EUROPEAN LAWYERS
EUROPEAN BARS
CCBE
BARREAUX EUROPÉENS
AVOCATS EUROPÉENS

Conseil des barreaux européens
La voix des avocats européens
Rue Joseph II, 40/8 - B-1000 Bruxelles
+32 (0)2 234 65 10 | ccbe@ccbe.eu | www.ccbe.eu

Position du CCBE sur la proposition de règlement établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfants

25/11/2022

Introduction et résumé

Le 11 mai 2022, la Commission européenne a présenté une proposition de règlement établissant des règles en vue de prévenir et de combattre les abus sexuels sur enfants[1]. La proposition prévoit des obligations pour les fournisseurs de services d'hébergement, de services de communication interpersonnelle, de boutiques d'applications logicielles, les fournisseurs d'accès à l'internet et d'autres services pertinents en ce qui concerne la détection, le signalement, la suppression et le blocage de matériels en ligne connus et nouveaux relatifs à des abus sexuel sur des enfants, ainsi que la sollicitation d'enfants (appelée « pédopiégeage »).

Le CCBE considère que les abus sexuels sur les enfants sont des crimes particulièrement graves et odieux et soutient pleinement les objectifs de lutte contre ces crimes et l'adoption de mesures spécifiques pour les prévenir et les combattre. Le CCBE a toutefois de sérieuses inquiétudes, partagées par le Comité européen de protection des données (« EDPB ») et le Contrôleur européen de la protection des données (« CEPD »)[2] quant aux menaces posées par la proposition sur le droit à la vie privée et la protection du secret professionnel.

Le CCBE conclut en particulier que :

- **Les garanties nécessaires pour assurer la protection des droits fondamentaux, y compris la confidentialité des communications, ont été écartées dans la proposition. L'essence même du droit à la confidentialité est sapée par la proposition, qui manque de clarté juridique, en tant que base juridique de l'obligation de détection, et de proportionnalité en ce qui concerne les atteintes et les limitations aux droits fondamentaux.**
- **Les garanties procédurales et la complexité du processus menant à l'adoption d'une injonction de détection ne peuvent pas remplacer les garanties substantielles visant à assurer la confidentialité des communications et la protection du secret professionnel.**
- **Le législateur européen doit adopter des dispositions légales claires et des garanties pour s'assurer que les droits fondamentaux de tous les citoyens sont correctement garantis et bien équilibrés. À cet égard, le CCBE est fortement opposé à l'approche selon laquelle la protection des droits fondamentaux est partiellement ou totalement déléguée à des parties privées.**
- **Les mesures proposées permettant aux fournisseurs de services de détecter et d'identifier des contenus devraient être retirées de la proposition en l'absence de dispositions juridiques claires et de garanties appropriées pour assurer le respect et le bon équilibre des droits fondamentaux des individus.**

[1] COM(2022) 2096 final
[2] Avis conjoint EDPB-EDPS 4/2022 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, 28 juillet 2022, page 5.

- **La proposition ne devrait pas empêcher les avocats de protéger de manière adéquate la confidentialité de leurs communications par des méthodes de chiffrement. Le législateur européen devrait prévoir la protection du « chiffrement de bout en bout » (« E2EE ») et s'assurer que les dispositions de la proposition ne peuvent en aucun cas affaiblir l'E2EE.**
- **La proposition devrait préciser et limiter les circonstances et les objectifs dans lesquels le Centre de l'UE peut transmettre des rapports à Europol. Tout transfert de données à caractère personnel à Europol doit être adéquat, pertinent et limité au strict nécessaire, tout en garantissant la qualité et la fiabilité des données. En outre, l'échange de données à caractère personnel entre le Centre de l'UE et Europol ne devrait avoir lieu qu'au cas par cas, à la suite d'une demande explicite et dûment évaluée.**

I. Obligation de détection

Le CCBE observe que les articles 7 à 10 de la proposition de règlement prévoient une obligation pour les fournisseurs de services d'hébergement et de communication interpersonnelle de détecter le matériel relatif à des abus sexuels sur enfants et les communications de pédopiégeage lorsqu'une autorité judiciaire ou une autorité administrative indépendante a émis une ordonnance de détection dans les conditions prévues aux articles 7 et 8. À cet égard, les fournisseurs doivent utiliser des technologies permettant de détecter la diffusion de matériel relatif à des abus sexuels sur enfants ou les communications de pédopiégeage dans les conditions prévues à l'article 10.

A. La nécessité de garantir le secret professionnel/*legal professional privilege*

1. Une protection spécifique

Le CCBE rappelle que pour que les avocats soient efficaces dans la défense des droits de leurs clients, il doit y avoir une confiance dans la confidentialité de leurs communications. La plupart des systèmes juridiques partagent une compréhension commune du fait que si le droit du citoyen à la préservation de la confidentialité, c'est-à-dire le droit du citoyen à être protégé contre toute divulgation de ses communications avec son avocat, devait être refusé, les personnes pourraient se voir refuser l'accès aux conseils juridiques et à la justice. Le secret professionnel est donc considéré comme un instrument permettant l'accès à la justice et le maintien de l'état de droit.

La Cour européenne des droits de l'homme a, à plusieurs reprises, lié le respect des relations entre avocats et clients au respect des **articles 6 et 8 de la Convention européenne des droits de l'homme**, en déclarant que « *le respect du droit du justiciable à un procès équitable »*[3] *dépend de la « relation de confiance entre [l'avocat et son client]* » et en soulignant à plusieurs reprises que l'atteinte aux relations entre avocats et clients peut violer l'article 8, qui protège le droit au respect de la vie privée et familiale. En effet, l'**article 8 « *accorde une protection renforcée aux échanges entre les avocats et leurs clients* »**. La Cour précise : « *Cela se justifie par le fait que les avocats se voient confier une mission fondamentale dans une société démocratique : la défense des justiciables. Or un avocat ne peut mener à bien cette mission fondamentale s'il n'est pas à même de garantir à ceux dont il assure la défense que leurs échanges demeureront confidentiels* »[4].

[3] CEDH, Michaud c. France (12323/11), 2012, §§117-118
[4] CEDH, Kopp c. Suisse (23224/94), 1998

La protection de la confidentialité des communications entre un avocat et son client a également été reconnue comme un **principe général du droit de l'UE** par la Cour européenne de justice[5] et a une **base juridique dans la Charte des droits fondamentaux de l'UE dans ses articles 7 sur le droit à la vie privée et 47 sur le droit à un procès équitable**.

2. Des atteintes encadrées

Selon l'article 52, paragraphe 1, de la Charte de l'Union européenne, les atteintes aux droits fondamentaux doivent être prévues par la loi, respecter l'essence de ces droits et, sous réserve du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent réellement à des objectifs d'intérêt général reconnus par l'Union ou à la nécessité de protéger les droits et libertés d'autrui. En outre, les droits contenus dans la Charte correspondant aux droits garantis par la CEDH devraient avoir le même sens et la même portée. Ceci s'applique au droit à la confidentialité des communications tel qu'il est garanti par l'article 7 de la Charte et l'article 8 de la CEDH. Le droit protégé par l'article 8 de la CEDH peut faire l'objet d'une atteinte qui doit être conforme à la loi, poursuivre un but légitime et être nécessaire dans une société démocratique pour atteindre l'objectif visé.

Toutefois, comme indiqué ci-dessus, la Cour européenne des droits de l'homme accorde une protection renforcée au titre de l'article 8 de la CEDH aux communications relevant de la protection du secret professionnel. En outre, le CCBE rappelle que si le droit de l'article 8 est peut être limité, le droit à un procès équitable selon l'article 6 de la CEDH est absolu[6] . **Par conséquent, si une communication relevant du secret professionnel entre dans le champ d'application de l'article 6 de la CEDH, compte tenu de la nature absolue de la protection offerte par cet article, il ne devrait alors pas y avoir de possibilité d'autoriser une atteinte**.

À cet égard, il convient de noter que dans les dispositions transitoires du **règlement (UE) 2021/1232**[7], adopté pour modifier la directive « vie privée et communications électroniques »[8] afin de lutter contre le matériel relatif à des abus sexuels sur enfants, dans l'attente de l'adoption de la proposition actuelle, le législateur européen a explicitement prévu une **clause sur la protection du secret professionnel**, considérant que les **règles temporaires visant à détecter les abus sexuels d'enfants en ligne devraient être « *sans préjudice des règles relatives au secret professionnel prévues par le droit national, telles que les règles relatives à la protection des communications professionnelles entre les médecins et leurs patients, entre les journalistes et leurs sources, ou entre les avocats et leurs clients, en particulier puisque la confidentialité des communications entre les avocats et leurs clients est capitale pour garantir l'exercice effectif des droits de la défense, qui constituent un élément essentiel du droit à un procès équitable.* ». Malheureusement, cette clause générale n'a pas été reprise par la Commission européenne dans la nouvelle proposition.

L'analyse suivante de la proposition révèle que les garanties nécessaires pour assurer la protection des droits fondamentaux, y compris la confidentialité des communications, ont été écartées. Le CCBE considère que l'essence même du droit à la confidentialité est sapée par la proposition, qui manque de clarté juridique, en tant que base juridique de l'obligation de détection, et de proportionnalité en ce qui concerne les atteintes et les limitations aux droits fondamentaux.

[5] CJCE, AM&S c. Commission, (155/79), 1982, §18

[6] CEDH, Niemietz c. Allemagne, (13710/88), 1992, §375

[7] Règlement (UE) 2021/1232 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

[8] Directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques)

B. L'absence de garanties suffisantes dans la proposition

1. Les garanties procédurales et le rôle des acteurs privés

Le CCBE note qu'une procédure complexe conduit à l'émission d'une injonction de détection, en commençant par une évaluation des risques effectuée par le fournisseur de services et les mesures d'atténuation possibles. Si un « *risque important* » subsiste, l'autorité publique nationale concernée, appelée autorité de coordination, lance la procédure d'adoption d'une injonction de détection. Avant de demander une telle injonction à l'autorité judiciaire ou administrative compétente, l'autorité de coordination doit échanger avec le fournisseur de services.

Les conditions pour demander l'émission d'une injonction de détection sont définies à l'article 7(4) qui exige l'existence d'un « *risque important »* que le service soit utilisé à des fins d'abus sexuels en ligne sur des enfants. L'évaluation de l'existence d'un tel risque est prévue à l'article 7(5), (6) et (7) pour chaque catégorie d'injonction de détection (concernant la diffusion de matériel connu et nouveau relatif à des abus sexuels sur enfants et le pédopiégeage).

Malgré les dispositions complémentaires de l'article 7(5)-(7), les conditions préalables à l'adoption d'une injonction de détection, reposant sur la démonstration d'un risque important, sont basées sur des concepts larges et vagues, manquant de la clarté juridique nécessaire à la bonne mise en œuvre de la proposition et à l'équilibre des droits en jeu. En effet, l'émission d'une injonction de détection ne nécessite pas de soupçon concret et n'est pas liée à des cas individuels. La détermination d'un « *risque important* » suffit et ce dernier « *est réputé exister* » lorsque « *il est probable* » que le service est utilisé pour la diffusion de matériel relatif à des abus sexuels sur enfants ou pour le pédopiégeage. Comme l'indiquent l'EDPB et le CEPD, des **dispositions aussi vagues et l'incertitude juridique rendent difficile l'application des exigences légales de la proposition de manière prévisible et non arbitraire par les fournisseurs de services concernés et les tribunaux ou les autorités indépendantes délivrant l'injonction, et conduiront à des « *divergences considérables sur la mise en œuvre concrète de la proposition dans l'Union* »**[9] .

Le CCBE est également profondément préoccupé par la participation d'acteurs privés pour identifier, recueillir et transmettre des informations sur le contenu alors qu'ils ne sont soumis à aucune obligation de secret professionnel ni à aucun contrôle démocratique. Comme l'ont fait remarquer les organismes européens de protection des données, les fournisseurs et les autorités ciblés bénéficient d'une large marge d'appréciation dans la mise en balance des droits fondamentaux des personnes. Les fournisseurs de services pourraient par conséquent avoir une influence dans l'ensemble du processus menant à l'émission d'une injonction de détection. Ils doivent procéder à l'évaluation initiale des risques (article 3), adopter des mesures d'atténuation en tenant « *dûment compte* » des « *conséquences potentielles* » sur l'exercice des droits fondamentaux de toutes les parties concernées (article 4), avant de faire rapport et d'interagir avec l'autorité de coordination qui décidera de demander ou non une injonction de détection.

À cet égard, le CCBE fait remarquer que, en ce qui concerne l'évaluation des risques, une liste d'éléments doit être prise en compte par les fournisseurs conformément à l'article 3(2)(a) à (e), tels que ce qui est interdit ou restreint dans leurs conditions générales ; la manière dont les utilisateurs utilisent le service ; la manière dont le service est utilisé ou susceptible d'être utilisé par les enfants ; les tranches d'âge et le risque de sollicitation d'une tranche d'âge ; les fonctionnalités existantes pour établir des contacts. En ce qui concerne les mesures d'atténuation à prendre, l'article 4 exige l'adoption de mesures telles que l'adaptation des systèmes de modération ou de recommandation de contenu du fournisseur.

Cependant, comme l'indiquent l'EDPB et le CEPD, les critères des articles 3 et 4 peuvent sembler pertinents mais laissent une large marge d'interprétation et d'appréciation en utilisant des termes abstraits, vagues et génériques. Le CCBE convient que « ***ces critères ne répondent pas aux critères de sécurité juridique et de***

[9] Avis conjoint EDPB-EDPS 4/2022, §37

prévisibilité nécessaires pour justifier une ingérence dans la confidentialité des communications entre particuliers qui constitue une ingérence manifeste dans les droits fondamentaux à la vie privée et à la liberté d'expression »[10].

Par ailleurs, en ce qui concerne le considérant (17) qui précise que les fournisseurs devraient pouvoir indiquer qu'ils sont disposés et préparés à se voir adresser une injonction de détection pendant la phase de signalement du risque à l'autorité publique compétente, il apparaît que leurs points de vue sur l'adoption éventuelle d'une injonction seront entendus alors qu'il « ***n'est pas imaginable de 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 les plus efficaces, mais les moins intrusives [...]*** »[11]. Ainsi, que les fournisseurs ciblés auront un rôle important dans la mise en balance des droits en jeu, en particulier la confidentialité des communications. Cette implication est assez inquiétante après les récentes fuites de données et les scandales qui ont montré l'incapacité de certains fournisseurs à traiter correctement des contenus très sensibles. Malgré des cadres réglementaires, supposés solides en Europe, de grandes plateformes ont contourné pendant des années la législation sur la protection des données et la vie privée, démontrant l'inefficacité des mécanismes réglementaires pour garantir la confidentialité des communications et la protection des données.

À cet égard, les garanties procédurales et la complexité du processus menant à l'adoption d'une injonction de détection ne sont pas suffisantes et ne peuvent pas remplacer les garanties substantielles[12] visant à assurer la confidentialité des communications et la protection du secret professionnel. En outre, le CCBE est fermement opposé à l'approche selon laquelle la protection des droits fondamentaux est partiellement ou totalement déléguée à des parties privées. Il appartient aux législateurs de l'UE d'adopter des dispositions juridiques et des garanties claires pour s'assurer que les droits fondamentaux de tous les citoyens sont correctement garantis et bien équilibrés.

2. Technologies utilisées pour détecter le matériel relatif à des abus sexuels sur enfants et le pédopiégeage

Conformément à l'article 10 de la proposition, les fournisseurs de services ciblés qui reçoivent une injonction de détection l'exécutent en installant et en exploitant des technologies permettant de détecter la diffusion de matériel connu ou nouveau relatif à des abus sexuels sur enfants ou la sollicitation d'enfants. Ces technologies ne doivent pas être en mesure d'extraire des communications pertinentes d'autres informations que celles strictement nécessaires à la détection, conformément à l'état de la technique dans le secteur et au moins intrusif en ce qui concerne l'incidence sur les droits des utilisateurs à la vie privée et à la confidentialité des communications.

Toutefois, le CCBE note que, comme le soulignent l'EDPB et le CEPD, « *les technologies actuellement disponibles reposent sur le* ***traitement automatisé des données de contenu de tous les utilisateurs concernés*** [...]. *En outre, les technologies actuellement disponibles, en particulier celles qui permettent de détecter le nouveau matériel relatif à des abus sexuels sur enfants ou le pédopiégeage, sont connues pour avoir* ***des taux d'erreur relativement élevés*** *»[13].* Ceci est d'autant plus alarmant que « *les conditions générales pour l'émission d'une injonction de détection en vertu de la proposition, c'est-à-dire l'application à l'ensemble d'un service et pas seulement à des communications sélectionnées, la durée allant jusqu'à 24 mois pour le matériel connu ou nouveau relatif à des abus sexuels sur enfants et jusqu'à 12 mois pour le pédopiégeage, etc. peuvent conduire à une portée très large de l'injonction dans la pratique.* ***En conséquence, la surveillance serait en réalité générale et indiscriminée par nature, et non ciblée en pratique*** *».*

[10] *Ibid*. §27
[11] *Ibid*. §29
[12] *Ibid*. §30
[13] *Ibid*. §52

De même, dans sa précédente analyse d'impact sur les règles temporaires de lutte contre le matériel relatif à des abus sexuels sur enfants et le pédopiégeage du règlement (UE) 2021/1232, le service de recherche du Parlement européen a conclu que « ***les techniques de détection du pédopiégeage basées sur le texte impliquent une analyse automatisée et un balayage sans discernement du contenu des communications et des données de trafic connexes et sont sujettes à des erreurs et vulnérables aux abus. Sans garanties supplémentaires claires et précises, ces technologies ne pourraient pas satisfaire au test de nécessité et de proportionnalité de l'article 52, paragraphe 1, de la Charte*** »[14].

Le CCBE partage les conclusions de l'EDPB-CEPD selon lesquelles « *la proposition pourrait devenir la base d'un balayage de facto généralisé et indiscriminé du contenu de pratiquement tous les types de communications électroniques de tous les utilisateurs dans l'UE/EEE.* ***En conséquence, la législation pourrait conduire les gens à s'abstenir de partager des contenus légaux par crainte d'être ciblés en fonction de leur action*** »[15].

Le CCBE considère que les technologies en cause, ainsi que les conditions de leur utilisation, ne prévoient pas de garanties suffisantes afin d'assurer la protection du secret professionnel et la confidentialité des communications. En s'appliquant à tous les utilisateurs et en opérant une analyse automatisée de toutes les communications, de manière non proportionnée, ces technologies peuvent permettre le repérage et l'interception de communications relevant du secret professionnel partagées par les clients et leurs avocats, entraînant des violations du secret professionnel. **Au-delà de leur manque de proportionnalité, le CCBE souligne que dans tous les cas, les fournisseurs de services devraient être tenus de s'assurer que la technologie qu'ils utilisent garantit qu'il n'y a aucune ingérence dans n'importe quel type de données ou de communications relevant du secret professionnel. Ils doivent être tenus de déployer des moyens technologiques qui garantissent l'impossibilité d'accéder à du contenu protégé par le secret professionnel**.

Compte tenu des développements ci-dessus, le CCBE conclut que les mesures proposées permettant aux fournisseurs de service de détecter et d'identifier des contenus devraient être retirées de la proposition en l'absence de dispositions juridiques claires et de garanties appropriées pour assurer le respect et le bon équilibre des droits fondamentaux des individus.

II. La prévention des tentatives visant à compromettre le chiffrement

Le CCBE note également que, tel que l'ont soulevé l'EDPB et le CEPD, la proposition pourrait avoir une incidence sur l'utilisation du chiffrement de bout en bout (« E2EE »). Le considérant 26 de la proposition indique que les fournisseurs ont le choix des technologies utilisées pour se conformer aux injonctions de détection, ce qui ne doit pas être compris comme une incitation ou une désincitation à l'utilisation d'une technologie donnée, à condition que les technologies et les mesures d'accompagnement répondent aux exigences du règlement proposé, y compris la technologie de chiffrement de bout en bout. Comme l'expliquent l'EDPB et le CEPD, « *la simple éventualité d'une injonction de détection est susceptible de peser lourdement sur les choix techniques des fournisseurs, notamment en raison du délai limité dont ils disposeront pour se conformer à une telle injonction et des lourdes sanctions auxquelles ils s'exposeraient en cas de manquement. En pratique, cela pourrait conduire certains fournisseurs à cesser d'utiliser l'E2EE* ».

En outre, il est étonnant de constater que la **clause sur la protection du chiffrement de bout en bout**, prévue par le règlement (UE) 2021/1232, n'a pas été reprise dans la proposition de la Commission européenne, de même que la clause sur la protection du secret professionnel[16].

[14] Étude 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 – étude d'impact de substitution ciblée, février 2021, page 37.

[15] Avis conjoint EDPB-CEPD 4/2022, §55

[16] Considérant (25) du règlement (UE) 2021/1232 : « *Le chiffrement de bout en bout est un outil important pour garantir la sécurité et la confidentialité des communications des utilisateurs, y compris les communications des enfants. Tout*

Le CCBE considère que la proposition ne devrait pas empêcher les avocats de protéger de manière adéquate la confidentialité de leurs communications par des méthodes de chiffrement. Le CCBE a rappelé la vulnérabilité particulière des avocats aux attaques illégales du gouvernement ou de pirates informatiques privés, en raison du fait qu'ils conservent de manière confidentielle des informations sensibles qui leur sont fournies par leurs clients et qui ne peuvent être divulguées[17]. Une protection cryptographique adéquate est nécessaire. Par conséquent, le CCBE appelle le législateur européen à prévoir la protection de l'E2EE et à s'assurer que les dispositions de la proposition ne peuvent en aucun cas affaiblir l'E2EE.

III. La coopération entre le nouveau Centre de l'UE et Europol

Enfin, le CCBE note que le chapitre IV établit un Centre de l'UE chargé de prévenir et de combattre les abus sexuels sur enfants en tant que nouvelle agence décentralisée pour assurer la mise en œuvre de ses dispositions. Le Centre de l'UE devrait travailler en étroite coopération avec Europol, avec un emplacement partagé, un large accès aux bases de données et aux systèmes d'information. Selon l'article 48, le Centre de l'UE devrait transmettre à Europol et aux autorités nationales compétentes les rapports qui ne sont pas manifestement infondés pour enquêter ou engager des poursuites en cas d'abus sexuel potentiel sur un enfant. De même, l'article 53 exige 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* ».

Le CCBE a précédemment commenté et exprimé ses préoccupations quant aux pouvoirs accordés à Europol dans son nouveau mandat concernant la collecte, le traitement et l'échange de données à caractère personnel. Il a estimé que des dispositions claires et précises devaient régir les justifications de la collecte, du traitement et de l'échange de données à caractère personnel par Europol, qui ne doivent pas contourner les garanties essentielles telles que la nécessité d'une autorisation judiciaire préalable ainsi que le système de contrôle indépendant et impartial. Dans sa position, le CCBE a précisé que tout transfert de données personnelles à des parties privées effectué par Europol doit respecter les garanties essentielles (base juridique claire, nécessité et proportionnalité, contrôle judiciaire indépendant et recours effectifs)[18]. Par ailleurs, comme l'ont soulevé l'EDPB et le CEPD, le mandat d'Europol se limite à soutenir et à renforcer les actions des autorités nationales compétentes et leur coopération mutuelle dans la prévention et la lutte contre la criminalité grave transfrontalière[19], et les organes de l'Union qui fournissent des informations à Europol doivent déterminer la ou les finalités pour lesquelles ces informations doivent être traitées par Europol et dans quelles conditions[20].

Par conséquent, le CCBE considère que la transmission des rapports à Europol ne peut pas avoir lieu de manière générale et automatisée. Le CCBE soutient la recommandation de l'EDPB et du CEPD selon laquelle la proposition devrait préciser et limiter les circonstances et les objectifs dans lesquels le Centre de l'UE peut transmettre des rapports à Europol. Elle devrait également exiger que tout transfert de données à caractère personnel à Europol soit adéquat, pertinent et limité au strict nécessaire, tout en

affaiblissement du chiffrement pourrait potentiellement être exploité de manière abusive par des tiers malveillants. Aucune disposition du présent règlement ne saurait dès lors être interprétée comme une interdiction ou un affaiblissement du chiffrement de bout en bout ».

[17] Recommandations du CCBE sur la protection du secret professionnel dans le cadre des activités de surveillance, p. 20

[18] Position du CCBE sur la proposition de règlement 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, 6 mai 2021.

[19] Règlement (UE) 2016/794, article 3

[20] *Ibid*. article 19

garantissant la qualité et la fiabilité des données[21]. En ce qui concerne l'accès mutuel aux systèmes d'information pertinents entre le Centre de l'UE et Europol, le CCBE constate que la proposition ne précise ni les critères ni les garanties spécifiques permettant un tel accès aux données personnelles hautement sensibles. À cet égard, le CCBE soutient les recommandations de l'EDPB et du CEPD qui considèrent que l'échange de données à caractère personnel entre le Centre de l'UE et Europol ne devrait avoir lieu qu'au cas par cas, à la suite d'une demande explicite et dûment évaluée[22].

[21] Avis conjoint EDPB-CEPD 4/2022, §126

[22] *Ibid*. §§129-133