EXPOSÉ DES MOTIFS

Mesdames, Messieurs,

Le 11 mai dernier, la Commission européenne a présenté une proposition de règlement visant à prévenir et combattre les abus sexuels sur les enfants en ligne. Ce règlement vise à instaurer la possibilité, pour les autorités nationales compétentes, d'émettre des injonctions de détection de contenus pédopornographiques et de « pédopiégeage » (« *grooming* »). Il instituerait en outre un « *centre de l'Union européenne* » autonome, placé auprès d'Europol, chargé de soutenir les États membres et les fournisseurs de services en ligne dans leur lutte contre ces contenus.

Au titre de la commission des affaires européennes, les rapporteurs soutiennent la nécessité d'améliorer la lutte contre la pédopornographie, dont l'ampleur et le caractère transfrontière appellent une réponse européenne plus ferme. Pleinement convaincus par la finalité de cette proposition de règlement, ils observent néanmoins que ses dispositions soulèvent certaines difficultés en matière de protection des droits et libertés fondamentaux, qu'ils ont examinées plus avant et sur lesquelles ils proposent au Sénat de se positionner par le biais d'une résolution.

I. Pourquoi une proposition de règlement pour mieux lutter contre les abus sexuels contre les enfants en ligne ?

A. La diffusion des outils numériques a permis la prolifération des contenus concernant les abus sexuels sur mineurs

Le développement d'Internet dans les dernières décennies a permis une **prolifération de contenus en ligne relatifs à des abus sexuels commis sur mineurs**.

Alors que les abus sexuels et l'exploitation sexuelle des enfants, y compris la pédopornographie, constituent des crimes particulièrement graves, punis dans tous les États membres de l'Union européenne, cette dernière est aujourd'hui **le premier hébergeur de contenus à caractère pédopornographique dans le monde**[1(*)]. Elle est également **l'un des principaux lieux de consultation** de tels contenus : le nombre de signalements d'abus sexuels commis en ligne contre des enfants au sein de l'Union européenne est ainsi passé de 23 000 en 2010 à plus de 725 000 en 2019, impliquant plus de 3 millions d'images et de vidéos.

Pour la France, le rapport annuel pour 2021 de l'association Point de contact recense, pour 2021, 20 081 contenus concernant des « violences sexuelles sur mineurs », représentant plus de 90% des contenus illégaux traités (22 231 au total). Mme Laurence Pécaut-Rivolier, magistrate, membre du collège de l'Autorité de régulation de la communication audiovisuelle et numérique (ARCOM) et personnalité qualifiée chargée de s'assurer du bien-fondé des demandes de retrait de contenus terroristes et pédopornographiques effectuées au titre de l'article 6-1 de la loi de 2004 pour la confiance dans l'économie numérique (LCEN)[2(*)], a évoqué devant les rapporteurs de la commission des affaires européennes un volume de 150 000 contenus terroristes ou pédopornographiques traités en 2021, contre 500 en 1995 (dont environ 70 % de contenus à caractère pédopornographiques).

B. L'Union européenne a mis en oeuvre des outils communs de lutte contre les abus sexuels sur mineurs, qui montrent aujourd'hui leurs limites

La problématique des abus sexuels sur mineurs est inégalement traitée dans les différents États membres. C'est pourquoi le législateur européen a voulu fixer **un cadre de règles minimales afin de mettre fin aux distorsions en la matière : la directive 2011/92/UE[3(*)] définit les infractions liées aux abus sexuels et à l'exploitation sexuelle des enfants, ainsi que celles liées à la pédopornographie et à la sollicitation d'enfants à des fins sexuelles, et demande aux États membres de « *prendre les mesures nécessaires* » pour les punir**.

Concernant plus spécifiquement **la lutte contre la pédopornographie**, elle impose la mise en place par les États membres de **dispositifs permettant la suppression rapide des pages internet** diffusant des contenus à caractère pédopornographique hébergées sur leur territoire et les autorise, de manière subsidiaire, à prendre des mesures de blocage de ces pages[4(*)].

Ces dispositions ont été transposées en France dans la LCEN par une loi de 2014[5(*)], dont l'article 6-1 forme depuis lors le socle de la lutte contre les contenus pédopornographiques en ligne (voir encadré).

La lutte contre les abus sexuels sur mineurs en ligne en France

En France, la pédopornographie est punie de cinq ans d'emprisonnement et de 75.000 euros d'amende[6(*)].

En conséquence, l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) de la police judiciaire, qui gère la ***plateforme de signalement PHAROS***[7](*)*, peut, en application de l'article 6-1 de la LCEN*[8](*)*, demander aux éditeurs et aux hébergeurs en ligne de retirer les contenus pédopornographiques. En cas de non-retrait de ces contenus, l'OCLCTIC peut demander par notification aux fournisseurs d'accès internet (FAI) de bloquer sans délai l'accès à ces contenus, et aux moteurs de recherche ou annuaires de procéder au déréférencement des services hébergeant ces contenus.*

Cette procédure administrative s'exerce sous la surveillance d'une ***personnalité qualifiée indépendante***[9](*)*, chargée de vérifier le bien-fondé des demandes de retrait, et qui a la possibilité d'exercer un recours devant le tribunal administratif contre une demande injustifiée.*

La France bénéficie aussi de l'expertise du ***centre national d'analyse des images pédopornographiques (CNAIP)****, rattaché à la gendarmerie nationale, qui gère une base de données contenant plusieurs dizaines de millions d'images et vidéos à caractère pédopornographique récoltées au cours d'enquêtes menées en France, soutenant le travail des autorités répressives luttant contre les abus sexuels sur mineurs.*

Par ailleurs, **certains fournisseurs de services en ligne ont décidé, sur une base volontaire, de procéder à la détection de contenus pédopornographiques** diffusés sur leurs services et de les retirer, notamment dans le cadre de leur politique interne de modération. En outre, conformément à la loi américaine, ils signalent ces contenus au Centre américain pour les enfants disparus et exploités (NCMEC), qui partage les images pédopornographiques ainsi signalées avec les autorités répressives d'environ 150 pays dans le monde, notamment en Europe[10](*). Lors de son audition, M. Franck Dannerolle, chef de l'OCRVP (Office central pour la répression des violences aux personnes) de la police judiciaire, a indiqué qu'en 2022, la France avait été destinataire de 100 000 signalements de la part du NCMEC.

Au niveau opérationnel, l'agence européenne de coopération policière **Europol dispose de l'une des bases de données les plus importantes au monde sur l'exploitation sexuelle des enfants. L'agence a fait de la lutte contre l'exploitation sexuelle des enfants, contre la production et la diffusion de contenus pédopornographiques en ligne, l'une de ses priorités**. Son unité dédiée, le centre européen de lutte contre la cybercriminalité (EC3), joue ainsi un **rôle clé pour soutenir les enquêtes des services compétents des États membres en matière de pédopornographie,** avec une équipe dédiée (*AP Twins*), disponible en permanence. Ainsi, en 2021, cette équipe dédiée a appuyé 72 opérations, dont le démantèlement, en mai 2021, du site pédopornographique « *Boystown* » qui comptait 400 000 utilisateurs enregistrés.

En outre, depuis 2017, l'agence a souhaité mobiliser le public dans cette lutte par sa campagne *« Stop the child abuse - Trace an object* », qui diffuse en ligne des objets issus de contenus pédopornographiques afin de faciliter l'identification des enfants concernés et leur sauvetage[11](*).

Enfin, entre 2014 et 2020, des actions de collaboration entre Europol et les États membres ont permis l'identification de près de 360 enfants victimes et de 150 auteurs d'abus et le succès de plusieurs enquêtes.

C. Le bilan insuffisant de ces actions justifie des efforts supplémentaires et une adaptation de la réglementation

En premier lieu, **en 2019, l'application de la directive 2011/92/UE demeurait partielle**, incitant la Commission européenne à lancer une procédure d'infraction contre 23 États membres, dont la France.

En deuxième lieu, même si, compte tenu de leur trafic, la contribution des fournisseurs de services en ligne à la lutte contre les contenus pédopornographiques est avérée[12](*), **l'efficacité de leurs actions volontaires de lutte contre ces contenus n'a jamais pu être évaluée avec fiabilité par des tiers**, faute d'accès à leurs données.

Enfin, de manière plus conjoncturelle, la période de confinement résultant de la pandémie de covid-19 a coïncidé avec une **augmentation notable des abus sexuels contre les enfants**, en ligne et hors ligne.

En outre, dans ce contexte, la réforme du code des communications électroniques européen[13](*) intervenue en 2018 impliquait l'**intégration**, à partir du 21 décembre 2020, **des services de communications interpersonnelles non fondées sur la numérotation (courrier électronique, messagerie instantanée, téléphonie par internet)** dans le champ d'application de la directive dite « vie privée et communications électroniques »[14](*), qui garantit la confidentialité des communications et des données relatives au trafic, intégration qui menaçait **la sécurité juridique des actions de détection des contenus illégaux volontairement effectués par les fournisseurs.**

Dans ce contexte, l'Union européenne a adopté, le 24 juillet 2020, une stratégie européenne pour une lutte plus efficace contre les abus sexuels commis contre des enfants. Afin de surmonter la difficulté spécifique posée par l'intégration des services de communications interpersonnelles non fondées sur la numérotation dans

le champ de la directive « *e-privacy* » et de sécuriser les actions volontaires mises en place par les fournisseurs de service, elle a adopté une **réglementation dérogeant temporairement aux dispositions de la directive « vie privée et communications électroniques »**[15](*), permettant aux fournisseurs de détecter et de signaler tout abus sexuel commis contre un enfant en ligne, et de bloquer le compte de l'utilisateur concerné ou de suspendre son accès au service.

Ce règlement intérimaire arrivant à **expiration le 3 août 2024**, la Commission européenne propose, conformément à la stratégie de 2020, l'adoption d'une législation européenne pérenne plus ambitieuse, visant à remplacer les actions volontaires des fournisseurs par des obligations harmonisées. **C'est l'objet du présent projet de règlement soumis à l'examen du Sénat (II).**

Ce texte sera très prochainement complété par une refonte de la directive 2011/92/CE relative à la lutte contre les abus sexuels sur enfants, annoncée dans le programme de travail de la Commission européenne pour 2023 et destinée à renforcer la prévention, les enquêtes et les poursuites en matière d'abus sexuels commis sur des enfants.

II. Le nouveau règlement permettrait d'imposer aux fournisseurs de services en ligne de nouvelles obligations, notamment en matière de détection des contenus concernant des abus sexuels sur les enfants en ligne

La proposition de règlement COM(2022) 209 final **imposerait des obligations précises aux fournisseurs** de services d'hébergement et de services de communications interpersonnelles afin de mieux lutter contre les abus sexuels sur les enfants en ligne (chapitres I à III) et **instituerait un centre de l'Union européenne** en soutien à la lutte contre les contenus pédopornographiques en ligne (chapitre IV).

A. De nouvelles obligations de détection et de retrait des contenus illégaux seraient imposées aux fournisseurs de services en ligne

1. Un dispositif d'évaluation des risques

Le premier changement majeur introduit par la proposition serait d'imposer aux fournisseurs de services en ligne une **obligation d'évaluation régulière des risques d'utilisation de leurs services à des fins d'abus sexuels en ligne sur les enfants**[16](*) **et, si un risque se confirme, une obligation d'atténuation de ce dernier** par des mesures efficaces, ciblées et proportionnées, appliquées avec diligence, telles que l'adaptation du contrôle interne du service, le renforcement de la modération des contenus... Les fournisseurs seraient tenus de faire rapport sur les risques identifiés et les mesures d'atténuation prises aux autorités de contrôle compétentes de l'État membre concerné[17](*) (articles 3 à 5).

Les fournisseurs devraient prendre **des mesures spécifiques de vérification permettant l'identification des enfants utilisateurs**, si un risque de « pédopiégeage » (c'est-à-dire, de sollicitation d'un enfant par un adulte à des fins d'acte sexuel) était spécifiquement repéré (article 4)[18](*).

2. Des dispositifs d'injonction obligeant les fournisseurs de services à détecter et à retirer les contenus pédopornographiques

En outre, la proposition introduit pour les fournisseurs, sous certaines conditions, des **obligations de détection** des abus sexuels sur enfants en ligne, **de signalement** de tout abus sexuel potentiel et **de retrait** du « matériel » identifié (sections 3 à 5 ; articles 7 à 15) ; en cas de non mise en conformité, les autorités de l'État membre compétent se verraient reconnaître le pouvoir de demander aux fournisseurs d'accès à internet (FAI) le blocage des sites contrevenants (art. 16 à 24).

Concrètement, l'obligation de détection se traduirait par l'**émission d'une injonction par l'autorité judicaire ou l'autorité administrative indépendante compétente**, sur demande d'une « autorité de coordination pour les questions relatives aux abus sexuels sur enfants »[19](*). L'autorité de coordination disposerait de **pouvoirs d'enquête et de coercition** auprès des fournisseurs[20](*) (articles 27 à 32).

Cette demande d'injonction de détection devrait être précédée des enquêtes nécessaires et d'une analyse d'impact (en cas de première demande) et permettre au fournisseur visé ainsi qu'au « centre de l'Union européenne chargé de prévenir et de combattre les abus sexuels sur enfants » qui serait créé, de formuler leurs observations.

Il reviendrait ensuite à l'autorité de coordination nationale ayant demandé l'injonction de solliciter du fournisseur un plan de mise en oeuvre de cette demande, et, si cette dernière concerne des contenus de « pédopiégeage », un avis de l'autorité nationale en charge de la protection des données à caractère personnel, puis de transmettre sa demande à l'autorité judiciaire ou administrative indépendante en capacité d'émettre l'injonction, avec l'ensemble des documents recueillis (plan, avis et observations). Cette dernière en évaluerait

la pertinence, au regard de plusieurs critères mentionnés dans la proposition (notamment la probabilité d'une utilisation du service pour la diffusion de matériel relatif à des abus sexuels sur les enfants, l'existence d'éléments probants indiquant que le service ou un service comparable a été utilisé à ces fins dans les 12 derniers mois, etc. ; art. 7).

Les modalités de mise en oeuvre d'une telle injonction devraient respecter plusieurs conditions procédurales, notamment une période d'application maximale de 24 mois (12 mois concernant la sollicitation d'enfants), la nécessité d'un contrôle humain régulier (articles 7 à 11)[21](*).

Le retrait de contenus et le blocage de l'accès à un service internet seraient également déclenchés par une injonction, obéissant aux mêmes modalités, l'injonction de retrait devant toutefois faire l'objet d'une « évaluation diligente » préalable par l'autorité de coordination, et le fournisseur qui en serait saisi devrait l'exécuter **« dès que possible », et au plus tard dans les 24 heures suivant sa réception**. La période d'application d'une injonction de blocage, quant à elle, ne devrait **pas dépasser un an**.

En outre, tout fournisseur constatant la présence sur son service de contenus relatifs à des abus sexuels sur les enfants en ligne devrait le signaler au nouveau centre de l'Union européenne (art. 12 et 13), à charge pour ce dernier de traiter ce signalement et, si ce dernier n'est pas dénué de fondement, de le transmettre à Europol et aux autorités répressives compétentes de l'État membre concerné. En outre, le centre tiendrait à jour une base de données de ces signalements (articles 45 et 48).

3. La proposition demeure peu ambitieuse sur les droits des victimes

La proposition se contente de rappeler le droit des victimes d'abus sexuels à être informées, à leur demande, sur le « matériel » relatif à des abus sexuels en ligne sur lequel elles apparaissent et qui aurait fait l'objet d'un signalement, ainsi que leur **droit d'être assistées dans leurs demandes de retrait de tels contenus** par les fournisseurs et par le centre de l'Union européenne. Leurs demandes devraient être formulées auprès de l'autorité de coordination compétente (articles 20 et 21).

Cette prudence, que l'on peut déplorer, est sans doute liée au fait que la Commission européenne souhaite réserver de nouvelles mesures en faveur des victimes à la refonte prochaine de la directive 2011/92/UE, qui devrait intervenir cette année.

B. La création d'un centre européen dédié à la prévention et à la lutte contre les abus sexuels sur les enfants

La proposition de règlement instituerait un **« *centre de l'Union européenne chargé de prévenir et de combattre les abus sexuels sur enfants* »**, qui serait un organisme de l'Union européenne doté de la personnalité juridique. Il siégerait à La Haye aux Pays-Bas, pour travailler à proximité de l'agence Europol, installée sur place (chapitres IV et V ; articles 40 à 84).

Ce centre aurait pour principales missions :

- la réception des signalements de contenus pédopornographiques transmis par les fournisseurs et leur « filtrage », avant classement sans suite ou envoi aux services répressifs compétents pour mener les investigations à leur sujet ;

- la contribution aux processus de détection et de retrait (formulation d'avis sur les injonctions de détection ; réception des injonctions de retrait et de blocage...) en soutien aux autorités compétentes des États membres et à Europol (mise en place d'un système de partage d'informations fiables...) ;

- la création et la mise à jour de bases de données sur les indicateurs pertinents pour détecter des abus sexuels en ligne et sur les signalements, et leur mise à disposition des fournisseurs et des autorités compétentes ;

- l'établissement d'une liste de technologies pouvant être utilisées par les fournisseurs pour détecter ou retirer des contenus et leur mise à disposition de ces derniers ;

- une activité de recherches et d'études.

En pratique, le centre serait dirigé par un directeur exécutif, nommé pour cinq ans (articles 64 et 65), épaulé par un conseil d'administration[22](*), qui définirait les orientations générales des actions du centre (articles 56 et 57), et par un conseil exécutif[23](*) (articles 61 et 62), chargé de la bonne exécution des missions. Le centre partagerait cependant ses fonctions administratives avec Europol « y compris les fonctions liées à la gestion du personnel, aux technologies de l'information et à l'exécution du budget. » (article 53).

III. La position de la commission des affaires européennes du Sénat

Les rapporteurs de la commission des affaires européennes souhaitent avant tout souligner leur **soutien de principe à une réforme visant une meilleure coordination européenne pour éradiquer les abus sexuels sur les enfants en ligne.** Ainsi qu'indiqué précédemment, **les signalements effectués volontairement par les**

fournisseurs de services en ligne aux autorités répressives ont à plusieurs reprises permis d'appréhender des pédocriminels, voire de démanteler des réseaux, ainsi que l'a notamment confirmé aux rapporteurs de la commission des affaires européennes M. Franck Dannerolle.

Néanmoins, trois points particuliers ont retenu leur attention :

- les risques d'atteintes à la vie privée, notamment dans le champ des communications interpersonnelles ;

- le risque de perte d'efficacité qui pourrait être généré par le nouveau système, et notamment le risque d'un « trop-plein » de signalements qui risquerait de compliquer le travail des autorités répressives ;

- la plus-value incertaine apportée par le nouveau centre créé par le règlement.

A. Le fort risque d'atteinte aux droits et libertés fondamentales, notamment en matière de protection de la vie privée, nécessite une réduction du champ d'application de l'injonction de détection et la mise en place de garanties fermes

1. L'introduction d'une dérogation généralisée au principe de confidentialité des communications

Ainsi que précisé antérieurement, **la proposition de règlement concerne tant les contenus publics (à l'exemple de ceux présents et librement accessibles sur les réseaux sociaux) que les contenus de communications interpersonnelles**, tels que les courriels, les boucles de messageries privées et la téléphonie en ligne - les contenus audio étant également explicitement inclus. L'application d'injonctions de détection ne pourrait donc se faire que par dérogation à la directive de 2002 sur la confidentialité des communications précitée (actuellement en cours de révision), qui garantit la confidentialité des communications interpersonnelles et, partant, le droit à la vie privée, tel que protégé par la Charte (art. 7).

La directive admet certes que les États membres puissent adopter, au titre d'un objectif d'intérêt général, des mesures législatives, nécessaires, appropriées et proportionnées, visant à limiter la confidentialité des communications, afin d'assurer la prévention, la recherche, la détection et la poursuite des infractions pénales qui en résultent. Mais en l'espèce, la proposition de règlement introduirait une dérogation généralisée au principe de confidentialité des communications.

Ce qui serait paradoxal, à l'heure où la Cour de justice de l'Union européenne (CJUE) et la Cour européenne des droits de l'Homme (CEDH) développent une approche restrictive des exceptions à ce principe[24(*)].

En outre, techniquement, **les recherches de contenus envisagées seraient impossibles sur des ensembles de contenus faisant l'objet de chiffrements de bout en bout**. En pratique, afin d'être en mesure de se conformer au règlement, les fournisseurs de services de communication interpersonnelle cryptés devraient renoncer, partiellement ou en partie, au chiffrement des contenus, ce qui comporterait des **risques pour la confidentialité des communications et la sécurité**.

2. Une possible atteinte à l'interdiction de surveillance généralisée des contenus

En ce qui concerne les contenus publics - tels que ceux présents, en particulier, sur les plateformes de réseaux sociaux - , la possibilité d'émettre des injonctions de détection des contenus pédopornographiques ou de pédopiégeage est une **atteinte manifeste à l'interdiction de surveillance généralisée des contenus**, posée par la directive sur le commerce électronique de 2000, et réaffirmée récemment dans le *Digital Services Act*. Ce risque a été souligné par les représentants de la commission nationale informatique et libertés (CNIL) lors de leur audition par les rapporteurs, au cours de laquelle ils ont précisé que la proposition rendait possible une analyse généralisée et systématique du contenu de quasiment tout type de communication électronique.

Si des exceptions à ce principe existent, notamment pour la recherche de contenus sous droits d'auteur, aux termes de la directive sur les droits voisins de 2019[25(*)], elles demeurent pour l'instant ciblées, et limitées à la recherche de contenus déjà connus[26(*)]. Ainsi, **la recherche de contenus déjà identifiés**, comme le permet la technique du « hachage » (empreinte numérique attribuée à une image ou à une vidéo, permettant de les retrouver facilement), **ne paraît pas soulever de difficulté**.

En revanche, la recherche de nouveaux contenus *via* des logiciels d'intelligence artificielle paraît plus discutable, en particulier au regard des **faibles performances des logiciels d'intelligence artificielle** (IA) aujourd'hui disponibles. Selon un chiffre cité par la Commission européenne elle-même dans son étude d'impact, les technologies d'IA actuellement disponibles sur le marché[27(*)] génèreraient environ 12 % de faux positifs pour la détection de nouveaux contenus. Ainsi, un nombre considérable de contenus parfaitement légaux pourraient être portés à la connaissance des autorités de contrôle, au **risque d'affecter la liberté d'expression, y compris dans l'espace public**.

Les **risques de « sur censure »**, qui n'apporteraient rien à la lutte contre les abus sexuels contre les enfants, doivent également être pris en compte, lorsque serait confiée à des acteurs privés une détection de contenus

dont il n'est pas certain que les autorités de contrôle auraient les moyens techniques et humains de vérifier les paramètres.

En outre, en ce qui concerne le « **pédopiégeage** », l'analyse et la qualification des conversations incriminées ne pourraient reposer que sur un recoupement de leur contenu avec des données à caractère personnel (qu'elles soient fournies directement par l'utilisateur ou déduites, par exemple, des contenus qu'il a publiés ou consultés ou du profil de ses cercles d'« amis » sur les réseaux sociaux). En effet, le contenu en cause n'est, dans la majeure partie des cas, pas suffisant pour qualifier des pratiques de « pédopiégeage », ainsi que l'ont confirmé aux rapporteurs, notamment, les représentants de la CNIL. Ces derniers ont relevé que le comité européen de protection des données (EDPB), qui réunit les homologues de la CNIL dans les différents États membres, avait particulièrement pointé les faibles performances de l'intelligence artificielle pour la détection du pédopiégeage, et ses risques pour la protection des données à caractère personnel. Or, **les garanties apportées par la proposition pour éviter de déclencher une injonction de détection (évaluation et atténuation des risques par les fournisseurs), et limiter l'utilisation des données à caractère personnel** une fois cette injonction émise (art. 10, 3 c) et 4 a) et b)), parais**sent insuffisantes au regard du risque de « chalutage généralisé » des données par les fournisseurs que pourrait ouvrir une telle réglementation**.

Elles se bornent en effet à indiquer que les technologies utilisées doivent être « conformes à l'état de la technique dans le secteur et [...] les moins intrusives 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 » et que ces dernières ne doivent être traitées que dans le but de satisfaire aux obligations du règlement.

Simultanément, si **les efforts d'harmonisation des conditions de lutte contre les abus sexuels en ligne au niveau européen sont bienvenus**, force est de constater que la procédure de détection, basée sur une série de consultations et scindée en deux étapes menées par des autorités distinctes (demande de l'injonction de détection ; émission de l'injonction de détection), se déroulerait sur une longue durée (plusieurs semaines voire plusieurs mois). La longueur d'une telle procédure vise à permettre d'analyser la nécessité de la détection envisagée, mais également parce que cette procédure d'injonction de détection est conçue principalement comme un mécanisme incitatif à l'égard des fournisseurs.

Ainsi, en raison de cette complexité procédurale et de l'absence de fiabilité des technologies d'intelligence artificielle qui seraient utilisées, **ces injonctions de détection ne constitueraient pas un gage d'efficacité accrue de la lutte contre la diffusion d'abus sexuels en ligne sur les enfants**. À l'évidence, au regard des principes de confidentialité des communications et de protection de la vie privée, le dispositif envisagé ne respecterait pas le principe de proportionnalité.

C'est pourquoi vos rapporteurs demandent la suppression des dispositions de la proposition de règlement autorisant, sur émission d'une injonction de détection, la recherche indifférenciée de contenus pédopornographiques et de « pédopiégeage » dans les services de communications interpersonnelles, face à un risque de surveillance de masse des communications.

Ce faisant, loin d'affaiblir cette proposition de règlement qui harmoniserait la réponse européenne contre les abus sexuels sur les enfants, ce choix la sécuriserait juridiquement.

En tout état de cause, les rapporteurs proposent d'entourer les injonctions de détection de garanties supplémentaires, à savoir :

- que les autorités nationales compétentes **évaluent en détail les risques** posés par l'utilisation des services en ligne concernés, en tenant dûment compte des mesures d'atténuation prises par ces derniers, avant d'envisager des injonctions de détection de contenu, afin de limiter ces dernières au strict nécessaire, à due proportion des risques détectés. Pour ce faire, il est indispensable que ces autorités de contrôle soient dotées de moyens financiers et humains leur permettant d'exercer ces missions, et qu'elles aient **accès aux données pertinentes des fournisseurs de service en ligne** ;

- que soit renforcé le **rôle de contrôle du comité européen de la protection des données (EDPB) et des autorités nationales de protection des données** dans l'établissement de lignes directrices concernant les injonctions de détection, mais aussi dans l'établissement d'une liste des technologies mises à disposition des fournisseurs ; et que soit soutenu, pour ces technologies, le principe de **protection des données dès la conception et par défaut** ;

- que les pouvoirs publics soient soutenus dans la mise au point de tels outils de détection fiables.

Simultanément, afin de renforcer les outils à la disposition des autorités compétentes et de « donner toutes ses chances » à la présente réglementation en s'inspirant des succès de la loi française, il semble cohérent

d'**intégrer les moteurs de recherche et annuaires** dans le champ d'application du règlement, afin de pouvoir, en plus du blocage de sites contrevenants, prévoir des **injonctions de déréférencement** de contenus illégaux ; les rapporteurs de la commission des affaires européennes souhaitent donc que les discussions en cours au Conseil à ce sujet aboutissent.

A. Une exigence supplémentaire : tirer le meilleur de l'exemple PHAROS

La procédure d'injonction devrait être complétée par des réponses souples des autorités compétentes en matière de traitement des signalements et de retrait des contenus pédopornographiques.

À cet égard, le **système français**, qui repose sur la plateforme PHAROS, est **jugé très efficace** par nos partenaires européens. Aussi, ~~ils~~ les rapporteurs recommandent de **prendre exemple sur son fonctionnement**, ou à tout le moins de prendre garde, dans la rédaction du futur règlement, à **permettre à PHAROS de conserver son rôle pivot** dans le retrait des contenus de pédopornographie et leur transmission, en tant que de besoin, aux services répressifs compétents.

La plateforme PHAROS

Créée en 2009, la plateforme PHAROS reçoit des signalements concernant les contenus illégaux sur internet, qui peuvent émaner de tout citoyen (anonymement ou non), via *le formulaire en ligne de la plateforme. PHAROS sert de relais pour demander, après évaluation du bien-fondé de la demande, le retrait de ces contenus aux hébergeurs de services en ligne concernés, l'article 6-1 de la LCEN précitée lui ayant donné un pouvoir d'injonction de retrait (et le cas échéant de blocage ou déréférencement) à l'égard des contenus pédopornographiques et terroristes. Le retrait doit intervenir sous 24 heures maximum.*

Elle oriente par ailleurs les signalements qui ressortissent de la criminalité aux services répressifs compétents, en France ou à l'étranger, via *Europol ou Interpol.*

Sa compétence se limite aux contenus publics, à l'exclusion des communications privées.

L'équipe de PHAROS est constituée d'une cinquantaine de personnes, membres des forces de police et de gendarmerie.

Les représentants de la plateforme PHAROS, que vos rapporteurs ont auditionnés, ont souligné que les signalements effectués actuellement par les utilisateurs ou les fournisseurs de services en ligne sur une base volontaire constituaient déjà un **volume important de signalements, en croissance constante**.

Il conviendra alors, dans la mise en oeuvre du règlement, de **calibrer les injonctions afin que les services répressifs, ou avant eux PHAROS, ne soient pas « noyés » sous des signalements non significatifs ou non exploitables**, en particulier du fait des faibles performances des logiciels employés. Le rôle de « filtrage », que la proposition de règlement confie en l'état au nouveau centre de l'Union européenne qu'elle crée, semble néanmoins limiter ce risque. Par ailleurs les rapporteurs **saluent la mise en place de capacités de détection et de traitement proprement européennes**, alors que les services répressifs français et européens travaillent pour l'instant dans une large mesure sur la base des signalements effectués par le Centre américain pour les enfants disparus et exploités (NCMEC).

En outre, les rapporteurs observent que la plateforme **PHAROS**, composée de personnels sous tutelle du ministère de l'intérieur, **ne constitue pas une autorité administrative indépendante au sens de la proposition de règlement**, et ne pourrait donc, dans la rédaction initiale de ce dernier, disposer du pouvoir d'émettre des injonctions de retrait, dans les conditions prévues à l'article 14 du règlement ; il convient toutefois, au vu de son efficacité unanimement saluée, de préserver le rôle central de cette plateforme dans la lutte contre les contenus de pédopornographie en ligne. Par conséquent, les rapporteurs de la commission des affaires européennes soutiennent les démarches du Gouvernement pour considérer la plateforme comme l'une des « autorités nationales compétentes » habilitées à mettre en oeuvre la présente réglementation, au sens de son article 25.

Plus largement, vos rapporteurs souhaitent insister sur la nécessité de **renforcer considérablement les capacités des services de police et de justice**, afin de donner suite aux signalements qui seront ainsi permis et, ce faisant, de permettre non seulement l'assainissement de l'espace public en ligne, mais également la neutralisation des pédocriminels.

C. Un centre de l'Union européenne dont la nécessité n'apparaît pas évidente

Le nouveau centre de l'Union européenne envisagé pour faciliter les efforts de prévention et de lutte contre les abus sexuels sur les enfants, se placerait en intermédiaire entre les fournisseurs et les services répressifs pour le traitement des signalements pédopornographiques, avec un rôle de traitement et, plus généralement, une

mission affichée de « facilitateur » entre ces acteurs. De fait, il est surtout attendu de ce centre qu'il « filtre » les signalements pertinents parmi la masse de ceux qui lui seront transmis, afin que cette tâche ne vienne pas encombrer l'action des services répressifs.

Cependant, son intervention **allongerait *de facto* les échanges entre ces acteurs**, tout comme ses avis préalables étireraient la procédure d'injonctions de détection. Ce qui est évidemment préjudiciable dans des situations où les jours, parfois, les heures, comptent.

Quant aux missions prévues de production d'indicateurs, d'établissement d'une liste de « technologies » neutres pouvant être utilisées par les fournisseurs et de soutien aux victimes dans leurs demandes de retrait de contenus pédopornographiques les concernant, elles ne semblent pas nécessiter une **nouvelle structure coûteuse**. Doté d'une centaine d'agents, ce centre, qui bénéficierait de l'autonomie juridique, aurait en effet un **coût de fonctionnement évalué à plus de 28 millions d'euros annuels** par la Commission européenne, alors même qu'il partagerait ses fonctions administratives, « y compris les fonctions liées à la gestion du personnel, aux technologies de l'information et à l'exécution du budget », avec l'agence européenne de coopération policière, Europol. Ce partage des fonctions « support » avec Europol invalide l'argument avancé par certaines personnes auditionnées par les rapporteurs pour justifier la création d'un centre *ad hoc* , à savoir la nécessaire indépendance de ce centre afin de garantir la proportionnalité des mesures prévues pour le traitement des signalements.

D'autres éléments constitutifs de cette structure soulignent en réalité sa dépendance à l'égard d'Europol et de la Commission européenne : en effet, le centre et Europol s'accorderaient *«* mutuellement un accès aussi large que possible aux informations et systèmes d'information pertinents ». Le directeur exécutif du centre serait nommé sur proposition de la Commission européenne et cette dernière serait également chargée de l'évaluation de son action dans les six mois précédant la fin de son mandat.

En réalité, **l'Union européenne dispose déjà d'une agence opérationnelle permettant de coordonner les actions de prévention et de lutte contre les abus sexuels sur les enfants, à savoir Europol**.

Ainsi les rapporteurs de la commission des affaires européennes suggèrent de renoncer à la création envisagée d'un centre dédié et de transfert les missions qu'il était prévu de lui confier à Europol qui pourrait créer en son sein un pôle dédié, à condition que ses moyens soient augmentés à due proportion.

D. La lutte contre les abus sexuels en ligne sur mineurs devrait inclure une forte dimension préventive, en complément du volet répressif

1. Améliorer la responsabilité des acteurs du numérique

Dans la ligne des précédents travaux de la commission des affaires européennes, notamment sur le règlement européen sur les services numériques, les rapporteurs de la commission des affaires européennes souhaitent souligner le **rôle déterminant joué par le modèle économique des plateformes en ligne dans la prolifération des contenus préjudiciables aux mineurs**. Ils déplorent, à ce titre, que l'article 19 de la proposition réaffirme le régime de responsabilité limitée des hébergeurs, en disposant que **les fournisseurs de services en lignes ne pourront être tenus pour « responsables d'infractions sexuelles contre des enfants au seul motif qu'ils exercent, de bonne fois, les activités nécessaires pour se conformer aux exigences du règlement ».**

Ils s'interrogent en outre sur l'opportunité de confier, une fois de plus, le contrôle de l'espace public en ligne aux acteurs privés du numérique : sans méconnaître la réelle efficacité de certaines initiatives prises, y compris par les GAFAM, en matière de lutte contre les contenus pédopornographiques, il est en effet indispensable de reconnaître que **l'assainissement de l'espace public - et *a fortiori* privé - en ligne ne pourra constituer pour eux un objectif que tant qu'il est compatible avec leurs propres objectifs de rentabilité**. Il est ainsi crucial que les autorités nationales et européennes soient en mesure de faire pression sur ces acteurs privés, *via* une règlementation contraignante, assortie de la possibilité de sanctionner leurs lacunes dans la lutte contre les contenus pédopornographiques (et de manière plus large, les autres contenus illégaux et préjudiciables)[28(*)].

Pour ce faire, il est **indispensable que les autorités de régulation soient en mesure de pouvoir auditer ces services elles-mêmes, ou puissent confier de tels audits à des chercheurs qualifiés et indépendants de ces acteurs privés**. Cela suppose le renforcement de leurs moyens humains et financiers, mais également le renforcement de l'obligation d'ouverture des données des fournisseurs de services numériques à ces auditeurs ou chercheurs, ainsi que le Sénat le demandait déjà dans sa résolution du 14 janvier 2022 sur le règlement européen sur les services numériques[29(*)].

De telles capacités d'audit externe permettraient en outre à ces autorités de régulation, ou à la Commission européenne elle-même, de rendre publics, si nécessaire, les éventuels manquements des fournisseurs à leurs obligations au titre du règlement, dans une **logique de « *name and shame* »** qui pourrait, à terme, permettre de détourner utilisateurs et surtout annonceurs publicitaires de ces services, en jouant sur le **risque réputationnel**.

2. Renforcer le volet préventif pour protéger les enfants dans l'espace numérique

Enfin, dans la ligne des travaux réalisés récemment par d'autres instances du Sénat[30(*)], les rapporteurs de la commission des affaires européennes souhaitent rappeler l'importance de **développer des méthodes alternatives de protection des enfants en ligne reposant sur un renforcement des mesures d'éducation aux usages du numérique**, ainsi que sur les **dispositifs de contrôle parental et de contrôle de l'âge en ligne respectueux de la vie privée**.

À ce titre, il semblerait par exemple pertinent d'**obliger les très grandes plateformes à mettre en oeuvre sur les services, à leurs frais, des campagnes de communication visant à rappeler à leurs utilisateurs la réglementation applicable en matière de contenus pédopornographiques**.

Les rapporteurs rappellent également la recommandation, faite dans le cadre de la résolution n° 70 (2021-2022) du 14 janvier 2022 précitée, de prévoir un **droit à l'oubli renforcé pour les mineurs**, pour les contenus les concernant diffusés sur les très grandes plateformes.

LISTE DES PERSONNES ENTENDUES OU AYANT TRANSMIS DES ÉLÉMENTS D'INFORMATION

Instances européennes

Parlement européen

- M. Patrick BREYER, député européen (ALL - Verts)

Europol (réponses écrites)

Services de l'État

Ministère de l'Intérieur

- M. Jean MAFART, directeur des affaires européennes et des affaires internationales

- M. Frank DANNEROLLE, chef de l'OCRVP (Office central pour la répression des violences aux personnes)

- Mme Marine CORGIÉ, chargée de mission, direction des affaires européennes et des affaires internationales

Plateforme PHAROS

- Commandant Jean-Baptiste BALDO, chef de service

- Mme Mélanie MARIE, chargée de mission, section des négociations européennes de la division des relations internationales de la Direction Centrale de la Police Judiciaire.

Autorités de régulation et agence de l'État

Autorité de régulation de la communication audiovisuelle et numérique

- M. Roch-Olivier MAISTRE, président

- Mme Laurence PÉCAUT-RIVOLIER, membre du collège, personnalité qualifiée chargée de s'assurer du bien-fondé des demandes de retrait de contenus terroristes et pédopornographiques

- M. Guillaume BLANCHOT, directeur général

Commission nationale Informatique et Libertés (CNIL)

- M. Bertrand PAILHES, directeur des technologies et de l'innovation

- M. Armand HESLOT, chef du service de l'expertise technologique

- Mme Ashanti EGEA, juriste au service des affaires économiques

- Mme Chirine BERRICHI, conseillère pour les questions parlementaires et institutionnelles

- Entreprises (réponses écrites)

- Google France (réponses écrites)

- Meta (réponses écrites)

- [sollicité, TikTok n'a pas apporté de réponse]

* [1] Exposé des motifs de la communication de la Commission européenne COM(2020) 607 final du 24 juillet 2020 valant « Stratégie de l'Union européenne en faveur d'une lutte plus efficace contre les abus sexuels commis contre des enfants ».

* [2] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

* [3] Directive 2011/92/CE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil. Il faut également signaler la directive 2012/29/CE du 25 octobre 2012 qui établit des normes minimales concernant les droits, le soutien et la protection des victimes de la criminalité.

* [4] Article 25 de la directive.

* [5] Loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme.

* [6] Article 227-23 du code pénal.

* [7] Plateforme d'Harmonisation, d'Analyse, de Recoupement et d'Orientation des Signalements.

* [8] Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

* [9] Initialement placée auprès de la Commission nationale Informatique et Libertés (CNIL), cette personnalité siège, depuis le 7 juin 2022, auprès de l'ARCOM.

* [10] L'article 18 du récent règlement sur les services numériques (règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE) enjoint à tout fournisseur de services d'hébergement d'informer promptement les autorités répressives ou judiciaires de l'État membre compétent lorsqu'il a connaissance d'informations « conduisant à soupçonner qu'une infraction pénale présentant une menace pour la vie ou la sécurité d'une ou plusieurs personnes a été commise [...] ou est susceptible d'être commise ».

* [11] Au 1er juillet 2021, cette campagne avait permis d'identifier et de sauver 23 enfants et de poursuivre cinq pédocriminels, après identification.

* [12] À titre d'exemple, l'analyse d'impact de la proposition de règlement souligne que la société Facebook était, en 2020, à l'origine de 95% des signalements d'abus sexuels commis contre des enfants au centre national sur les enfants disparus et exploités des États-Unis.

* [13] Directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen.

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

* [15] 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 impersonnelles 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.

* [16] La première évaluation devrait être effectuée dans les trois mois de l'entrée en vigueur du présent texte. Les suivantes devraient être établies tous les trois ans.

* [17] Qui, conformément au principe du pays d'origine, est l'État membre d'établissement du service.

* [18] Signalons en complément que le nouveau règlement sur les services numériques ou « DSA » (règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE), impose aux fournisseurs de « très grandes plateformes en ligne » d'évaluer spécifiquement les risques systémiques présentés par l'utilisation de leurs services notamment en matière de diffusion de contenus illicites, et tout effet négatif réel ou prévisible pour l'exercice des droits fondamentaux, notamment ceux relatifs aux droits de l'enfant consacrés à l'article 24 de la Charte ; il fait également, plus largement, obligation à tout fournisseur de service en ligne de retirer « promptement » tout contenu illicite dès qu'il en a connaissance, sous peine de voir sa responsabilité engagée. Une procédure nouvelle de notification doit en outre faciliter le signalement de tels contenus par les utilisateurs.

* [19] La désignation de l'une et de l'autre relevant des compétences de l'État membre compétent.

* [20] Par exemple : possibilité d'inspecter les locaux d'un fournisseur ; pouvoir d'ordonner la cessation des infractions constatées, d'infliger des amendes, ou de demander aux juridictions compétentes, la restriction temporaire de l'accès des utilisateurs au service concerné ; pouvoir de notification à un fournisseur afin d'obtenir le retrait de contenus.

* [21] Plusieurs garanties sont prévues au profit des fournisseurs de service en ligne qui seraient dans l'impossibilité technique ou opérationnelle de mettre en oeuvre une injonction de détection, de retrait ou d'injonction (art. 8, 14 ou 17).

* [22] Le conseil d'administration serait composé d'un représentant par État membre et de deux représentants de la Commission européenne disposant du droit de vote. Il comprendrait également un expert désigné par le Parlement européen et un représentant d'Europol, avec voix consultative.

* [23] Le conseil exécutif serait composé du président et du vice-président du conseil d'administration, de deux autres membres du conseil d'administration disposant du droit de vote et des deux représentants de la Commission européenne y siégeant. Le président du conseil d'administration serait aussi celui du conseil exécutif.

* [24] À titre d'exemple, la CJUE interdit désormais toute conservation généralisée et indifférenciée, à titre préventif, des données de trafic et de localisation au nom de la lutte contre la criminalité grave (CJUE, La Quadrature du Net, *French data network* et autres contre Premier ministre, Garde des Sceaux et autres, C-511/18, C-512/18 et C-520/18 du 6 octobre 2020).

* [25] Directive (UE) 2019/790 du Parlement européen et du Conseil du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique et modifiant les directives 96/9/CE et 2001/29/CE.

* [26] La CJUE a approuvé les dispositions de cette directive, notamment parce que l'obligation de détection ne s'applique qu'aux contenus qui ont été signalés par les ayant-droits.

* [27] En l'occurrence la technologie d'IA du « Projet Artemis » de Microsoft.

* [28] La résolution n° 70 (2021-2022) du 14 janvier 2022 sur la proposition de règlement du Parlement européen et du Conseil relatif à un marché intérieur des services numériques (Législation sur les services numériques - *Digital Services Act* - DSA) et modifiant la directive 2000/31/CE, COM(2020) 825 final recommandait notamment de faire apparaître dans les évaluations des risques systémiques devant être faites par les très grandes plateformes une section spécifique aux risques concernant les enfants, en tenant particulièrement compte des risques d'atteinte à leur santé physique et psychique.

* [29] Résolution n° 70 (2021-2022) du 14 janvier 2022 précitée.

* [30] Notamment le rapport d'information n° 900 (2021-2022) du 27 septembre 2022, fait par Mmes Annick Billon, Alexandra Borchio Fontimp, Laurence Cohen et Laurence Rossignol, fait au nom de la délégation aux droits des femmes - *Porno ; l'enfer du décor*.

A lire aussi

- **28 février 2023 :** Abus sexuels sur les enfants : une lutte prioritaire à mener aussi au niveau européen
- **28 février 2023 :** Réforme des retraites - Avis n° 373
- **28 février 2023 :** Réforme des retraites - Rapport n° 375
- **28 février 2023 :** Audition des Agences de l'eau au Sénat : au-delà de la gestion de crise, la politique de l'eau doit s'inscrire dans le long terme et mobiliser des moyens accrus
- **28 février 2023 :** Consigne : une méthode de concertation contraire à l'esprit de la loi, appelant à une vigilance renforcée
- **28 février 2023 :** PLFRSS 2023 : Préserver la retraite par répartition, garantir l'équité de la réforme