment compte lors de l'évaluation des mesures de détection obligatoire de matériel ou de sollicitation d'enfants, en particulier si elles entraînent un affaiblissement ou une dégradation du chiffrement[23].

14. L'article 52, paragraphe 1, de la Charte prévoit également que toute limitation de l'exercice d'un droit fondamental garanti par la Charte doit être prévue par la loi. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si 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[24]. 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[25]. Cette législation doit 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[26]. Comme l'a précisé la CJUE, la nécessité de disposer de telles garanties est d'autant plus importante lorsque les données à caractère personnel

[19] Arrêt de la CJUE dans l'affaire C-362/14, *Schrems*, point 94.
[20] Arrêt de la CJUE dans les affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland et Seitlinger e.a.*, point 39.
[21] Ibidem, point 40.
[22] Voir Conseil des droits de l'homme, Résolution 47/16 sur la promotion, la protection et l'exercice des droits de l'homme sur Internet, document des Nations unies A/HRC/RES/47/16 (26 juillet 2021).
[23] Voir également le considérant 5 du règlement provisoire.
[24] Voir «Guide pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel» 11 avril 2019, disponible à l'adresse suivante: https://edps.europa.eu/sites/default/files/publication/17-06-01_necessity_toolkit_final_en.pdf.
[25] Arrêt de la CJUE dans les affaires jointes C-511/18, C-512/18 et C-520/18, *La Quadrature du Net e.a.*, point 132.
[26] Ibidem.

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[27].

15. La proposition limiterait l'exercice des droits et obligations prévus à l'article 5, paragraphes 1 et 3, et à l'article 6, paragraphe 1, de la directive 2002/58/CE («directive vie privée et communications électroniques»)[28] dans la mesure où cela est nécessaire à l'exécution des injonctions de détection émises conformément à la section 2 du chapitre 1er de la proposition. L'EDPB et le CEPD estiment qu'il est donc nécessaire d'évaluer la proposition non seulement à la lumière de la Charte et du RGPD, mais également à la lumière des articles 5 et 6 et de l'article 15, paragraphe 1, de la directive «vie privée et communications électroniques».

[27] Ibidem.

[28] 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 du respect de la vie privée dans le secteur des communications électroniques (directive «vie privée et communications électroniques») telle que modifiée par la directive 2006/24/CE et la directive 2009/136/CE.

4. OBSERVATIONS PARTICULIÈRES

4.1 Lien avec la législation existante

4.1.1 Lien avec le RGPD et la directive «vie privée et communications électroniques»

16. La proposition indique qu'elle est sans préjudice des règles découlant d'autres actes de l'Union, notamment du RGPD[29] et la directive «vie privée et communications électroniques». Contrairement au règlement provisoire, la proposition ne prévoit pas de dérogation temporaire explicite à l'exercice des droits et obligations énoncés à l'article 5, paragraphes 1 et 3, et à l'article 6, paragraphe 1, de la directive «vie privée et communications électroniques», mais une limitation de l'exercice de ces droits et obligations. En outre, il convient de noter que le règlement provisoire prévoit une dérogation exclusivement aux dispositions de l'article 5, paragraphe 1, et de l'article 6, paragraphe 1, et non à l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques».

17. La proposition renvoie en outre à l'article 15, paragraphe 1, de la directive «vie privée et communications électroniques», qui permet aux États membres d'adopter des mesures législatives visant à limiter la portée des droits et obligations prévus aux articles 5 et 6 de ladite directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée au sein d'une société démocratique, notamment pour prévenir et détecter des infractions pénales et mener des enquêtes et des poursuites en la matière. Selon la proposition, l'article 15, paragraphe 1, de la directive «vie privée et communications électroniques» s'applique par analogie lorsque la proposition limite l'exercice des droits et obligations prévus aux articles 5, paragraphes 1 et 3, et à l'article 6, paragraphe 1, de la directive «vie privée et communications électroniques».

18. L'EDPB et le CEPD rappellent que la CJUE a clairement indiqué que l'article 15, paragraphe 1, de la directive «vie privée et communications électroniques» doit être interprété de manière stricte, ce qui signifie que l'exception au principe de confidentialité des communications autorisée par l'article 15, paragraphe 1, doit rester une exception et ne pas devenir la règle[30]. Comme indiqué plus en détail dans le présent avis conjoint, l'EDPB et le CEPD considèrent que la proposition ne satisfait pas aux exigences de nécessité (stricte), d'efficacité et de proportionnalité. En outre, l'EDPB et le CEPD concluent que la proposition impliquerait que l'ingérence dans la confidentialité des communications peut en fait devenir la règle plutôt que de rester l'exception.

4.1.2 Lien avec le règlement (UE) 2021/1232 et incidence sur la détection volontaire des abus sexuels commis contre des enfants en ligne

19. Conformément à l'article 88 de la proposition, cette dernière abrogerait le règlement provisoire, qui prévoit une dérogation temporaire à certaines dispositions de la directive «vie privée et communications électroniques» afin de permettre l'utilisation volontaire de technologies pour la détection de matériel et de sollicitation d'enfants par les fournisseurs de services de communications interpersonnelles non fondés sur la numérotation. Par conséquent, à compter de la date d'application du règlement proposé, aucune dérogation à la directive «vie privée et communications électroniques»

[29] 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) (Texte présentant de l'intérêt pour l'EEE) (JO L 119 du 4.5.2016, p. 1).
[30] Arrêt du 21 décembre 2016, affaires jointes C-203/15 et C-698/15 *Tele2 Sverige AB et Watson*, point 89.

ne permettrait la détection volontaire des abus sexuels commis contre des enfants en ligne par ces fournisseurs.

20. Étant donné que les obligations de détection introduites par la proposition ne s'appliqueraient qu'aux destinataires d'injonctions de détection, il serait important de préciser dans le texte de la proposition de règlement que l'utilisation volontaire de technologies pour la détection de matériel et de la sollicitation d'enfants reste autorisée uniquement dans la mesure où elle est autorisée par la directive «vie privée et communications électroniques» et le RGPD. Cela signifierait, par exemple, que les fournisseurs de services de communications interpersonnelles non fondés sur la numérotation seraient empêchés d'utiliser ces technologies sur une base volontaire, sauf si les lois nationales transposant la directive «vie privée et communications électroniques» le permettent, conformément à l'article 15, paragraphe 1, de la directive «vie privée et communications électroniques» et à la Charte.

21. Plus généralement, la proposition de règlement gagnerait à être clarifiée en ce qui concerne le statut de la détection volontaire d'abus sexuels commis contre des enfants en ligne après la date d'application du règlement proposé, ainsi que la transition du régime de détection volontaire prévu dans le règlement provisoire aux obligations de détection énoncées dans la proposition de règlement. Par exemple, l'EDPB et le CEPD recommandent de préciser que la proposition de règlement ne prévoirait pas de base légale pour le traitement de données à caractère personnel à la seule fin de détecter les abus sexuels commis contre des enfants en ligne sur une base volontaire.

4.2 Base légale en vertu du RGPD

22. La proposition vise à établir une base légale, au sens du RGPD, pour le traitement des données à caractère personnel aux fins de la détection de matériel et de pédopiégeage. En conséquence, l'exposé des motifs note ce qui suit: «En ce qui concerne les activités de détection obligatoires impliquant le traitement de données à caractère personnel, la proposition, en particulier avec les injonctions de détection prises sur son fondement, établit ainsi le motif de traitement visé à l'article 6, paragraphe 1, point c), du RGPD, qui prévoit le traitement des données à caractère personnel nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis en vertu du droit de l'Union ou du droit national»[31].

23. L'EDPB et le CEPD se félicitent de la décision de la Commission d'éliminer l'insécurité juridique quant à la base juridique du traitement des données à caractère personnel, qui est apparue dans le cadre du règlement provisoire. L'EDPB et le CEPD sont également d'accord avec la conclusion de la Commission selon laquelle les conséquences du déploiement de mesures de détection sont trop lourdes et graves pour laisser aux fournisseurs de services la décision de mettre en œuvre de telles mesures[32]. Dans le même temps, l'EDPB et le CEPD font observer que toute base juridique obligeant les fournisseurs de services à porter atteinte aux droits fondamentaux à la protection des données et au respect de la vie privée ne sera valable que dans la mesure où elle respecte les conditions énoncées à l'article 52, paragraphe 1, de la Charte, comme analysé dans les sections suivantes.

4.3 Obligations en matière d'évaluation et d'atténuation des risques

24. En vertu du chapitre II, section 1, de la proposition, les fournisseurs de services d'hébergement et les fournisseurs de services de communications interpersonnelles sont tenus d'identifier, d'analyser et

[31] Ibidem, p. 4.
[32] Voir proposition, COM(2022) 209 final, p. 14.

d'évaluer, pour chacun des services qu'ils proposent, le risque d'utilisation du service à des fins d'abus sexuels commis contre des enfants en ligne, puis d'essayer de minimiser le risque identifié en appliquant «des mesures d'atténuation raisonnables, adaptées au risque identifié».

25. L'EDPB et le CEPD notent que, lors de la réalisation d'une évaluation des risques, le fournisseur devrait tenir compte en particulier des éléments énumérés à l'article 3, paragraphe 2, points a) à e), de la proposition, notamment: les interdictions et restrictions prévues dans les conditions générales du fournisseur; la manière dont les utilisateurs utilisent le service et son incidence sur ce risque; la manière dont le fournisseur a conçu et exploite le service, y compris le modèle économique, la gouvernance et les systèmes et processus pertinents, et son incidence sur ce risque. En ce qui concerne le risque de sollicitation d'enfants, les éléments proposés à prendre en considération sont les suivants: la mesure dans laquelle le service est utilisé ou est susceptible d'être utilisé par des enfants; les groupes d'âge et le risque de sollicitation par groupe d'âge; la disponibilité de fonctionnalités permettant une recherche des utilisateurs, de fonctionnalités permettant aux utilisateurs d'établir un contact direct avec d'autres utilisateurs, notamment au moyen de communications privées et de fonctionnalités permettant aux utilisateurs de partager des images ou des vidéos avec d'autres utilisateurs.

26. Si l'EDPB et le CEPD reconnaissent que ces critères semblent pertinents, l'EDPB et le CEPD craignent néanmoins que ces critères laissent une marge d'interprétation et d'appréciation assez large. Plusieurs critères sont décrits en termes très génériques (par exemple, «la manière dont les utilisateurs utilisent le service et son incidence sur ce risque») ou se rapportent à des fonctionnalités de base qui sont communes à de nombreux services en ligne (par exemple, la «possibilité pour les utilisateurs de partager des images ou des vidéos avec d'autres utilisateurs»). En tant que tels, les critères semblent susceptibles de faire l'objet d'une appréciation subjective (et non objective).

27. De l'avis de l'EDPB et du CEPD, il en va de même pour les mesures d'atténuation des risques à prendre en vertu de l'article 4 de la proposition. Des mesures telles que l'adaptation, au moyen de mesures techniques et opérationnelles appropriées et de la dotation en personnel, des systèmes de modération ou de recommandation de contenu du fournisseur semblent pertinentes pour réduire le risque identifié. Toutefois, s'ils sont appliqués dans le cadre d'un processus complexe d'évaluation des risques et combinés à des termes abstraits et vagues pour décrire le niveau de risque acceptable (par exemple, «dans une mesure appréciable»), ces critères ne répondent pas aux critères de sécurité juridique et de prévisibilité nécessaires pour justifier une ingérence dans la confidentialité des communications entre particuliers qui constitue une ingérence manifeste dans les droits fondamentaux au respect de la vie privée et à la liberté d'expression.

28. Bien que les fournisseurs ne soient pas autorisés à porter atteinte à la confidentialité des communications dans le cadre de leurs stratégies d'évaluation et d'atténuation des risques avant de recevoir une injonction de détection, il existe un lien direct entre les obligations en matière d'évaluation et d'atténuation des risques et les obligations de détection qui en découlent. L'article 7, paragraphe 4, de la proposition subordonne l'émission d'une injonction de détection à l'existence de preuves d'un risque important que le service concerné puisse être utilisé à des fins d'abus sexuels commis contre des enfants en ligne. Avant l'émission d'une injonction de détection, il convient de suivre un processus complexe impliquant les fournisseurs, l'autorité de coordination et l'autorité judiciaire ou toute autre autorité administrative indépendante responsable de l'émission de l'injonction. Premièrement, les fournisseurs doivent évaluer le risque d'utilisation de leurs services à des fins d'abus sexuels commis contre des enfants en ligne (article 3 de la proposition) et évaluer d'éventuelles mesures d'atténuation des risques (article 4 de la proposition) pour réduire ce risque. Les résultats de cet exercice doivent ensuite être communiqués à l'autorité de coordination

compétente (article 5 de la proposition). Si l'évaluation des risques montre qu'un risque important subsiste malgré les efforts déployés pour l'atténuer, l'autorité de coordination entend le fournisseur sur un projet de demande d'émission d'une injonction de détection et donne au fournisseur la possibilité de formuler des observations. Le fournisseur est également tenu de présenter un plan de mise en œuvre, y compris un avis de l'autorité compétente en matière de protection des données en cas de détection de pédopiégeage. Si l'autorité de coordination poursuit l'affaire, une injonction de détection est demandée et finalement émise par une juridiction ou une autre autorité administrative indépendante. Par conséquent, l'évaluation initiale des risques et les mesures choisies pour réduire le risque identifié constituent une base déterminante pour l'évaluation, par l'autorité de coordination, ainsi que par l'autorité judiciaire ou administrative compétente, de la nécessité d'une injonction de détection.

29. L'EDPB et le CEPD prennent note des étapes complexes conduisant à l'émission d'une injonction de détection, qui comprennent une évaluation initiale des risques par le fournisseur et la proposition du fournisseur de mesures d'atténuation des risques, ainsi que la poursuite de l'interaction entre le fournisseur et l'autorité de coordination compétente. L'EDPB et le CEPD estiment qu'il existe une possibilité importante pour le fournisseur d'influencer le résultat du processus. À cet égard, l'EDPB et le CEPD font observer que le considérant 17 de la proposition dispose que les fournisseurs devraient être en mesure d'indiquer, dans le cadre du signalement des risques, «qu'ils sont disposés et préparés» à se voir ultérieurement adresser une injonction de détection. Par conséquent, on ne saurait supposer que chaque fournisseur cherchera à éviter l'émission d'une injonction de détection afin de préserver la confidentialité des communications de ses utilisateurs en appliquant les mesures d'atténuation les plus efficaces, mais les moins intrusives, en particulier lorsque ces mesures d'atténuation portent atteinte à la liberté d'entreprise du fournisseur conformément à l'article 16 de la Charte.

30. Le CEPD et l'EDPB tiennent à souligner que les garanties procédurales ne peuvent jamais remplacer complètement les garanties substantielles. Par conséquent, le processus complexe conduisant à l'émission éventuelle d'une injonction de détection décrit ci-dessus devrait s'accompagner d'obligations substantielles claires. L'EDPB et le CEPD estiment que la proposition manque de clarté sur plusieurs éléments clés (par exemple, les notions de «risque important», de «mesure appréciable», etc.), auxquels il ne peut être remédié par la présence de plusieurs niveaux de garanties procédurales. Cela est d'autant plus pertinent que les entités chargées d'appliquer ces garanties (par exemple, les fournisseurs, les autorités judiciaires, etc.) disposent d'une large marge d'appréciation quant à la manière d'équilibrer les droits en jeu dans chaque cas individuel. Compte tenu des importantes ingérences dans les droits fondamentaux qui découleraient de l'adoption de la proposition, le législateur devrait veiller à ce que la proposition clarifie le moment et le lieu où de telles ingérences sont autorisées. Tout en reconnaissant que les mesures législatives ne peuvent pas être trop prescriptives et doivent laisser une certaine souplesse dans leur application pratique, l'EDPB et le CEPD estiment que le texte actuel de la proposition laisse trop de place à d'éventuels abus en raison de l'absence de règles matérielles claires.

31. Compte tenu de l'incidence potentiellement significative sur un très grand nombre de personnes concernées (c'est-à-dire potentiellement tous les utilisateurs de services de communications interpersonnelles), l'EDPB et le CEPD soulignent la nécessité d'un niveau élevé de sécurité juridique, de clarté et de prévisibilité de la législation afin de garantir que les mesures proposées sont réellement efficaces pour atteindre l'objectif qu'elles poursuivent et, dans le même temps, qu'elles portent le moins atteinte aux droits fondamentaux en jeu.

4.4 Conditions d'émission des injonctions de détection

32. L'article 7 de la proposition prévoit que l'autorité de coordination du lieu d'établissement aura le pouvoir de demander à l'autorité judiciaire compétente de l'État membre qui l'a désignée ou à une autre autorité administrative indépendante de cet État membre d'émettre une injonction de détection enjoignant à un fournisseur de services d'hébergement ou à un fournisseur de services de communications interpersonnelles de prendre les mesures prévues à l'article 10 pour détecter les abus sexuels sur enfants en ligne sur un service particulier.

33. L'EDPB et le CEPD tiennent dûment compte des éléments suivants à remplir avant l'émission d'une décision de détection:

    a. il existe des preuves de l'existence d'un risque important que le service soit utilisé à des fins d'abus sexuels commis contre des enfants en ligne, au sens de l'article 7, paragraphes 5, 6 ou 7, selon le cas;

    b. les raisons de l'émission de l'injonction de détection l'emportent sur les conséquences négatives pour les droits et les intérêts légitimes de toutes les parties concernées, eu égard notamment à la nécessité d'assurer un juste équilibre entre les droits fondamentaux de ces parties.

34. La signification du risque important est précisée à l'article 7, paragraphes 5 et suivants, en fonction du type d'injonction de détection considéré. Un risque important est assumé dans le cas d'injonctions de détection concernant la détection de matériel connu si:

    a. il est probable, en dépit des mesures d'atténuation que le fournisseur aurait pu prendre ou qu'il prendra, que le service est utilisé, dans une mesure appréciable, pour la diffusion de matériel connu relatif à des abus sexuels sur enfants; et

    b. il existe des preuves que le service, ou un service comparable si le service n'a pas encore été proposé dans l'Union à la date de la demande d'émission de l'injonction de détection, a été utilisé au cours des 12 derniers mois et dans une mesure appréciable pour la diffusion de matériel connu relatif à des abus sexuels sur enfants.

35. Pour émettre une injonction de détection pour du matériel inconnu, la probabilité et les éléments de preuve factuels doivent faire référence à du matériel inconnu, et une injonction de détection préalable pour du matériel connu doit avoir été émise et avoir donné lieu à un nombre important de signalements concernant du matériel par le fournisseur (article 7, paragraphe 6, de la proposition). Dans le cas d'une injonction de détection concernant le pédopiégeage, le risque important est réputé exister lorsque le fournisseur est considéré comme un fournisseur de services de communications interpersonnelles, qu'il est probable que le service est utilisé dans une mesure appréciable pour la sollicitation d'enfants et qu'il existe des preuves que le service a été utilisé dans une mesure appréciable pour la sollicitation d'enfants (article 7, paragraphe 7, de la proposition).

36. L'EDPB et le CEPD font observer que, même avec les spécifications de l'article 7, paragraphes 5 à 7, de la proposition, les conditions d'émission d'une injonction de détection sont dominées par des termes juridiques vagues, tels que «ampleur appréciable», «nombre significatif», et sont en partie répétitives, étant donné que les preuves d'un abus antérieur contribueront souvent à établir la probabilité d'un abus futur.

37. La proposition prévoit un système dans lequel, pour décider si une injonction de détection est nécessaire, une décision prévisionnelle concernant l'utilisation future d'un service à des fins d'abus

sexuels commis contre des enfants en ligne doit être prise. Il est donc compréhensible que les éléments énoncés à l'article 7 aient un caractère pronostique. Toutefois, le recours à des notions vagues dans la proposition rend difficile, pour les fournisseurs, ainsi que pour l'autorité judiciaire ou autre autorité administrative indépendante compétente, d'appliquer les exigences légales introduites par la proposition de manière prévisible et non arbitraire. L'EDPB et le CEPD craignent que ces notions larges et vagues n'entraînent un manque de sécurité juridique et conduisent également à des divergences considérables dans la mise en œuvre concrète de la proposition dans l'Union, en fonction des interprétations qui seront données à des notions telles que «probabilité» et «mesure appréciable» par des autorités judiciaires ou d'autres autorités administratives indépendantes dans les États membres. Un tel résultat ne serait pas acceptable compte tenu du fait que les dispositions relatives aux injonctions de détection pour les fournisseurs de services de communications interpersonnelles constitueront des «limitations» au principe de confidentialité des communications énoncé à l'article 5 de la directive «vie privée et communications électroniques» et que leur clarté et leur prévisibilité sont donc de la plus haute importance pour garantir l'application uniforme de ces limitations dans l'ensemble de l'Union.

4.5 Analyse de la nécessité et de la proportionnalité des mesures envisagées[33]

38. Comme indiqué ci-dessus, trois types d'injonctions de détection peuvent être émis: les injonctions de détection concernant la diffusion de matériel connu relatif à des abus sexuels sur enfants (article 7, paragraphe 5, de la proposition), les injonctions de détection concernant la de matériel nouveau relatif à des abus sexuels sur enfants (article 7, paragraphe 6, de la proposition) et les injonctions de détection concernant la sollicitation d'enfants (article 7, paragraphe 7, de la proposition). Chaque injonction de détection nécessiterait normalement une technologie différente pour sa mise en œuvre pratique. Par conséquent, elles ont un niveau d'intrusion différent et, partant, une incidence différente sur les droits au respect de la vie privée et à la protection des données à caractère personnel.

39. Les technologies permettant de détecter le matériel connu relatif à des abus sexuels sur enfants sont généralement des technologies de mise en correspondance en ce sens qu'elles s'appuient sur une base de données existante de matériel connu, auquel elles peuvent comparer des images (y compris des images fixes tirées de vidéos). Pour permettre la mise en correspondance, les images que le fournisseur traite ainsi que les images figurant dans la base de données doivent avoir été numérisées, généralement en les convertissant en valeurs de hachage. Ce type de technologie de hachage présente un taux de faux positifs estimé à 1 sur 50 milliards (soit un taux de faux positifs de 0,000000002 %).[34]

40. Pour la détection de nouveau matériel, un autre type de technologie est généralement utilisé, y compris les classificateurs et l'intelligence artificielle (IA)[35]. Toutefois, leurs taux d'erreur sont généralement nettement plus élevés. Par exemple, le rapport d'analyse d'impact indique qu'il existe des technologies de détection de nouveau matériel dont le taux de précision peut être fixé à 99,9 %

[33] Voir également le guide rapide du CEPD sur la nécessité et la proportionnalité [The EDPS quick guide to necessity and proportionality], disponible à l'adresse suivante: https://edps.europa.eu/sites/default/files/publication/20-01-28_edps_quickguide_en.pdf.
[34] Voir Commission européenne, document de travail des services de la Commission, rapport d'analyse d'impact accompagnant le document Proposition de règlement du Parlement européen et du Conseil établissant des règles visant à prévenir et à combattre les abus sexuels commis contre des enfants, SWD(2022) 209 final (ci-après le «rapport d'analyse d'impact» ou «SWD(2022) 209 final»), p. 281, note de bas de page 511.
[35] Rapport d'analyse d'impact, p. 281.

(c'est-à-dire 0,1 % de faux positifs), mais avec ce taux de précision, ils ne sont en mesure d'identifier que 80 % du total du matériel dans l'ensemble de données pertinent[36].

41. En ce qui concerne la détection de sollicitation d'enfants dans les communications textuelles, le rapport d'analyse d'impact explique qu'elle repose généralement sur la détection de modèles. Le rapport d'analyse d'impact fait constater que certaines des technologies existantes de détection concernant le pédopiégeage présentent un «taux de précision» de 88 %[37]. Selon la Commission, cela signifie que «sur 100 conversations identifiées comme constituant potentiellement une sollicitation criminelle d'enfants, 12 peuvent être écartées lors du contrôle [selon la proposition, par le centre de l'UE] et ne seront pas signalées aux autorités répressives»[38]. Toutefois, même si, contrairement au règlement provisoire, la proposition s'appliquait également aux communications audio, le rapport d'analyse d'impact ne précise pas les solutions technologiques qui pourraient être utilisées pour détecter le pédopiégeage dans un tel contexte.

4.5.1 Efficacité de la détection

42. Le «principe de nécessité» suppose le besoin de procéder à une évaluation factuelle combinée de l'efficacité des mesures envisagées pour atteindre l'objectif poursuivi et de déterminer si cette mesure est moins intrusive que d'autres moyens de réaliser le même objectif[39]. L'efficacité des mesures existantes par rapport à la proposition de mesure constitue également un autre élément à prendre en considération dans l'évaluation de la proportionnalité[40]. Si des mesures poursuivant un objectif similaire ou identique existent déjà, leur efficacité doit être évaluée dans le cadre de l'examen de la proportionnalité. Faute d'avoir réalisé cette évaluation, il sera considéré que l'examen du critère de proportionnalité pour une nouvelle mesure n'a pas été dûment mené.

43. La détection de matériel ou de pédopiégeage par les fournisseurs de services d'hébergement et les fournisseurs de services de communications interpersonnelles est susceptible de contribuer à l'objectif global de prévention et de lutte contre les abus sexuels commis contre des enfants et la diffusion en ligne de matériel relatif à des abus sexuels sur enfants. Dans le même temps, la nécessité d'évaluer l'efficacité des mesures prévues dans la proposition soulève trois questions clés:

- Les mesures de détection des abus sexuels commis contre des enfants en ligne peuvent-elles être facilement contournées?
- Quel sera l'effet des activités de détection sur les mesures prises par les services répressifs?[41]

---

[36] Ibidem, p. 282.
[37] Ibidem, p. 283.
[38] Proposition, COM(2022) 209 final, p. 14, note de bas de page 32.
[39] CEPD, 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. 5; CEPD, 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. 8.
[40] CEPD, 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. 11.
[41] Selon le rapport d'analyse d'impact, annexe II, p. 132, 85,71 % des personnes interrogées dans le cadre de l'enquête sur les services répressifs ont fait part de leurs préoccupations concernant l'augmentation du matériel relatif à des abus sexuels sur enfants au cours de la dernière décennie et le manque de ressources (humaines, techniques).

- Comment la proposition réduit-elle l'insécurité juridique?

44. Il n'appartient pas à l'EDPB et au CEPD de répondre à ces questions en détail. Toutefois, l'EDPB et le CEPD notent que ni le rapport d'analyse d'impact ni la proposition ne répondent pleinement à ces questions.

45. En ce qui concerne la possibilité de contourner la détection de matériel, il convient de noter qu'à l'heure actuelle, il ne semble pas y avoir de solution technologique pour détecter le matériel partagé sous une forme chiffrée. Par conséquent, toute activité de détection – même l'examen côté client destiné à contourner le chiffrement de bout en bout proposé par le fournisseur [42] – peut être facilement contournée en chiffrant le contenu à l'aide d'une application distincte avant de l'envoyer ou de le télécharger. Ainsi, les mesures de détection envisagées dans la proposition pourraient avoir un impact moindre sur la diffusion de matériel sur l'internet que ce que l'on pourrait espérer.

46. En outre, la Commission s'attend à une augmentation du nombre de signalements d'abus sexuels commis contre des enfants auprès des services répressifs grâce à l'adoption des obligations de détection introduites par la proposition[43]. Toutefois, ni la proposition ni le rapport d'analyse d'impact n'expliquent comment cela permettra de remédier aux lacunes de la situation actuelle. Compte tenu des ressources limitées des services répressifs, il semble nécessaire de mieux comprendre si l'augmentation du nombre de signalements aurait une incidence significative sur les activités répressives contre les abus sexuels commis contre des enfants. En tout état de cause, l'EDPB et le CEPD souhaitent souligner que ces signalements devraient être évalués en temps utile afin de garantir qu'une décision sur la pertinence pénale des éléments signalés soit prise le plus tôt possible et de limiter autant que possible la conservation des données dénuées de pertinence.

4.5.2 Pas de mesure moins intrusive

47. En supposant que les effets positifs de la détection de matériel et de pédopiégeage envisagés par la Commission puissent se concrétiser, la détection doit être la mesure la moins intrusive de mesures tout aussi efficaces. L'article 4 de la proposition prévoit que, dans un premier temps, les fournisseurs devraient envisager l'adoption de mesures d'atténuation visant à réduire le risque d'utilisation de leur service à des fins d'abus sexuels commis contre des enfants en ligne en dessous du seuil justifiant l'émission d'une injonction de détection. S'il existe des mesures d'atténuation susceptibles d'entraîner une réduction substantielle du niveau de pédopiégeage ou de matériel échangé au sein du service concerné, ces mesures constitueraient souvent des mesures moins intrusives qu'une injonction de détection[44]. Par conséquent, si le fournisseur concerné n'adopte pas ces mesures sur une base volontaire, il devrait être possible pour l'autorité administrative ou judiciaire indépendante compétente de rendre obligatoire et exécutoire la mise en œuvre de mesures d'atténuation au lieu d'émettre une injonction de détection. De l'avis de l'EDPB et du CEPD, le fait que l'article 5, paragraphe 4, de la proposition autorise l'autorité de coordination à «exiger» introduise, réexamine, supprime ou étende les mesures d'atténuation n'est pas suffisant, étant donné qu'une telle exigence ne serait pas exécutoire de manière indépendante; le non-respect ne serait «sanctionné» qu'en ordonnant une injonction de détection.

---

[42] Voir également section 4.10 ci-après.
[43] Voir, entre autres, le rapport d'analyse d'impact, annexe 3, SWD(2022) 209 final, p. 176.
[44] Par exemple, des mesures telles que le blocage du côté du client de la transmission de matériel en empêchant le téléchargement et l'envoi du contenu des communications électroniques pourraient être envisagées, car elles pourraient contribuer, dans certains contextes, à empêcher la circulation de matériel connu.

48. Par conséquent, l'EDPB et le CEPD estiment que l'autorité de coordination ou l'autorité administrative ou judiciaire indépendante compétente devrait être explicitement habilitée à imposer des mesures d'atténuation moins intrusives avant ou au lieu d'émettre une injonction de détection.

4.5.3 Proportionnalité au sens strict

49. Pour qu'une mesure respecte le principe de proportionnalité inscrit à l'article 52, paragraphe 1, de la charte, les avantages résultant de la mesure ne doivent pas être contrebalancés par les inconvénients causés par la mesure au regard de l'exercice des droits fondamentaux. En conséquence, le principe de proportionnalité «limite les autorités dans l'exercice de leurs pouvoirs en exigeant d'elles qu'elles parviennent à un équilibre entre les moyens utilisés et l'objectif visé (ou le résultat atteint)»[45].

50. 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: [46]

- 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);
- l'**étendue de la 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 elle affecte également **d'autres droits fondamentaux** (par exemple, le droit à la liberté d'expression, comme dans les affaires *Digital Rights Ireland et Seitlinger e.a.* et *Tele2 Sverige et Watson*)[47].

[45] Voir affaire C-343/09, *Afton Chemical*, point 45; affaires jointes C-92/09 et C-93/09, *Volker und Markus Schecke et Hartmut Eifert*, point 74; affaires C-581/10 et C-629/10, *Nelson e.a.*, point 71; affaire C-283/11, *Sky Österreich*, point 50; et affaire C-101/12, *Schaible*, point 29. Voir également CEPD, Guide pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel (11 avril 2017).

[46] 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

[47] Voir également CEPD, 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 (10 novembre 2020), p. 9 et suivantes.

51. 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[48].

52. Dans les trois types d'injonctions de détection (détection de matériel connu, de nouveau matériel et de pédopiégeage), les technologies actuellement disponibles reposent sur le traitement automatisé des données relatives au contenu de tous les utilisateurs concernés. Les technologies utilisées pour analyser le contenu sont souvent complexes, impliquant généralement l'utilisation de l'IA. En conséquence, le comportement de cette technologie peut ne pas être pleinement compréhensible pour l'utilisateur du service. En outre, on sait que les technologies actuellement disponibles, en particulier celles permettant de détecter du nouveau matériel ou du pédopiégeage, présentent des taux d'erreur relativement élevés[49]. En outre, il existe un risque d'être signalé au centre de l'UE conformément à l'article 12, paragraphe 1, et à l'article 48, paragraphe 1, de la proposition, sur la base de la détection de matériel «potentiel».

53. En outre, les conditions générales d'émission d'une injonction de détection en vertu de la proposition, c'est-à-dire appliquées à l'ensemble d'un service et pas seulement aux communications sélectionnées[50], la durée maximale de 24 mois pour le matériel connu ou nouveau et jusqu'à 12 mois pour le pédopiégeage[51], etc., peuvent donner lieu à une portée très large de l'injonction dans la pratique. En conséquence, la surveillance serait en réalité de nature générale et indifférenciée et ne serait pas ciblée dans la pratique.

54. À la lumière de ce qui précède, l'EDPB et le CEPD sont également préoccupés par les éventuels effets paralysants pour l'exercice de la liberté d'expression. L'EDPB et le CEPD rappellent que cet effet paralysant est jugé d'autant plus probable que la clarté de la législation est faible.

55. En l'absence de la spécificité, de la précision et de la clarté requises pour satisfaire à l'exigence de sécurité juridique[52], et compte tenu de sa large portée, à savoir l'ensemble des fournisseurs de services pertinents de la société de l'information proposant de tels services dans l'Union[53], la proposition ne garantit pas que seule une approche ciblée de la détection de matériel et de pédopiégeage aura effectivement lieu. Dès lors, l'EDPB et le CEPD estiment que, dans la pratique, la proposition pourrait servir de base à l'examen de facto généralisé et indifférencié du contenu de pratiquement tous les types de communications électroniques de tous les utilisateurs dans l'UE/EEE. En conséquence, la législation peut amener les citoyens à s'abstenir de partager des contenus licites par crainte qu'ils puissent être ciblés sur la base de leur action.

56. Cela étant dit, l'EDPB et le CEPD reconnaissent 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, l'EDPB et le CEPD font 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

[48] 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
[49] Voir détails ci-dessus, section 4.5, et ci-dessous, sous-section 4.8.2.
[50] Voir article 7, paragraphe 1, de la proposition.
[51] Voir article 7, paragraphe 9, de la proposition.
[52] Voir arrêt de la CJUE dans l'affaire C-197/96, *Commission des Communautés européennes/République française*, point 15.
[53] Voir article premier, paragraphe 2, de la proposition.

cas de matériel précédemment confirmés en vue de détecter du matériel. En outre, il convient d'établir une distinction entre la détection de «matériel connu» et celle de «nouveau matériel». En outre, l'incidence devrait être davantage différenciée entre les mesures destinées aux fournisseurs de services d'hébergement et celles imposées aux fournisseurs de services de communications interpersonnelles.

4.5.4 Détection de matériel connu relatif à des abus sexuels sur enfants

57. Si, selon le considérant 4, la proposition devrait être formulée «de manière technologiquement neutre», tant l'efficacité des mesures de détection proposées que leur incidence sur les personnes dépendront fortement du choix de la technologie appliquée et des indicateurs sélectionnés. Ce fait est reconnu par la Commission dans son rapport d'analyse d'impact, annexe 8[54], et confirmé par d'autres études, telles que l'analyse d'impact ciblée du service de recherche du Parlement européen sur la proposition de la Commission relative à la dérogation temporaire à la directive «vie privée et communications électroniques» aux fins de la lutte contre les abus sexuels commis contre des enfants en ligne à partir de février 2021[55].

58. L'article 10 de la proposition fixe un certain nombre d'exigences pour les technologies à utiliser à des fins de détection, notamment en ce qui concerne leur efficacité, leur fiabilité et leur nature la moins intrusive en ce qui concerne l'incidence sur les droits des utilisateurs à la vie privée et familiale, y compris la confidentialité des communications, et à la protection des données à caractère personnel.

59. Dans ce contexte, l'EDPB et le CEPD notent qu'à l'heure actuelle, les seules technologies qui semblent pouvoir satisfaire de manière générale à ces normes sont celles utilisées pour détecter du matériel connu, c'est-à-dire les technologies de mise en correspondance reposant sur une base de données de hachages comme référence.

4.5.5 Détection de matériel inconnu relatif à des abus sexuels sur enfants

60. L'évaluation des mesures visant à détecter du matériel (nouveau) précédemment inconnu aboutit à des conclusions différentes en ce qui concerne leur efficacité, leur fiabilité et leur limitation de l'incidence sur les droits fondamentaux au respect de la vie privée et à la protection des données.

61. Premièrement, comme expliqué dans le rapport d'analyse d'impact relatif à la proposition, les technologies actuellement utilisées pour détecter le matériel précédemment inconnu comprennent les classificateurs et l'IA. Un classificateur est un algorithme qui trie les données en classes étiquetées, ou catégories d'informations, grâce à la reconnaissance de modèles[56]. Ces technologies ont donc des résultats et des effets différents en matière de précision, d'efficacité et de niveau d'intrusion. Dans le même temps, elles sont également plus exposés aux erreurs.

62. Les techniques utilisées pour détecter le matériel précédemment inconnu sont similaires à celles utilisées pour détecter la sollicitation d'enfants, car ces deux types de techniques reposent non pas

[54] Voir les informations sur les taux de faux positifs dans le rapport d'analyse d'impact, annexe 8, p. 279 et suivantes.
[55] Voir la proposition de la Commission relative à la dérogation temporaire à la directive «vie privée et communications électroniques» aux fins de la lutte contre les abus sexuels commis contre des enfants en ligne: analyse d'impact ciblée de substitution (service de recherche du Parlement européen, février 2021), p. 14 et suivantes.
[56] Rapport d'analyse d'impact, annexe 8, p. 281

sur de simples technologies de mise en correspondance, mais sur des modèles prédictifs utilisant des technologies d'IA. L'EDPB et le CEPD estiment qu'un niveau élevé de prudence devrait être de mise lors de la détection de matériel précédemment inconnu, étant donné qu'une erreur du système aurait de graves conséquences pour les personnes concernées, qui seraient automatiquement signalées comme ayant éventuellement commis une infraction très grave et dont les données à caractère personnel et les détails de leurs communications seraient signalés.

63. Deuxièmement, les indicateurs de performance trouvés dans la littérature, dont certains sont mis en évidence dans le rapport d'analyse d'impact qui accompagnait la proposition[57], ne fournissent que très peu d'informations sur les conditions qui ont été utilisées pour leur calcul et sur leur adéquation avec les conditions réelles, ce qui signifie que leurs performances réelles pourraient être nettement inférieures à ce qui est attendu, ce qui se traduirait par une précision moindre et un pourcentage plus élevé de «faux positifs».

64. Troisièmement, les indicateurs de performance devraient être pris en considération dans le contexte spécifique de l'utilisation des outils de détection pertinents et fournir un aperçu exhaustif du comportement des outils de détection. Lors de l'utilisation d'algorithmes d'intelligence artificielle sur des images ou des textes, il est bien documenté que des biais et des discriminations peuvent survenir en raison du manque de représentativité de certains groupes de population dans les données utilisées pour entraîner l'algorithme. Ces biais devraient être identifiés, mesurés et ramenés à un niveau acceptable afin que les systèmes de détection soient réellement bénéfiques pour la société dans son ensemble.

65. Bien qu'une étude des technologies utilisées pour la détection ait été réalisée, l'EDPB et le CEPD estiment qu'une analyse plus approfondie est nécessaire pour évaluer la fiabilité des outils existants[58]. Cette analyse devrait s'appuyer sur des indicateurs de performance exhaustifs et évaluer l'incidence des erreurs potentielles dans les conditions réelles pour toutes les personnes concernées par la proposition.

66. Comme indiqué ci-dessus, l'EDPB et le CEPD ont de sérieux doutes quant à la mesure dans laquelle les garanties procédurales prévues à l'article 7, paragraphe 6, de la proposition sont suffisantes pour compenser ces risques. En outre, comme indiqué précédemment, ils notent que la proposition utilise des termes plutôt abstraits et vagues pour décrire le niveau de risque acceptable (par exemple, «mesure appréciable»).

67. L'EDPB et le CEPD craignent que ces notions larges et vagues n'entraînent un manque de sécurité juridique et provoquent également de fortes divergences dans la mise en œuvre concrète de la proposition dans l'Union, en fonction des interprétations qui seront données à des notions telles que «probabilité» et «mesure appréciable» par des autorités judiciaires ou d'autres autorités administratives indépendantes dans les États membres. Cela est également préoccupant compte tenu du fait que les dispositions relatives aux injonctions de détection constitueront des «limitations» au principe de confidentialité énoncé à l'article 5 de la directive «vie privée et communications électroniques». Il convient donc d'améliorer leur clarté et leur prévisibilité dans le règlement proposé.

[57] Rapport d'analyse d'impact, annexe 8, p. 281 à 283.
[58] Rapport d'analyse d'impact, p. 279 et suivantes.

4.5.6 Détection de sollicitation d'enfants (pédopiégeage)

68. L'EDPB et le CEPD font observer que les mesures proposées concernant la détection de la sollicitation d'enfants («pédopiégeage»), qui impliquent une analyse automatisée du discours ou du texte, sont susceptibles de constituer l'ingérence la plus importante dans les droits des utilisateurs à la vie privée et familiale, y compris la confidentialité des communications, et à la protection des données à caractère personnel.

69. Si la détection de matériel connu et même nouveau peut se limiter à l'analyse d'images et de vidéos, la détection de pédopiégeage s'étendrait par définition à toutes les communications textuelles (et éventuellement audio) qui relèvent d'une injonction de détection. Par conséquent, l'intensité de l'ingérence dans la confidentialité des communications concernées est beaucoup plus importante.

70. L'EDPB et le CEPD considèrent que l'analyse automatisée générale et indifférenciée de facto des communications textuelles transmises par l'intermédiaire de services de communications interpersonnelles en vue d'identifier la sollicitation potentielle d'enfants ne respecte pas les exigences de nécessité et de proportionnalité. Même si la technologie utilisée se limite à l'utilisation d'indicateurs, l'EDPB et le CEPD considèrent que le déploiement d'une telle analyse générale et indifférenciée est excessif et peut même porter atteinte au cœur même du droit fondamental au respect de la vie privée consacré à l'article 7 de la Charte.

71. Comme nous l'avons déjà indiqué, l'absence de garanties substantielles dans le cadre des mesures de détection de la sollicitation d'enfants ne peut être compensée uniquement par des garanties procédurales. En outre, le problème du manque de clarté et de sécurité juridiques suffisantes (par exemple, l'utilisation de termes juridiques vagues tels que «mesure appréciable») est encore plus grave dans le cas de l'analyse automatisée de communications personnelles textuelles, par rapport à la comparaison de photos fondée sur la technologie de hachage.

72. Par ailleurs, l'EDPB et le CEPD considèrent que l'«effet paralysant» sur la liberté d'expression est particulièrement important lorsque les communications textuelles (ou audio) des particuliers sont examinées et analysées à grande échelle. L'EDPB et le CEPD rappellent que cet effet paralysant est d'autant plus grave que la clarté de la loi est faible.

73. En outre, comme indiqué dans le rapport d'analyse d'impact[59] et dans l'étude du service de recherche du Parlement européen[60], le taux de précision des technologies de détection de pédopiégeage textuel est nettement inférieur au taux de précision des technologies de détection de matériel connu[61]. Les techniques de détection de pédopiégeage sont conçues pour analyser et attribuer des notes de probabilité à chaque aspect de la conversation. Par conséquent, l'EDPB et le CEPD les considèrent également exposés aux erreurs et vulnérables aux abus.

4.5.7 Conclusion sur la nécessité et la proportionnalité des mesures envisagées

74. En ce qui concerne la nécessité et la proportionnalité des mesures de détection envisagées, l'EDPB et le CEPD sont particulièrement préoccupés en ce qui concerne les mesures envisagées pour la détection de matériel inconnu et la sollicitation d'enfants (pédopiégeage), en raison de leur caractère

[59] Rapport d'analyse d'impact, annexe 8, p. 281 à 283.
[60] p. 15 à 18.
[61] Voir ci-dessus, point 40.

intrusif compte tenu de l'octroi potentiel d'un accès généralisé au contenu des communications, de leur nature probabiliste et des taux d'erreur associés à ces technologies.

75. En outre, on peut déduire de la jurisprudence de la Cour que les mesures permettant aux autorités publiques d'avoir accès de manière généralisée au contenu d'une communication sont plus susceptibles d'affecter le contenu essentiel des droits garantis par les articles 7 et 8 de la Charte. Ces considérations sont particulièrement pertinentes en ce qui concerne les mesures de détection de la sollicitation d'enfants envisagées par la proposition.

76. En tout état de cause, l'EDPB et le CEPD considèrent que l'ingérence créée notamment par les mesures de détection de la sollicitation d'enfants va au-delà de ce qui est strictement nécessaire et proportionné. Ces mesures devraient donc être supprimées de la proposition.

4.6 Obligations en matière de signalement

77. L'EDPB et le CEPD recommandent de compléter la liste des exigences spécifiques en matière de signalement figurant à l'article 13 de la proposition par l'obligation d'inclure dans le signalement des informations sur la technologie spécifique qui a permis au fournisseur de prendre connaissance des contenus abusifs pertinents, au cas où le fournisseur aurait eu connaissance d'abus sexuels potentiels commis contre des enfants à la suite de mesures prises pour exécuter une injonction de détection émise conformément à l'article 7 de la proposition.

4.7 Obligations de retrait et de blocage

78. L'une des mesures envisagées par la proposition pour atténuer les risques de diffusion de matériel est l'émission d'injonctions de suppression et de blocage qui obligeraient les fournisseurs à retirer du matériel en ligne relatif à des abus sexuels sur enfants, à désactiver ou à en bloquer l'accès[62].

79. Bien que l'incidence des injonctions de retrait sur la protection des données et le respect de la vie privée des communications soit relativement limitée, à titre de remarque générale, l'EDPB et le CEPD rappellent le principe fondamental à respecter, selon lequel toute mesure de ce type devrait être aussi ciblée que possible.

80. Dans le même temps, l'EDPB et le CEPD attirent l'attention sur le fait que les fournisseurs de services d'accès à l'internet n'ont accès à l'URL précise du contenu que si ce contenu est mis à disposition dans un texte clair. Chaque fois que le contenu est rendu accessible via une adresse HTTPS, le fournisseur d'accès à l'internet n'aura pas accès à l'URL précise, à moins de rompre le chiffrement de la communication. Par conséquent, l'EDPB et le CEPD ont des doutes quant à l'efficacité des mesures de blocage et estiment qu'il serait disproportionné d'exiger des fournisseurs de services d'accès à l'internet qu'ils déchiffrent les communications en ligne afin de bloquer celles concernant le matériel.

81. En outre et de manière plus générale, il convient de noter que le blocage (ou la désactivation) de l'accès à un élément numérique est une opération qui a lieu au niveau du réseau et que sa mise en œuvre peut s'avérer inefficace en cas de copies multiples (éventuellement similaires et non identiques) d'un même élément. En outre, une telle opération peut s'avérer disproportionnée si le blocage affecte d'autres éléments numériques, et non illégaux, lorsqu'ils sont conservés sur le

[62] Proposition, articles 14 et 16.

même serveur et rendus inaccessibles au moyen de commandes réseau (par exemple, l'adresse IP ou la liste noire DNS). Qui plus est, toutes les approches du blocage au niveau du réseau ne sont pas aussi efficaces et certaines peuvent facilement être contournées par des compétences techniques plutôt élémentaires.

82. Enfin, les pouvoirs des autorités de coordination en ce qui concerne l'émission d'injonctions de blocage devraient être clarifiés dans la proposition de règlement. Par exemple, au vu du libellé actuel de l'article 16, paragraphe 1, et de l'article 17, paragraphe 1, il n'apparaît pas clairement si les autorités de coordination sont habilitées à émettre ou uniquement à demander l'émission d'injonctions de blocage[63].

4.8 Technologies et garanties pertinentes

4.8.1 Protection des données dès la conception et protection des données par défaut

83. Les exigences de la proposition qui s'appliquent aux technologies à déployer pour la détection de matériel et la sollicitation d'enfants ne semblent pas suffisamment strictes. En particulier, l'EDPB et le CEPD ont fait observer que, contrairement aux dispositions analogues du règlement provisoire[64], la proposition ne fait aucune référence expresse au principe de protection des données dès la conception et par défaut, et ne prévoit pas que les technologies utilisées pour examiner le texte dans les communications ne doivent pas pouvoir déduire la substance du contenu des communications. La proposition prévoit simplement, à l'article 10, paragraphe 3, point b), que les technologies ne doivent pas permettre d'«extraire» des communications pertinentes d'autres informations que celles strictement nécessaires à la détection. Toutefois, cette norme ne semble pas suffisamment stricte, car il pourrait être possible de *déduire* d'autres informations de la substance du contenu d'une communication sans en *extraire* des informations en tant que telles.

84. Par conséquent, le CEPD et l'EDPB recommandent d'introduire dans la proposition un considérant stipulant que le principe de protection des données dès la conception et de protection des données par défaut énoncé à l'article 25 du règlement (UE) 2016/679 s'applique aux technologies régies par l'article 10 de la proposition en vertu de la loi et n'a donc pas dû être repris dans le texte juridique. En outre, il convient de modifier l'article 10, paragraphe 3, point b), de manière à ce que non seulement aucune autre information ne soit extraite, mais également qu'elle ne soit pas déduite, comme le prévoit actuellement l'article 3, paragraphe 1, point b), du règlement provisoire.

4.8.2 Fiabilité des technologies

85. La proposition part du principe que plusieurs types de solutions technologiques peuvent être utilisées par les fournisseurs de services pour exécuter des injonctions de détection. En particulier, la proposition part du principe que des systèmes d'intelligence artificielle sont disponibles et fonctionnent pour la détection de matériel inconnu et pour la détection de sollicitations d'enfants[65], et que certaines autorités de coordination pourraient les considérer comme les plus avancées. Si

[63] L'article 16, paragraphe 1, de la proposition est libellé comme suit: «L'autorité de coordination du lieu d'établissement a le pouvoir de demander à l'autorité judiciaire compétente de l'État membre qui l'a désignée ou à une autorité administrative indépendante de cet État membre d'émettre une injonction de blocage […]», tandis que l'article 17, paragraphe 1, est libellé comme suit: «L'autorité de coordination du lieu d'établissement émet les injonctions de blocage visées à l'article 16 […]» (soulignement ajouté).
[64] Règlement provisoire, article 3, paragraphe 1, point b).
[65] Voir rapport d'analyse d'impact, p. 281 et 282.

l'efficacité de la proposition dépend de la fiabilité de ces solutions technologiques, très peu d'informations sont disponibles sur l'utilisation généralisée et systématique de ces techniques, ce qui mérite un examen attentif.

86. En outre, même si l'EDPB et le CEPD ont dû les utiliser dans leur évaluation de la proportionnalité, en raison de l'absence de solutions de remplacement, il convient de noter que les indicateurs de performance des technologies de détection mentionnés dans le rapport d'analyse d'impact qui accompagnait la proposition ne fournissent que très peu d'informations sur la manière dont elles ont été évaluées et sur la question de savoir s'ils reflètent les performances réelles des technologies concernées. Il n'existe aucune information sur les essais ou les référentiels utilisés par les vendeurs de technologies pour mesurer ces performances. Sans ces informations, il n'est pas possible de reproduire les essais ou d'évaluer la validité des déclarations de performance. À cet égard, il convient de noter que, bien que les indicateurs de performance puissent être interprétés comme suggérant que certains outils de détection présentent un niveau élevé de précision (par exemple, la précision de certains outils de détection de pédopiégeage est de 88 %)[66], ces indicateurs devraient être examinés à la lumière de l'utilisation pratique envisagée des outils de détection et de la gravité des risques qu'une évaluation incorrecte d'un matériel donné entraînerait pour les personnes concernées. En outre, l'EDPB et le CEPD considèrent que, dans le cadre d'un traitement à risque aussi élevé, un taux d'échec de 12 % présente un risque élevé pour les personnes concernées qui ont fait l'objet de faux positifs, même lorsque des garanties sont en place pour empêcher les faux signalements à des services répressifs. Il est très peu probable que les fournisseurs de services puissent engager des ressources suffisantes pour examiner un tel pourcentage de faux positifs.

87. Comme indiqué précédemment[67], les indicateurs de performance devraient fournir un aperçu exhaustif du comportement des outils de détection. Lors de l'utilisation d'algorithmes d'intelligence artificielle sur des images ou des textes, il est bien documenté que des biais et des discriminations peuvent survenir en raison du manque de représentativité de certains groupes de population dans les données utilisées pour entraîner l'algorithme. Ces biais devraient être identifiés, mesurés et ramenés à un niveau acceptable afin que les systèmes de détection soient réellement profitables à la société dans son ensemble.

88. Bien qu'une étude des technologies utilisées pour la détection ait été réalisée[68], l'EDPB et le CEPD estiment qu'une analyse plus approfondie est nécessaire afin d'évaluer de manière indépendante la fiabilité des outils existants dans les cas d'utilisation réelle. Cette analyse devrait s'appuyer sur des indicateurs de performance exhaustifs et évaluer l'incidence des erreurs potentielles dans les conditions réelles pour toutes les personnes concernées par la proposition. Étant donné que ces technologies constituent la base sur laquelle se fonde la proposition, l'EDPB et le CEPD considèrent que cette analyse revêt une importance capitale pour évaluer l'adéquation de la proposition.

89. L'EDPB et le CEPD notent également que la proposition ne définit pas d'exigences technologiques spécifiques, que ce soit en ce qui concerne les taux d'erreur, l'utilisation de classificateurs et leur validation, ou d'autres restrictions. Cela laisse à la pratique le soin d'élaborer de tels critères lors de l'évaluation de la proportionnalité de l'utilisation d'une technologie spécifique, ce qui contribue encore davantage au manque de précision et de clarté.

---

[66] Ibidem, p. 283.
[67] Voir points 63 et 64 ci-dessus.
[68] Voir rapport d'analyse d'impact, p. 279 et suivantes.

90. Compte tenu de l'importance des conséquences pour les personnes concernées en cas de faux positifs, l'EDPB et le CEPD estiment que les taux de faux positifs doivent être réduits au maximum et que ces systèmes doivent être conçus tout en gardant à l'esprit que la grande majorité des communications électroniques ne comprennent ni matériel ni sollicitations d'enfants, et que même un taux de faux positifs très faible impliquera un nombre très élevé de faux positifs compte tenu du volume de données qui feront l'objet d'une détection. Plus généralement, l'EDPB et le CEPD sont également préoccupés par le fait que la performance des outils disponibles indiquée dans le rapport d'analyse d'impact ne reflète pas d'indicateurs précis et comparables concernant les taux de faux positifs et de faux négatifs, et considèrent que des indicateurs de performance comparables et significatifs pour ces technologies devraient être publiés, avant de les considérer comme disponibles et efficaces.

4.8.3 Examen des communications audio

91. Contrairement au règlement provisoire[69], la proposition n'exclut pas de son champ d'application l'examen des communications audio dans le cadre de la détection de pédopiégeage[70]. L'EDPB et le CEPD estiment que l'examen des communications audio est particulièrement intrusif, car il nécessiterait normalement une interception active, continue et «en direct». En outre, dans certains États membres, le caractère privé de la parole bénéficie d'une protection particulière[71]. En outre, étant donné que, en principe, tout le contenu de la communication audio devrait être analysé, cette mesure est susceptible de porter atteinte au contenu essentiel des droits garantis par les articles 7 et 8 de la Charte. Par conséquent, cette méthode de détection devrait rester en dehors du champ d'application des obligations de détection énoncées dans la proposition de règlement, tant en ce qui concerne les messages vocaux que les communications en direct, d'autant plus que le rapport d'analyse d'impact qui accompagnait la proposition n'a pas identifié de risques ou de changements spécifiques dans le paysage des menaces qui justifieraient son utilisation[72].

4.8.4 Vérification de l'âge

92. La proposition encourage les fournisseurs à recourir à des mesures de vérification de l'âge et d'évaluation de l'âge pour identifier les enfants utilisateurs de leurs services[73]. À cet égard, l'EDPB et le CEPD notent qu'il n'existe actuellement aucune solution technologique capable d'évaluer avec certitude l'âge d'un utilisateur dans un contexte en ligne, sans s'appuyer sur une identité numérique officielle, qui n'est pas accessible à tous les citoyens européens à ce stade[74]. Par conséquent, le recours envisagé dans la proposition à des mesures de vérification de l'âge pourrait entraîner l'exclusion, par exemple, d'adultes paraissant jeunes de l'accès aux services en ligne, ou le déploiement d'outils de vérification de l'âge très intrusifs, ce qui pourrait empêcher ou décourager l'utilisation légitime des services concernés.

93. À cet égard, et même si le considérant 16 de la proposition mentionne les outils de contrôle parental comme d'éventuelles mesures d'atténuation, l'EDPB et le CEPD recommandent que le règlement

[69] Voir règlement provisoire, article 1er, paragraphe 2.
[70] Voir proposition, article 1er.
[71] Voir, par exemple, article 201 du code pénal allemand.
[72] Voir rapport d'analyse d'impact.
[73] Voir proposition, article 4, paragraphe 3, et article 6, paragraphe 1, point c), et considérant 16.
[74] Voir par exemple la recommandation 7 de la CNIL: vérifier l'âge de l'enfant et l'accord des parents dans le respect de sa vie privée (9 août 2021).

proposé soit modifié afin de permettre expressément aux fournisseurs de s'appuyer sur des mécanismes de contrôle parental en plus ou en lieu et place de la vérification de l'âge.

4.9 Préservation des informations

94. L'article 22 de la proposition limite les finalités pour lesquelles les fournisseurs soumis à la proposition peuvent conserver les données relatives au contenu et les autres données traitées dans le cadre des mesures prises pour se conformer aux obligations énoncées dans la proposition. Toutefois, la proposition indique que les fournisseurs peuvent également conserver ces informations afin d'améliorer l'efficacité et la précision des technologies permettant de détecter les abus sexuels sur enfants en ligne aux fins de l'exécution d'une injonction de détection, mais qu'ils ne conservent aucune donnée à caractère personnel à cette fin[75].

95. L'EDPB et le CEPD estiment que seuls les fournisseurs qui utilisent leurs propres technologies de détection devraient être autorisés à conserver des données afin d'améliorer l'efficacité et la précision des technologies, tandis que ceux qui utilisent les technologies fournies par le centre de l'UE ne devraient pas bénéficier de cette possibilité. En outre, l'EDPB et le CEPD notent qu'il pourrait être difficile de garantir, dans la pratique, qu'aucune donnée à caractère personnel ne soit conservée à cette fin, étant donné que la plupart des données relatives au contenu et des autres données traitées à des fins de détection sont susceptibles d'être considérées comme des données à caractère personnel.

4.10 Incidence sur le chiffrement

96. Les autorités européennes de protection des données n'ont cessé de plaider en faveur de la disponibilité généralisée d'outils de chiffrement robustes et contre tout type de portes dérobées[76]. En effet, le chiffrement est important pour garantir le respect de tous les droits de l'homme hors ligne et en ligne[77]. En outre, les technologies de chiffrement contribuent de manière fondamentale à la fois au respect de la vie privée et de la confidentialité des communications, ainsi qu'à l'innovation et à la croissance de l'économie numérique, qui repose sur le niveau élevé de confiance que ces technologies offrent.

97. Dans le contexte des communications interpersonnelles, le chiffrement de bout en bout («E2EE») est un outil essentiel pour garantir la confidentialité des communications électroniques, car il offre de solides garanties techniques contre l'accès au contenu des communications par toute personne autre que l'expéditeur et le ou les destinataires, y compris par le fournisseur. Empêcher ou décourager de quelque manière que ce soit l'utilisation du système E2EE, imposer aux fournisseurs de services l'obligation de traiter les données de communications électroniques à d'autres fins que la fourniture de leurs services, ou leur imposer une obligation de transmettre de manière proactive des communications électroniques à des tiers, entraînerait le risque que les fournisseurs proposent des services moins chiffrés afin de mieux respecter les obligations, affaiblissant ainsi le rôle du chiffrement en général et portant atteinte au respect des droits fondamentaux des citoyens européens. Il convient de noter que, si le système E2EE est l'une des mesures de sécurité les plus couramment utilisées dans

[75] Proposition, article 22, paragraphe 1.
[76] Voir, par exemple, groupe de travail «Article 29» sur la protection des données, déclaration du groupe de travail «Article 29» sur le chiffrement et son incidence sur la protection des personnes physiques à l'égard du traitement de leurs données à caractère personnel dans l'UE (11 avril 2018).
[77] Voir Conseil des droits de l'homme, Résolution 47/16 sur la promotion, la protection et l'exercice des droits de l'homme sur Internet, document des Nations unies A/HRC/RES/47/16 (26 juillet 2021).

le contexte des communications électroniques, d'autres solutions techniques (par exemple, l'utilisation d'autres systèmes cryptographiques) pourraient être ou devenir tout aussi importantes pour sécuriser et protéger la confidentialité des communications numériques. Par conséquent, leur utilisation ne devrait pas non plus être empêchée ou découragée.

98. Le déploiement d'outils d'interception et d'analyse des communications électroniques interpersonnelles est fondamentalement en contradiction avec le système E2EE, étant donné que ce dernier vise à garantir techniquement qu'une communication reste confidentielle entre l'expéditeur du destinataire.

99. Par conséquent, même si la proposition n'établit pas d'obligation d'interception systématique pour les fournisseurs, la simple possibilité qu'une injonction de détection soit émise est susceptible de peser lourdement sur les choix techniques opérés par les fournisseurs, en particulier compte tenu du délai limité qu'ils devront respecter pour se conformer à une telle injonction et des lourdes sanctions qu'ils encourraient en cas de manquement à cette obligation[78]. Dans la pratique, cela pourrait amener certains fournisseurs à cesser d'utiliser le système E2EE.

100. L'incidence d'une dégradation ou du découragement de l'utilisation de système E2EE, qui peut résulter de la proposition, doit être évaluée correctement. Chacune des techniques visant à contourner le caractère respectueux de la vie privée du système E2EE présentées dans le rapport d'analyse d'impact qui accompagnait la proposition introduirait des failles de sécurité[79]. Par exemple, l'examen côté client[80] entraînerait probablement un accès et un traitement substantiels et non ciblés de contenus non chiffrés sur les appareils de l'utilisateur final. Une telle dégradation substantielle de la confidentialité affecterait particulièrement les enfants, étant donné que les services qu'ils utilisent sont plus susceptibles d'être ciblés par des injonctions de détection, ce qui les rend vulnérables à la surveillance ou à l'écoute illicite. Dans le même temps, l'examen *côté serveur* est également fondamentalement incompatible avec le paradigme E2EE, étant donné que le canal de communication, chiffré de poste à poste, devrait être brisé, ce qui entraînerait le traitement massif de données à caractère personnel sur les serveurs des fournisseurs.

101. Alors que la proposition indique qu'elle «laisse [...] au fournisseur concerné le choix des technologies à utiliser pour se conformer efficacement aux injonctions de détection et ne devrait pas être compris en ce sens qu'il encouragerait ou découragerait l'utilisation d'une technologie donnée» [81], l'incompatibilité structurelle de certaines injonctions de détection avec le système E2EE devient en fait un puissant frein à l'utilisation du système E2EE. L'impossibilité d'accéder à des services utilisant le système E2EE et de les utiliser (qui constituent l'état actuel de la technique en matière de garantie technique de confidentialité) pourrait avoir un effet paralysant sur la liberté d'expression et l'utilisation légitime des services de communications électroniques à des fins privées. La Commission reconnaît également la relation négative entre la détection de matériel ou de pédopiégeage et le

[78] Voir proposition, article 35.

[79] Voir section 4.2 dans Abelson, Harold, Ross J. Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, John L. Callas, Whitfield Diffie, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Vanessa Teague et Carmela Troncoso, «Bugs in our Pockets: The Risks of Client-Side Scanning», ArXiv abs/2110.07450 (2021).

[80] L'examen côté client désigne globalement les systèmes qui examinent le contenu des messages pour les correspondances avec une base de données de contenu contestable avant l'envoi du message au destinataire prévu.

[81] Proposition, considérant 26.

système E2EE lorsqu'elle a noté dans le rapport d'analyse d'impact[82] la probabilité que la mise en œuvre du système E2EE par Facebook en 2023 mette un terme à l'examen volontaire de Facebook.

102. Afin de garantir que le règlement proposé ne porte pas atteinte à la sécurité ou à la confidentialité des communications électroniques des citoyens européens, l'EDPB et le CEPD estiment que le dispositif de la proposition devrait indiquer clairement qu'aucune disposition du règlement proposé ne devrait être interprétée comme interdisant ou affaiblissant le chiffrement, conformément à ce qui est indiqué au considérant 25 du règlement provisoire.

4.11 Surveillance, application et coopération

4.11.1 Rôle des autorités de contrôle nationales en vertu du RGPD

103. La proposition prévoit la mise en place d'un réseau d'autorités nationales de coordination, qui sera chargé de l'application et de l'exécution du règlement proposé[83]. Alors que le considérant 54 de la proposition indique que «les règles énoncées dans le présent règlement en matière de surveillance et de contrôle de l'application ne devraient pas être comprises comme portant atteinte aux pouvoirs et compétences des autorités de protection des données au titre du règlement (UE) 2016/679», l'EDPB et le CEPD sont d'avis que la relation entre les tâches des autorités de coordination et celles des autorités chargées de la protection des données devrait être mieux réglementée et que les autorités chargées de la protection des données devraient se voir accorder un rôle plus important dans le règlement proposé.

104. En particulier, les fournisseurs devraient être tenus de consulter les autorités chargées de la protection des données dans le cadre d'une procédure de consultation préalable telle que visée à l'article 36 du RGPD avant le déploiement de toute mesure de détection de matériel ou pédopiégeage, et non exclusivement dans le cadre de l'utilisation de mesures de détection de sollicitation d'enfants, comme le prévoit actuellement la proposition[84] . Toutes les mesures de détection devraient être considérées comme donnant lieu à un «risque élevé» par défaut et devraient donc faire l'objet d'une procédure de consultation préalable, qu'il s'agisse de pédopiégeage ou de matériel, comme c'est déjà le cas dans le cadre du règlement provisoire[85]. En outre, les autorités compétentes en matière de protection des données désignées au titre du RGPD devraient toujours être habilitées à donner leur avis sur les mesures de détection envisagées, et pas seulement dans des circonstances spécifiques[86].

105. Par ailleurs, le règlement proposé devrait établir un système permettant de traiter et de résoudre les différends entre les autorités compétentes et les autorités chargées de la protection des données en ce qui concerne les injonctions de détection. En particulier, les autorités chargées de la protection des données devraient avoir le droit de contester une injonction de détection devant les juridictions de l'État membre de l'autorité judiciaire compétente ou de l'autorité administrative indépendante qui a émis la décision de détection. À cet égard, l'EDPB et le CEPD notent la façon dont, dans la version actuelle de la proposition, l'autorité compétente peut rejeter l'avis de l'autorité compétente en matière de protection des données lorsqu'elle émet une injonction de détection. Cela pourrait conduire à des décisions contradictoires, étant donné que les autorités chargées de la protection des données conserveraient, comme le confirme l'article 36, paragraphe 2, du RGPD, l'ensemble de leurs

[82] Rapport d'analyse d'impact, p. 27.
[83] Proposition, article 25.
[84] Proposition, article 7, paragraphe 3, deuxième tiret b).
[85] Règlement provisoire, article 3, paragraphe 1, point c).
[86] Voir proposition, article 7, paragraphe 3, deuxième tiret c).

pouvoirs correctifs en vertu de l'article 58 du RGPD, y compris le pouvoir d'ordonner une interdiction de traitement.

4.11.2 Rôle du Comité européen de la protection des données

106. L'EDPB et le CEPD notent que la proposition prévoit, à l'article 50, paragraphe 1, troisième phrase, que «le centre de l'UE demande l'avis de son comité chargé des aspects technologiques et du comité européen de la protection des données» avant d'ajouter une technologie spécifique aux listes de technologies que les fournisseurs de services d'hébergement et les fournisseurs de services de communications interpersonnelles peuvent envisager d'utiliser pour exécuter des injonctions de détection. Elle prévoit en outre que l'EDPB rend ses avis dans un délai de huit semaines, qui peut être prolongé de six semaines si nécessaire, en fonction de la complexité de la question. Elle prévoit enfin que l'EDPB informe le centre de l'UE de toute prolongation dans un délai d'un mois à compter de la réception de la demande de consultation, ainsi que des motifs du retard.

107. Les tâches existantes de l'EDPB sont définies à l'article 70 du RGPD et à l'article 51 de la directive (UE) 2016/680 (ci-après la «directive en matière de protection des données dans le domaine répressif»)[87]. Dans le cadre de ces tâches, il est prévu que l'EDPB fournit des conseils à la Commission et émet des avis à la demande de la Commission, d'une autorité de contrôle nationale ou de son président. Alors que l'article 1er, paragraphe 3, point d), de la proposition dispose que les règles énoncées dans le RGPD et la directive en matière de protection des données dans le domaine répressif ne sont pas affectées par la proposition, le fait d'habiliter le centre de l'UE à demander l'avis de l'EDPB va au-delà des tâches qui lui sont confiées en vertu du RGPD et de la directive en matière de protection des données dans le domaine répressif. Il convient donc de préciser dans la proposition de règlement – au moins dans un considérant – que la proposition élargit les tâches de l'EDPB. À cet égard, l'EDPB et le CEPD apprécient le rôle important que la proposition attribue à l'EDPB en exigeant sa participation à la mise en œuvre pratique du règlement proposé. Dans la pratique, le secrétariat de l'EDPB joue un rôle essentiel en fournissant le soutien analytique, administratif et logistique nécessaire à l'adoption des avis de l'EDPB. Par conséquent, pour veiller à ce que l'EDPB et ses membres puissent s'acquitter de leurs tâches, il est essentiel d'allouer un budget et un personnel suffisants à l'EDPB. Malheureusement, la fiche financière législative de la proposition n'indique pas que des ressources supplémentaires seront mises à disposition pour l'exécution des tâches supplémentaires que la proposition confie à l'EDPB[88].

108. En outre, l'EDPB et le CEPD font observer que l'article 50 de la proposition n'indique pas comment le centre de l'UE procédera après avoir reçu un avis de l'EDPB[89]. Le considérant 27 de la proposition indique simplement que les conseils donnés par l'EDPB devraient être pris en considération par le centre de l'UE et la Commission européenne. Il convient donc de préciser quel sera l'objectif de l'avis demandé dans le cadre du processus prévu à l'article 50 de la proposition et comment le centre de l'UE doit agir après avoir reçu un avis de l'EDPB.

---

[87] 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 (JO L 119 du 4.5.2016, p. 89).

[88] Voir proposition, p. 105 et suivantes.

[89] Voir, en revanche, l'article 51, paragraphe 4, de la directive en matière de protection des données dans le domaine répressif.

109. En outre, l'EDPB et le CEPD considèrent que, si les lignes directrices de l'EDPB ou tout avis éventuel sur l'utilisation des technologies de détection évalueront l'utilisation de ces technologies à un niveau général, pour une consultation préalable au titre de l'article 36 du RGPD, l'autorité de contrôle nationale devra tenir compte des circonstances spécifiques et procéder à une évaluation au cas par cas du traitement envisagé par le responsable du traitement concerné. L'EDPB et le CEPD notent que les autorités de contrôle appliqueront et devraient appliquer les critères énoncés à l'article 36 du RGPD pour décider s'il est nécessaire de prolonger le délai fixé dans le RGPD pour rendre leurs avis en réponse à une consultation préalable, et qu'il n'est pas nécessaire d'appliquer des normes différentes lorsqu'une consultation préalable concerne l'utilisation d'une technologie de détection[90].

110. Enfin, en application de l'article 11 («Lignes directrices concernant les obligations de détection»), la proposition prévoit que la Commission peut publier des lignes directrices sur l'application des articles 7 à 10 de la proposition. L'article 11 de la proposition devrait être modifié afin de préciser que, outre les autorités de coordination et le centre de l'UE, la Commission devrait consulter l'EDPB sur le projet de lignes directrices en dehors du processus de consultation publique envisagé avant de publier des lignes directrices concernant les obligations de détection.

111. Par conséquent, cette tâche de l'EDPB, ainsi que son rôle dans le cadre juridique qui serait introduit par la proposition, justifient une évaluation plus approfondie par le législateur.

4.11.3 Rôle du centre de l'UE sur les abus sexuels commis contre des enfants

112. Le chapitre IV de la proposition créerait le centre de l'UE en tant que nouvelle agence décentralisée pour permettre la mise en œuvre de la proposition. Entre autres tâches, le centre de l'UE devrait faciliter l'accès des fournisseurs à des technologies de détection fiables; mettre à disposition, à des fins de détection, des indicateurs créés sur la base des abus sexuels commis contre des enfants en ligne, tels que vérifiés par les juridictions ou les autorités administratives indépendantes des États membres; fournir, sur demande, une certaine assistance en ce qui concerne la réalisation d'évaluations des risques; et apporter un soutien dans la communication avec les autorités nationales compétentes[91].

113. À cet égard, l'EDPB et le CEPD accueillent favorablement l'article 77, paragraphe 1, de la proposition, qui confirme que le traitement de données à caractère personnel par le centre de l'UE est soumis au RPDUE et prévoit que les mesures d'application dudit règlement par le centre de l'UE, y compris celles concernant la nomination d'un délégué à la protection des données du centre de l'UE, sont établies après consultation du CEPD. Toutefois, l'EDPB et le CEPD sont d'avis que plusieurs dispositions de ce chapitre méritent un examen plus approfondi.

114. En premier lieu, l'EDPB et le CEPD relèvent que l'article 48 de la proposition prévoit la transmission de tous les signalements qui ne sont pas «manifestement dénués de fondement»[92] aux services répressifs nationaux et à l'Agence de l'Union européenne pour la coopération des services répressifs (ci-après «Europol»). Ce seuil pour que le centre de l'UE transmette des signalements aux autorités répressives nationales et à Europol («qui ne sont pas manifestement dénués de fondement») semble trop bas, en

[90] Voir proposition, considérant 24.
[91] Voir COM(2022) 209 final, p. 7.
[92] Le terme «manifestement dénué de fondement» est décrit au considérant 65 de la proposition comme lorsqu'«il apparaît immédiatement, sans analyse factuelle ou juridique approfondie, que les activités signalées ne constituent pas des abus sexuels sur enfants en ligne».

particulier compte tenu du fait que l'objectif de la création du centre de l'UE, tel qu'énoncé dans le rapport d'analyse d'impact de la Commission[93], est d'alléger la charge pesant sur les services répressifs et Europol en ce qui concerne le filtrage des contenus signalés par erreur comme du matériel. À cet égard, il est difficile de comprendre pourquoi le centre de l'UE, en tant que pôle d'expertise, ne pourrait pas procéder à une évaluation juridique et factuelle plus approfondie pour limiter les risques de transmission des données de personnes innocentes aux services répressifs.

115. Deuxièmement, la disposition relative à la durée de conservation des données à caractère personnel par le centre de l'UE semble relativement ouverte compte tenu de la sensibilité des données concernées. Même s'il n'était pas possible de fixer une durée de conservation maximale pour la conservation de ces données, l'EDPB et le CEPD recommandent de fixer, dans la proposition, au moins un délai maximal pour examiner la nécessité de continuer à conserver les données et exiger une justification de la conservation prolongée après cette période.

116. En outre, compte tenu de la très grande sensibilité des données à caractère personnel devant être traitées par le centre de l'UE, l'EDPB et le CEPD sont d'avis que le traitement devrait faire l'objet de garanties supplémentaires, notamment pour assurer une surveillance efficace. Cela pourrait inclure l'obligation pour le centre de l'UE de tenir des registres pour les opérations de traitement effectuées dans les systèmes de traitement automatisé concernant les données (c'est-à-dire reflétant l'exigence relative aux données opérationnelles à caractère personnel au titre du chapitre IX du RPDUE), y compris l'enregistrement, la modification, l'accès, la consultation, la divulgation, la combinaison et l'effacement des données à caractère personnel. Les journaux des opérations de consultation et de communication permettent d'établir le motif, la date et l'heure de ces opérations, l'identification de la personne qui a consulté ou communiqué les données opérationnelles à caractère personnel, ainsi que, dans la mesure du possible, l'identité des destinataires. Ces registres seraient utilisés pour vérifier la licéité du traitement, l'autocontrôle, ainsi que pour garantir son intégrité et sa sécurité, et seraient mis à la disposition du délégué à la protection des données du centre de l'UE et du CEPD sur demande.

117. En outre, la proposition fait référence à l'obligation pour les fournisseurs d'informer les utilisateurs de la détection de matériel au moyen d'injonctions de détection, ainsi qu'au droit de déposer une plainte auprès d'une autorité de coordination[94]. Toutefois, la proposition ne fixe pas de procédures pour l'exercice des droits des personnes concernées, compte tenu également des lieux multiples où les données à caractère personnel peuvent être transmises et conservées en vertu de la proposition (centre de l'UE, Europol, services répressifs nationaux). L'obligation d'informer les utilisateurs devrait inclure l'obligation d'informer les personnes que leurs données ont été transmises et sont traitées par différentes entités, le cas échéant (par exemple, par les services répressifs nationaux et Europol). En outre, il devrait y avoir une procédure centralisée pour la réception et la coordination des demandes de droit d'accès, de rectification et d'effacement ou, à défaut, une obligation de coordination entre l'entité qui reçoit une demande de la personne concernée et les autres entités concernées.

118. L'EDPB et le CEPD notent qu'en vertu de l'article 50 de la proposition, le centre de l'UE est chargé de préciser la liste des technologies qui peuvent être utilisées pour exécuter les injonctions de détection. Toutefois, conformément à l'article 12, paragraphe 1, de la proposition, les fournisseurs sont tenus de signaler toutes les informations indiquant des abus sexuels potentiels commis contre des enfants en ligne sur leurs services, et pas seulement celles provenant de l'exécution d'une injonction de

[93] Voir, par exemple, page 349 du rapport d'analyse d'impact.
[94] Voir l'article 10, paragraphe 6, et, à la suite de la présentation d'un signalement au centre de l'UE, l'article 12, paragraphe 2, de la proposition.

détection. Il est très probable qu'une grande partie de ces informations provienne de l'application des mesures d'atténuation prises par les fournisseurs, conformément à l'article 4 de la proposition. Il semble donc essentiel de déterminer quelles pourraient être ces mesures, leur efficacité, leur taux d'erreur dans le signalement d'éventuels abus sexuels commis contre des enfants et leur incidence sur les droits et libertés des personnes. Bien que l'article 4, paragraphe 5, de la proposition dispose que la Commission, en coopération avec les autorités de coordination et le centre de l'UE et après avoir mené une consultation publique, peut publier des lignes directrices pertinentes, l'EDPB et le CEPD estiment important que le législateur inclue à l'article 50 la tâche incombant au centre de l'UE de fournir également une liste de mesures d'atténuation recommandées et de bonnes pratiques pertinentes qui sont particulièrement efficaces pour détecter les abus sexuels potentiels commis contre des enfants en ligne. Étant donné que ces mesures sont susceptibles de porter atteinte aux droits fondamentaux à la protection des données et au respect de la vie privée, il est également recommandé au centre de l'UE de demander l'avis de l'EDPB avant de publier une telle liste.

119. Enfin, les exigences de sécurité énoncées à l'article 51, paragraphe 4, de la proposition devraient être plus précises. À cet égard, il est possible de s'inspirer des exigences de sécurité énoncées dans d'autres règlements relatifs aux systèmes à grande échelle impliquant un traitement à haut risque, tels que le règlement (CE) nº 767/2008[95] (voir article 32), le règlement (CE) nº 1987/2006[96] (voir article 16), le règlement (CE) nº 2018/1862[97] (voir article 16) et le règlement (UE) nº 603/2013[98] (voir article 34).

4.11.4 Rôle d'Europol

120. La proposition prévoit une coopération étroite entre le centre de l'UE et Europol. En vertu du chapitre IV de la proposition, lorsqu'il reçoit des signalements de fournisseurs concernant du matériel suspect, le centre de l'UE les vérifie pour déterminer quels signalements peuvent donner lieu à une action (qui ne sont pas manifestement dénués de fondement) et les transmet à Europol ainsi qu'aux autorités répressives nationales[99]. Le centre de l'UE accorde à Europol l'accès à ses bases de données d'indicateurs et à ses bases de données de signalements afin d'aider Europol à enquêter sur des

[95] Règlement (CE) nº 767/2008 du Parlement européen et du Conseil du 9 juillet 2008 concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour (règlement VIS) (JO L 218 du 13.8.2008, p. 60)

[96] Règlement (CE) n° 1987/2006 du Parlement européen et du Conseil du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II) (JO L 381 du 28.12.2006, p. 4).

[97] Règlement (UE) 2018/1862 du Parlement européen et du Conseil du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, modifiant et abrogeant la décision 2007/533/JAI du Conseil, et abrogeant le règlement (CE) nº 1986/2006 du Parlement européen et du Conseil et la décision 2010/261/UE de la Commission (JO L 312 du 7.12.2018, p. 56).

[98] Règlement (UE) nº 603/2013 du Parlement européen et du Conseil du 26 juin 2013 relatif à la création d'Eurodac pour la comparaison des empreintes digitales aux fins de l'application efficace du règlement (UE) nº 604/2013 établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale introduite dans l'un des États membres par un ressortissant de pays tiers ou un apatride et relatif aux demandes de comparaison avec les données d'Eurodac présentées par les autorités répressives des États membres et Europol à des fins répressives, et modifiant le règlement (UE) nº 1077/2011 portant création d'une agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (JO L 180 du 29.6.2013, p. 1).

[99] Voir article 48 de la proposition.

suspicions d'abus sexuels commis contre des enfants[100]. En outre, le centre de l'UE se verrait accorder l'accès «aussi large que possible» aux systèmes d'information d'Europol[101]. Les deux agences partageront également des locaux et certaines infrastructures (non opérationnelles)[102].

121. L'EDPB et le CEPD font observer que plusieurs aspects liés à la coopération entre le centre de l'UE proposé et Europol suscitent des préoccupations ou nécessitent des précisions supplémentaires.

Sur la transmission des signalements par le centre de l'UE à Europol (article 48)

122. L'article 48 de la proposition de règlement impose au centre de l'UE de transmettre les signalements qui ne sont pas considérés comme manifestement dénués de fondement, ainsi que toute information supplémentaire pertinente, à Europol et à l'autorité ou aux autorités répressives compétentes de l'État membre ou des États membres susceptibles d'être compétentes pour enquêter sur les abus sexuels potentiels commis contre des enfants ou engager des poursuites en la matière. Bien que cet article confère à Europol le rôle d'identifier l'autorité répressive compétente lorsque l'État membre concerné n'est pas clair, la disposition prévoit en fait que tous les signalements sont transmis à Europol, que l'autorité nationale ait été ou non identifiée et que le signalement ait ou non déjà été transmis par le centre de l'UE.

123. Toutefois, la proposition ne précise pas quelle serait la valeur ajoutée de la participation d'Europol ou de son rôle attendu lors de la réception des signalements, en particulier dans les cas où l'autorité répressive nationale a été identifiée et notifiée en parallèle[103].

124. L'EDPB et le CEPD rappellent que le mandat d'Europol se limite à soutenir l'action des autorités compétentes des États membres et leur coopération mutuelle dans la prévention et la lutte contre les formes graves de criminalité affectant deux ou plusieurs États membres[104]. L'article 19 du règlement (UE) 2016/794[105] tel que modifié par le règlement (UE) 2022/991[106] (ci-après le «règlement Europol modifié») dispose qu'un organisme de l'Union fournissant des informations à Europol est tenu de déterminer la ou les finalités pour lesquelles ces informations doivent être traitées par Europol, ainsi que les conditions de leur traitement. Il est également chargé de veiller à l'exactitude des données à caractère personnel transférées[107].

---

[100] Voir article 46, paragraphes 4 et 5, de la proposition.
[101] Voir article 53, paragraphe 2, de la proposition.
[102] Notamment en ce qui concerne la gestion des ressources humaines, les technologies de l'information (TI), y compris la cybersécurité, le bâtiment et les communications.
[103] Le considérant 71 de la proposition ne fait qu'une référence générale à l'expérience d'Europol dans l'identification des autorités nationales compétentes dans des situations peu claires et à sa base de données de renseignements en matière pénale, ce qui peut contribuer à identifier des liens vers des enquêtes dans d'autres États membres.
[104] Voir article 3 du règlement Europol modifié.
[105] Règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI (JO L 135 du 24.5.2016, p. 53).
[106] Règlement (UE) 2022/991 du Parlement européen et du Conseil du 8 juin 2022 modifiant le règlement (UE) 2016/794 en ce qui concerne la coopération d'Europol avec les parties privées, le traitement de données à caractère personnel par Europol à l'appui d'enquêtes pénales et le rôle d'Europol en matière de recherche et d'innovation (JO L 169 du 27.6.2022, p. 1).
[107] Article 38, paragraphe 2, point a), du règlement Europol modifié.

125. Une transmission généralisée des signalements à Europol serait donc contraire au règlement Europol modifié et comporterait un certain nombre de risques en matière de protection des données. La duplication du traitement des données à caractère personnel pourrait conduire à ce que des copies multiples des mêmes données à caractère personnel hautement sensibles soient conservées en parallèle (par exemple au centre de l'UE, à Europol, au sein des autorités répressives nationales), avec des risques pour l'exactitude des données en raison de la désynchronisation potentielle des bases de données, ainsi que pour l'exercice des droits des personnes concernées. Par ailleurs, le seuil bas fixé dans la proposition pour le partage de signalements avec les services répressifs (ceux qui ne sont pas manifestement dénués de fondement) implique une forte probabilité que les faux positifs (c'est-à-dire les contenus signalés par erreur comme des abus sexuels commis contre des enfants) soient conservés dans les systèmes d'information d'Europol, éventuellement pendant des périodes prolongées[108].

126. L'EDPB et le CEPD recommandent dès lors que la proposition précise et limite les circonstances et les finalités dans le cadre desquelles le centre de l'UE pourrait transmettre des signalements à Europol, conformément au règlement Europol modifié. Cela devrait explicitement exclure les circonstances dans lesquelles des signalements ont été transmis à l'autorité répressive compétente de l'État membre, qui n'impliquent aucune dimension transfrontière. En outre, la proposition devrait inclure l'exigence selon laquelle le centre de l'UE ne transfère à Europol que des données à caractère personnel qui sont adéquates, pertinentes et limitées à ce qui est strictement nécessaire. Des garanties spécifiques doivent également être prévues pour garantir la qualité et la fiabilité des données.

[108] Selon le rapport d'analyse d'impact de la Commission, Europol n'a pu examiner que 20 % des 50 millions d'images et de vidéos de matériel uniques dans sa base de données, ce qui implique un manque de ressources pour agir sur les contributions de matériel qu'elle reçoit actuellement. Voir le rapport d'analyse d'impact accompagnant la proposition de règlement établissant des règles visant à prévenir et à combattre les abus sexuels commis contre des enfants, SWD(2022) 209, p. 47 et 48.

Article 53, paragraphe 2, sur la coopération entre le centre de l'UE et Europol

127. L'article 53, paragraphe 2, de la proposition dispose qu'Europol et le centre de l'UE s'accordent mutuellement «un accès aussi large que possible aux informations et systèmes d'information pertinents, lorsque cela est nécessaire à l'exécution de leurs missions respectives et conformément aux actes du droit de l'Union régissant cet accès».

128. L'article 46, paragraphes 4 et 5, de la proposition précisent en outre qu'Europol a accès à la base de données des indicateurs et des signalements du centre de l'UE, et l'article 46, paragraphe 6, établit la procédure d'octroi de cet accès: Europol présente une demande précisant la finalité et le degré d'accès requis pour atteindre cet objectif, qui est dûment évaluée par le centre de l'UE.

129. Les critères et garanties conditionnant l'accès d'Europol et l'utilisation ultérieure des données provenant des systèmes d'information du centre de l'UE ne sont pas précisés. De surcroît, il n'est pas expliqué pourquoi il est nécessaire d'accorder à Europol un accès direct aux systèmes d'information d'une agence non répressive contenant des données à caractère personnel hautement sensibles, dont le lien avec les activités criminelles et la prévention de la criminalité n'a peut-être pas été établi. Afin de garantir un niveau élevé de protection des données et le respect du principe de limitation de la finalité, l'EDPB et le CEPD recommandent que la transmission de données à caractère personnel du centre de l'UE à Europol n'ait lieu qu'au cas par cas, à la suite d'une demande dûment évaluée, au moyen d'un outil de communication d'échange sécurisé, tel que SIENA[109].

130. L'article 53, paragraphe 2, contient la seule référence, dans la proposition, à l'accès du centre de l'UE aux systèmes d'information d'Europol. Il n'apparaît donc pas clairement à quelles fins et selon quelles garanties spécifiques un tel accès aurait lieu.

131. L'EDPB et le CEPD rappellent qu'Europol est une agence répressive, créée en vertu des traités de l'UE, qui a pour mission essentielle de prévenir et de combattre les formes graves de criminalité. Les données opérationnelles à caractère personnel traitées par Europol sont donc soumises à des règles et garanties strictes en matière de traitement des données. Le centre de l'UE proposé n'est pas un organe répressif et ne devrait en aucun cas se voir accorder un accès direct aux systèmes d'information d'Europol.

132. L'EDPB et le CEPD notent en outre qu'une grande partie des informations d'intérêt partagé pour le centre de l'UE et Europol concerneront les données à caractère personnel relatives aux victimes d'infractions présumées, les données à caractère personnel des mineurs et les données à caractère personnel relatives à la vie sexuelle, qui constituent des catégories particulières de données à caractère personnel en vertu du règlement Europol modifié. Le règlement Europol modifié impose des conditions strictes en ce qui concerne l'accès à des catégories particulières de données à caractère personnel. L'article 30, paragraphe 3, du règlement Europol modifié dispose que seul Europol a un accès direct à ces données à caractère personnel, et plus particulièrement un nombre limité d'agents d'Europol dûment autorisés par le directeur exécutif[110].

133. L'EDPB et le CEPD recommandent donc de clarifier le libellé de l'article 53, paragraphe 2, de la proposition afin de refléter correctement les restrictions en vigueur en vertu du règlement Europol

[109] Application de réseau d'échange sécurisé d'informations (SIENA).

[110] En vertu du règlement Europol modifié, des exceptions à cette interdiction sont prévues pour les agences de l'Union créées en vertu du titre V du TFUE. Toutefois, compte tenu de la base juridique de la proposition (article 114 TFUE, relatif à l'harmonisation du marché intérieur), cette exception n'inclurait pas le centre de l'UE proposé.

modifié et de préciser les modalités d'accès du centre de l'UE. En particulier, tout accès aux données à caractère personnel traitées dans les systèmes d'information d'Europol, lorsqu'il est jugé strictement nécessaire à l'accomplissement des missions du centre de l'UE, ne devrait être accordé qu'au cas par cas, sur demande expresse, qui documente la finalité spécifique et la justification. Europol devrait être tenue d'évaluer ces demandes avec diligence et de ne transmettre des données à caractère personnel au centre de l'UE que lorsque cela est strictement nécessaire et proportionné à la finalité requise.

Article 10, paragraphe 6, sur le rôle d'Europol dans l'information des utilisateurs à la suite de la mise en œuvre d'une injonction de détection

134. L'EDPB et le CEPD se félicitent de l'obligation, prévue à l'article 10, paragraphe 6, de la proposition, que les fournisseurs informent les utilisateurs dont les données à caractère personnel peuvent être concernées par l'exécution d'une injonction de détection. Ces informations ne doivent être fournies aux utilisateurs qu'après avoir obtenu la confirmation d'Europol ou de l'autorité répressive nationale d'un État membre qui a reçu le signalement en vertu de l'article 48 de la proposition que la fourniture d'informations aux utilisateurs ne porterait pas atteinte aux activités de prévention et de détection des abus sexuels commis contre des enfants, ainsi que d'enquêtes et de poursuites en la matière.

135. Toutefois, la mise en œuvre pratique de cette disposition manque de précision. Lorsque les signalements sont transmis à la fois à Europol et à un service répressif d'un État membre, la proposition ne précise pas si une confirmation est requise de la part de l'un ou des deux destinataires, et les procédures/modalités d'obtention de cette confirmation ne sont pas énoncées dans la proposition (par exemple, si les confirmations doivent être transmises par l'intermédiaire du centre de l'UE). Compte tenu du volume élevé de matériel qu'Europol et les autorités répressives nationales pourraient être tenus de traiter, et de l'absence d'un délai précis pour fournir une confirmation («sans retard injustifié»), l'EDPB et le CEPD recommandent de clarifier les procédures applicables afin de garantir la réalisation de cette garantie dans la pratique. Qui plus est, l'obligation d'informer les utilisateurs devrait également inclure des informations sur les destinataires des données à caractère personnel concernées.

Sur la collecte de données et les rapports de transparence (article 83)

136. L'article 83, paragraphe 3, de la proposition prévoit que le centre de l'UE collecte des données et produit des statistiques relatives à un certain nombre de tâches qui lui incombent en vertu du règlement proposé. À des fins de contrôle, l'EDPB et le CEPD recommandent d'ajouter à cette liste des statistiques sur le nombre de signalements transmis à Europol conformément à l'article 48, ainsi que sur le nombre de demandes d'accès reçues par Europol au titre de l'article 46, paragraphe 4, et de l'article 46, paragraphe 5, y compris le nombre de demandes acceptées et refusées par le centre de l'UE.

5. CONCLUSION

137. Si l'EDPB et le CEPD se félicitent des efforts déployés par la Commission pour garantir une action efficace contre les abus sexuels commis contre des enfants en ligne, ils estiment que la proposition soulève de graves préoccupations en matière de protection des données et de respect de la vie privée. Par conséquent, l'EDPB et le CEPD inviteraient les colégislateurs à modifier la proposition de règlement, notamment pour veiller à ce que les obligations de détection envisagées respectent les normes applicables en matière de nécessité et de proportionnalité et n'entraînent pas un

affaiblissement ou une dégradation du chiffrement à un niveau général. L'EDPB et le CEPD restent disponibles pour apporter leur soutien au cours du processus législatif, si leur contribution est jugée nécessaire pour répondre aux préoccupations mises en évidence dans le présent avis conjoint.

Pour le Contrôleur européen de la protection des données	Pour le Comité européen de la protection des données
Le Contrôleur européen de la protection des données	La présidente
	(Andrea Jelinek)
Wojciech Wiewiorowski	