Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

COMMISSION SUPERIEURE DU NUMERIQUE ET DES POSTES

AVIS N°2023-07 DU 20 SEPTEMBRE 2023

SECURISER L'ESPACE NUMERIQUE POUR LES JEUNES

AVIS N°2023-07 DU 20 SEPTEMBRE 2023
SECURISER L'ESPACE NUMERIQUE POUR LES JEUNES

La haine en ligne et le cyberharcèlement prospèrent dangereusement, au détriment du bien-être de la Jeunesse et donc des Citoyens de la France de demain. Ce phénomène, d'une ampleur conséquente, appelle une mobilisation massive pour protéger et sécuriser nos enfants.

Face à cette situation, des initiatives sociétales et législatives émergent mais force est de constater que la situation ne s'est pas améliorée. C'est un climat dégradé auquel il convient, aujourd'hui, de rendre sa sérénité, tant à l'école que sur la toile.

Au-delà de la haine en ligne, un public de plus en plus jeune est confronté aux contenus pornographiques sur les plateformes de streaming ou sur certaines messageries, à la vente de stupéfiants sur les réseaux sociaux.

Alors que le règlement européen sur les services numériques (DSA), qui a pour objectif de renforcer la responsabilisation des plateformes, est entré en application le 25 aout 2023 pour lutter contre la diffusion de contenus illicites (atteintes à la dignité, contenus pédopornographiques, désinformation, vente de drogues …) et que le gouvernement vient de présenter un projet de loi visant à sécuriser et réguler l'espace numérique (procédure accélérée), il paraissait essentiel aux membres de la Commission supérieure d'étudier si ces textes et les dispositifs qu'ils proposent vont répondre de manière efficace, adaptée et concrète aux menaces bien réelles qui pèsent sur les plus jeunes dans l'espace numérique.

Le groupe de travail piloté par Mme Toine Bourrat, sénatrice des Yvelines et vice-présidente de la Commission supérieure du numérique et des postes, a examiné si les dispositifs tels qu'ils existent ou tels qu'ils sont envisagés par le DSA et le projet de loi visant à sécuriser et réguler l'espace numérique sont suffisamment protecteurs et s'ils doivent être renforcés. Il a notamment examiné les pistes souvent évoquées de la levée de l'anonymat et du pseudonymat sur les réseaux sociaux comme réponse à l'urgence de la situation.

A l'issue de ses travaux, les membres de la CSNP formulent 13 recommandations, adoptées à la majorité des membres, pour sécuriser l'espace numérique pour les jeunes, sous réserve de la conformité à la Constitution et de la cohérence avec les normes européennes :

- **Sur le cyberharcèlement**

  Recommandation n°1 : Assurer le traitement instantané des signalements d'un mineur victime de cyberharcèlement, en imposant aux plateformes la suspension immédiate de contenus haineux dont le mineur est la cible.

  Recommandation n°2 : Faciliter la levée de l'anonymat dans le cadre du cyberharcèlement de mineur.

  Recommandation n°3 : Imposer un nombre de modérateurs de langue française et de culture française aux plateformes et réseaux sociaux implantés sur le territoire national.

  Recommandations n°4 : Simplifier la chaîne des intervenants et renforcer les moyens dans la lutte contre le cyberharcèlement.

Recommandation n°5 : Faire financer par les plateformes et les réseaux sociaux des campagnes de sensibilisation et de prévention sur les dangers des réseaux sociaux.

Recommandation n°6 : Remettre aux victimes de cyberharcèlement une « fiche réflexe » à chaque dépôt de plainte

➢ **Sur l'accès aux contenus pornographiques**

Recommandation n°7 : Renforcer le contrôle de l'âge et de la majorité numérique par tout moyen, entre autres, par des paiements (versement d'une somme symbolique) par cartes bancaires.

Recommandation n°8 : Inclure dans le dispositif les messageries de type Télégram dédiées à la diffusion de contenus pornographiques et pédopornographiques, aux réseaux de prostitution des mineurs et autres trafics.

Recommandation n°9 : Introduire deux possibilités de déchiffrement, en amont, des données à l'égard de personnes identifiées et de plateformes ciblées pour des faits de pédopornographies avérées ou supposées.

➢ **Reprendre le contrôle face aux réseaux sociaux**

Recommandation n°10 : Renforcer les moyens de lutte contre le cyberharcèlement des établissements scolaires et maîtriser l'usage des smartphones et des tablettes au sein des établissements.

Recommandation n°11 : Former les parents sur l'impact et l'usage des réseaux sociaux dans le cadre de la formation et de la responsabilité sociale des entreprises.

Recommandation n°12 : Affermir les pouvoirs de l'Etat, ses prérogatives régaliennes en matière numérique pour assurer notre capacité à faire appliquer nos lois et à protéger nos concitoyens.

➢ **Vers une évolution législative du délai de prescription pour les injures et la diffamation en ligne**

Recommandation n°13 : Allonger le délai de prescription pour les actions de diffamation et d'injures commises en ligne à deux ans.

Recommandation n°1 : Assurer le traitement instantané des signalements d'un mineur victime de cyberharcèlement, en imposant aux plateformes la suspension immédiate de contenus haineux dont le mineur est la cible

Le Digital Services Act entré en vigueur le 25 aout 2023 renforce la responsabilité des plateformes au niveau européen. Le projet de loi SREN renforce les pouvoirs de l'Arcom qui pourra désormais, sans intervention du juge, ordonner le blocage de l'accès aux sites pornographiques qui ne contrôlent pas l'âge de leurs utilisateurs, après avoir prononcé une injonction administrative demeurée infructueuse. L'Arcom pourra sanctionner les sites en cas de non-retrait de contenus pédopornographiques dans les 24 heures.

La majorité des membres de la CSNP saluent ces progrès mais regrettent l'inaction des réseaux sociaux lors des émeutes qui se sont déroulées début juillet 2023 dans notre pays alors que ces mêmes plateformes, depuis le 25 aout, ont l'obligation d'effacer immédiatement les contenus haineux et risquent, en cas d'inaction, d'être sanctionnées par des amendes, mais également interdites d''exploitation sur le territoire européen.

La CSNP s'interroge, en outre, sur la capacité des services de la Commission européenne de gérer l'intégralité des demandes de retrait dans des délais rapides.

Or, pour lutter contre la viralité des messages de cyberharcèlement et de haine, il est essentiel de pouvoir retirer le plus rapidement possible ces messages des réseaux sociaux ou des plateformes.

Les membres de la CSNP souhaitent en effet que les requêtes d'un utilisateur mineur, victime de cyberharcèlement, soient traitées instantanément et que la charge de la preuve ne soit pas exclusivement supportée par l'agressé.

Les représentants des plateformes et des réseaux sociaux auditionnés par le groupe de travail ont indiqué qu'ils traitaient systématiquement les signalements de contenus haineux via leurs systèmes de modération respectifs, par l'usage de technologies reposant sur l'intelligence artificielle ou par des modérateurs. Ils nous ont également indiqué qu'ils donnaient suite immédiatement aux signalements effectués par les signaleurs de confiance.

Les membres de la Commission prennent acte de ces positions de principe mais ont malheureusement pu observer à l'occasion des évènements tragiques concomitants à ses travaux, le suicide de la jeune Lindsay et les émeutes qui ont secoué notre pays cet été, que ni les associations de protection de l'enfance, ni les pouvoirs publics, ni l'autorité judiciaire n'avaient été en mesure de suspendre ces messages haineux dans des délais suffisamment raisonnables et alors même, dans le cas du suicide de la jeune Lindsay, que son décès était déjà médiatisé et porté à l'attention des responsables publics et des plateformes.

Or, tous nos interlocuteurs, représentants d'associations, de forces de l'ordre, juges ou avocats, nous ont confirmé que la priorité était précisément le retrait immédiat de ces messages haineux pour que le mineur, victime de cyberharcèlement, puisse reprendre pied et sortir de cette spirale dans laquelle l'enferme la viralité des réseaux sociaux.

Dans ces conditions, la majorité des membres de la CSNP recommandent que dans le cas de cyberharcèlement d'un mineur, les plateformes et réseaux sociaux soient tenus de suspendre et

de retirer immédiatement tout contenu haineux signalé par ce mineur, son représentant légal ou une association, dès lors que la minorité de la victime est avérée.

A cet égard, la majorité des membres de la CSNP soutient l'amendement voté au Sénat dans le cadre du projet de loi « Sécuriser et réguler l'espace numérique » qui dispose que soit ajouté après l'alinéa 54 de l'article 22 : « Saisies d'un signalement de la part d'un mineur de moins de quinze ans portant sur un contenu illicite, ou contraire à leurs conditions générales d'utilisation, qui mentionne ce même mineur de moins de quinze ans inscrit sur une plateforme dans les conditions prévues à l'article 6-7 de la présente loi, les plateformes en ligne mettent le contenu précité hors d'accès sans délai et jusqu'à l'aboutissement de la procédure de traitement du signalement, quelle qu'en soit la nature. Le mineur ou ses représentants apportent, par tout moyen, la preuve que la personne mentionnée a moins de quinze ans ».

Les membres de la CSNP considèrent que la liberté d'expression, à laquelle ils sont bien naturellement attachés, doit dans ce cas très précis, être considérée au regard de la fragilité et de la vulnérabilité des victimes. Il restera toujours possible à l'auteur des propos signalés de démontrer qu'il n'enfreint pas les dispositions de l'article 222-33-2-2 du code pénal.

Par ailleurs, les membres de la CSNP recommandent la révision de l'article 6. I. 8 de la LCEN introduit par la loi n° 2021-1109 du 24 août 2021 qui substitue la « procédure accélérée au fond» aux actions en référé ou sur requête. Cette nouvelle disposition aurait pour effet de ralentir la procédure de plusieurs mois. Les membres de la CSNP demandent au Garde des Sceaux de clarifier cette situation pour, le cas échéant, la corriger.

<u>Recommandation n°2</u> : Faciliter la levée de l'anonymat en cas de cyberharcèlement de mineur.

Alors qu'il est communément admis que l'anonymat n'existe pas sur internet et que chaque message ou passage sur le net peut être identifié par une adresse IP, le groupe de travail a souhaité s'assurer que l'anonymat ne constituait pas un obstacle dans la lutte contre le cyberharcèlement et plus généralement dans la diffusion de contenus haineux.

L'ensemble des plateformes interrogées nous ont indiqué que *de facto* l'anonymat n'existait pas.

Pourtant, en pratique, la levée de l'anonymat peut s'avérer non seulement impossible mais également onéreuse.

Pour les praticiens du droit que nous avons interrogés, la levée de l'anonymat est un obstacle majeur : dans la moitié des cas, l'auteur de propos haineux ou de menaces utilise un VPN et se localise dans des pays et des juridictions qui ne coopèrent pas avec notre système judiciaire.

Pour les réseaux ou les plateformes dont le siège social se trouve aux Etats-Unis, la jurisprudence mouvante sur le respect du 1er amendement de la constitution américaine consacrant la liberté d'expression peut dans certains cas conduire à une fin de recevoir des demandeurs.

En pratique, seules les demandes de levée d'anonymat émanant du Parquet national numérique ont des chances d'aboutir dans le cadre de la coopération internationale. Les demandes émanant des magistrats français et des victimes représentées par leur avocat, qui constituent la quasi-totalité des demandes dirigées contre les réseaux sociaux, n'ont quasiment aucune chance d'aboutir.

Dans tous les cas, demander la levée de l'anonymat d'un compte suppose un certain nombre de démarches et du temps qui occasionnent des coûts estimés entre 5000 et 10 000 euros sans garantie d'identifier l'auteur. Or ces coûts s'avèrent rédhibitoires pour l'écrasante majorité des victimes.

De leur côté, les grandes plateformes disposent de moyens financiers considérables dont ne bénéficient pas les citoyens créant une asymétrie systémique.

La majorité des membres de la CSNP considèrent que cette situation n'est pas tolérable et proposent d'introduire la levée automatique de l'anonymat en cas de cyberharcèlement de mineur. Dès lors qu'un mineur, ou son représentant légal, est en mesure de démontrer qu'un message ou un contenu haineux le vise personnellement, les plateformes et réseaux sociaux doivent être tenus de lui communiquer l'adresse IP de l'ordinateur ou du portable et l'identité de l'auteur de ces messages ou de ces contenus.

En tout état de cause, la majorité des membres de la CSNP propose la révision de l'article 60-1-2 du Code de procédure pénale introduite par la loi du 2 mars 2022 qui empêche les juges de demander l'identification d'un compte dès lors que les auteurs d'un délit encourent une peine inférieure à un an.

En cas d'utilisation d'un VPN par l'auteur de propos haineux ou de cyberharcèlement pour masquer son identité, les membres de la CSNP considèrent que les plateformes doivent, sur réquisition du juge, suspendre immédiatement le compte concerné.

<u>Recommandation n°3</u> : Imposer un nombre de modérateurs de langue française et de culture française aux plateformes et réseaux sociaux implantés sur le territoire national.

Les réseaux sociaux et les plateformes utilisent massivement les solutions d'intelligence artificielle pour retirer *ex ante* des contenus violents ou pornographiques.

De l'aveu même du représentant de TiKTok France, l'intelligence artificielle n'est pas pleinement opérationnelle en matière de cyberharcèlement[1]. Dans ces conditions, il est essentiel que les plateformes et les réseaux sociaux emploient des modérateurs de langue et de culture françaises pour mieux appréhender les contenus haineux qui posent de véritables problèmes et qui ne peuvent être décelés par des modérateurs en nombres insuffisants, localisés à l'étranger et dont le français est dans le meilleur cas la deuxième ou troisième langue étrangère pratiquée.

Pour lutter efficacement contre le cyberharcèlement, la CSNP recommande que les plateformes emploient en France des modérateurs de langue et de culture françaises. Le nombre minimal des modérateurs sera évalué par l'Arcom.

<u>Recommandations n°4 :</u> Simplifier la chaîne des intervenants et renforcer les moyens dans la lutte contre le cyberharcèlement

Les dispositifs de lutte contre le cybercrime, contre la haine en ligne et le cyberhacèlement qui incluent le département informatique et électronique de l'Institut de recherches criminelles (IRCGN), la Brigade d'enquête sur les fraudes aux technologies de l'information (BEFTI), l'Office

[1] M. Garandeau était interrogé le 10 juillet dans le cadre de la Commission spéciale de l'Assemblée nationale sur le rôle des réseaux sociaux dans la propagation des émeutes qui se sont déroulées en France début juillet 2023.

central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), la plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (PHAROS) ont été renforcés avec la mise en place du pôle national de la haine en ligne, dit parquet national numérique, crée par la loi Avia en 2021.

Le projet de loi SREN confère de nouvelles responsabilités à l'ARCOM.

La question des effectifs et des moyens humains pour lutter contre les crimes, et singulièrement les crimes en ligne, se posent de manière récurrente. Sur le sujet du live streaming mettant en scène des enfants mineurs, il était observé que seuls 17 enquêteurs au sein de l'Office central pour la répression des violences aux personnes (OCRVP) et 8 enquêteurs au sein du Groupe de répression des atteintes aux mineurs du Centre de lutte contre les criminalités numériques (C3N) de la gendarmerie étaient dénombrés contre 320 enquêteurs spécialisés au Royaume-Uni (68 millions d'habitants) et 150 enquêteurs aux Pays-Bas[2] (18 millions d'habitants).

Les membres de la CSNP souhaitent qu'à l'occasion de l'examen du prochain projet de loi de finances, le Ministère de l'Intérieur et le Ministère de la Justice précisent les effectifs dédiés à la lutte contre la haine en ligne, la lutte contre le cyberharcèlement et fournissent des informations sur les services dédiés dans les autres pays européens.

Par ailleurs, alors que le dispositif d'alerte mis en place par le DSA et le projet de loi SREN repose sur l'intervention des signaleurs de confiance, majoritairement constitués par des associations à but non lucratifs éparses, les membres de la CSNP recommandent que l'Etat mette en place un dispositif simple et centralisé (type guichet unique ou numéro exclusif) pour structurer et garantir une « méthodologie » claire et unique.

<u>Recommandations n°5</u> : Faire financer par les plateformes et les réseaux sociaux des campagnes nationales de sensibilisation et de prévention sur leurs dangers en vue de lutter contre le cyberharcèlement

Les initiatives pour lutter contre le cyberharcèlement sont nécessaires. Au cours de ses travaux, le groupe de travail a eu l'occasion de rencontrer la Team anti-harcèlement du lycée Bascan de Rambouillet, l'association Génération numérique, la Maison de protection des familles et la cellule de prévention technique de la malveillance de Bois d'Arcy qui font un travail formidable pour détecter, prévenir et sensibiliser au cyberharcèlement mais ont un impact limité à la seule échelle locale.

Les membres de la CSNP proposent que des actions de sensibilisations soient amplifiées, renforcées au plan national par des campagnes de sensibilisation et de prévention sur les dangers dans l'espace numérique (TV, Radio, plateformes) et dont le coût financier sera pris en charge par les plateformes elles-mêmes.

<u>Recommandation n°6 : Remettre aux victimes de cyberharcèlement une « fiche réflexe » à chaque dépôt de plainte</u>

Les règles de procédures pénales sont généralement complexes et nécessitent de recueillir un certain nombre de preuves matérielles pour alimenter la procédure. Or, certaines des infractions commises sur les réseaux sociaux peuvent se confronter à des éléments de preuves qui sont éphémères, notamment par exemple les messages envoyés depuis la plateforme Snapchat.

[2] « Halte aux viols d'enfants sur Internet ! » par Maître Christiane Féral-Schuhl, publié dans Ouest-France le 20 mai 2023

Également, une victime de cyberharcèlement peut ressentir le besoin de changer de téléphone portable, de changer ses profils sur les réseaux sociaux, de supprimer ses messages etc. Toutes ces actions, entreprises par la victime, qui dans un souci souvent d'apaisement, supprime, à son corps défendant, les preuves matérielles, et impacte négativement la procédure et le travail des enquêteurs.

Afin de limiter l'effacement des éléments de preuve, les membres de la CSNP proposent qu'une « fiche réflexe » soit rédigée par les services du Ministère de l'Intérieur et qu'elle soit remise à chaque dépôt de plainte pour des faits de cyberharcèlement. Cette fiche pourrait mentionner par exemple l'importance d'enregistrer les messages incriminants ou d'en faire des captures écrans, mais également d'indiquer aux victimes de rester en possession de leur téléphone portable.

<u>Recommandation n°7 : Renforcer le contrôle de l'âge et de la majorité numérique par tout moyen, entre autres, par des paiements (versement d'une somme symbolique) par cartes bancaires.</u>

La majorité numérique est désormais établie à 15 ans.

L'Arcom se prononcera prochainement sur les moyens que devront mettre en œuvre les sites pornographiques pour limiter l'accès des mineurs à leurs sites.

Il ressort des auditions conduites par le groupe de travail piloté par Mme Toine Bourrat, sénatrice des Yvelines et vice-présidente de la CSNP, que les plateformes sont très réticentes à effectuer un contrôle poussé de l'identité et donc de l'âge des titulaires de comptes.

Les contrôles anthropomorphiques par intelligence artificielle sont encore trop imprécis et doivent être assortis d'autres contrôles. Ils posent, par ailleurs, la question du stockage de ces données.

Le contrôle par l'identité numérique lorsque celle-ci sera adoptée par l'ensemble de nos concitoyens pourra constituer un moyen de contrôle fiable.

En attendant, la majorité des membres de la CSNP sont favorables à ce que l'identité des titulaires de compte ou de leurs parents, soient vérifiés par le paiement par carte bancaire d'une somme modique, de quelques centimes.

Les paiements par carte bancaire sont désormais très largement banalisés. Cette solution permettrait 1./ de renforcer le contrôle exercé par les parents et 2./ aux plateformes et réseaux sociaux d'avoir une information vérifiée et fiable sur l'identité du titulaire du compte. En effet, la délivrance d'une carte bancaire est soumise à des règles de contrôle très strictes par des établissements extrêmement régulés et dont les données sont, de loin, les plus sécurisées.

<u>Recommandation n°8</u> : Inclure dans le dispositif les messageries de type Télégram dédiées à la diffusion de contenus pornographique et pédopornographiques, aux réseaux de prostitution des mineurs et autres trafics.

Les membres de la CSNP relèvent que le DSA et le projet de loi SREN ne s'appliquent pas aux messageries privées telles que WhatsApp, Signal ou Télégram.

Ces messageries bénéficient du régime du secret des correspondances privées alors même que ces messageries diffusent des contenus pornographiques, des contenus violents et haineux, et

contribuent à différents trafics (drogue, prostitution) et comptent parfois plus de 500 000 membres.

La majorité des membres de la CSNP recommandent que les messageries de type WhatsApp, Signal et Télégram entrent dans le champ d'application du projet de la loi SREN.

<u>Recommandation n°9 :</u> Introduire deux possibilités de déchiffrement en amont des données à l'égard de personnes identifiées et de plateformes ciblées pour des faits de pédopornographies avérées ou supposées.

En raison du chiffrement des échanges, qui peut aboutir à l'impossibilité matérielle, pour l'intégralité des plateformes, de transmettre des signalements, lesquels constituent actuellement la quasi-totalité des saisines services de police judiciaire en matière de pédocriminalité : le Code européen des communications électroniques de 2018 a créé un vide juridique sur la question du déchiffrement des données et a menacé la capacité des fournisseurs d'accès à détecter et signaler les contenus pédopornographiques.

Un règlement dérogatoire à la Directive e-privacy (n°2021-1232)[3] a été adopté en 2021 mais de manière temporaire, puisqu'applicable jusqu'au 3 août 2024. Dans la continuité des règlements relatifs à un marché intérieur des services numériques (Digital Service Act) et à la lutte contre la diffusion des contenus à caractère terroriste en ligne (Terrorist Content Online), une proposition de règlement relative à la prévention et la lutte contre les abus sexuels sur mineurs (dit règlement « ASM ») a été publiée par la Commission européenne le 11 mai 2022[4] afin de compléter le dispositif de régulation du numérique, et ce de manière pérenne.

Pour autant, la levée totale du chiffrement de bout en bout, souhaitable pour la détection des contenus pédopornographiques par les fournisseurs d'accès, se heurte à la protection des libertés individuelles et en particulier de la vie privée des utilisateurs des réseaux sociaux.

L'enjeu consiste dès lors à trouver un équilibre entre la protection des libertés, valeur commerciale des grandes plateformes, et la lutte contre les abus sexuels sur mineurs.

Les membres de la Commission, soucieux de la protection des libertés, proposent néanmoins l'introduction de deux possibilités de déchiffrement en amont des données, encadrées de manière stricte : d'une part à l'encontre de personnes identifiées (grâce notamment à des dénonciations de personnes physiques, ce qui en matière de pédocriminalité -où par hypothèse les auteurs agissent cachés, dans un échange interpersonnel avec leur victime parfois sous emprise-, est très rare) et d'autre part, sur autorisation judiciaire, à l'encontre de plateformes ciblées comme regroupant des échanges pédo-criminels sur une période déterminée.

<u>Recommandation n°10</u> : Renforcer les moyens de lutte contre le cyberharcèlement et maîtriser l'usage des smartphones et des tablettes au sein des établissements.

Les membres de la CSNP considèrent que des moyens doivent être déployés pour former et mieux communiquer sur le cyberharcèlement dans les établissements scolaires. Au volet

[3] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32021R1232
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN&qid=1652451192472

« prévention », chargé de rappeler que tout élève est une victime en puissance, se surajoute nécessairement celui de la présentation des « sanctions » encourues en cas de manquement.

Sur l'usage du téléphone portable dans les établissements scolaires, les membres de la CSNP considèrent que ce sujet relève du règlement intérieur des établissements mais que les lignes directrices doivent être clairement posées par le Ministre.

Depuis 2018, et l'adoption de la loi n°2018-698 du 3 août 2018, l'usage du téléphone portable est interdit que ce soit en classe, en inter-cours, ou à la récréation. En pratique, force est de constater que le téléphone portable continue de perturber la transmission sereine des connaissances. Son usage est à l'origine d'une part importante des incivilités et des perturbations au sein des établissements. Les enseignants parlent de l'omniprésence des smartphones à l'école, donc de l'omniprésence des réseaux sociaux qui les rend plus vulnérables au cyberharcèlement et facilitent l'accès aux images violentes : les enseignants sont filmés à leur insu en cours, les élèves sont filmés à leur insu, en cours, dans la cour ou dans les toilettes.

La CSNP estime qu'il convient de donner à chaque établissement les moyens administratifs et matériels permettant aux élèves de déposer leur téléphone durant la journée et de le récupérer avant de quitter l'établissement.

La CSNP propose d'intégrer systématiquement, dans les Règlements intérieurs d'établissements signés par l'élève et ses responsables légaux en début d'année scolaire, une charte rappelant les sanctions encourues en matière de cyberharcèlement afin de les informer sur leur responsabilité.

Quelle que soit leur connaissance des plateformes, les parents doivent rester des repères pour accompagner leurs enfants. Ils sont donc les premiers garants du bon usage des outils numériques qu'ils mettent entre leurs mains. En dehors du champ scolaire, c'est à eux qu'il appartient de définir les règles d'utilisation (heures de déconnexion, durée d'utilisation, présence du téléphone dans la chambre la nuit…).

<u>Recommandation n°11</u> : Former les parents sur l'impact et l'usage des réseaux sociaux dans le cadre de la formation et de la responsabilité sociale des entreprises et des administrations publiques

Au cours des auditions conduites par le groupe de travail, plusieurs constats ont été partagés :

- la plupart des parents ne savent pas et n'imaginent même pas à quels contenus sont exposés leurs enfants.
- les parents, dans leur très grande majorité, maitrisent encore mal les fonctionnalités du contrôle parental.
- les parents qui participent aux réunions d'information organisés par les établissements scolaires ou autre organisations sont généralement déjà sensibilisés aux sujets de cyberharcèlement et aux maux générés par les réseaux sociaux.

Ces constats valables pour les parents valent également pour l'ensemble des adultes.

Les membres de la CSNP recommandent que des formations sur les réseaux sociaux, l'usage des smartphones et le cyberharcèlement, soient déployées en entreprises et dans les administrations publiques en associant les organisations représentatives des entreprises,

MEDEF et CPME, des chambres consulaires CCI et CMA, et des organisations syndicales des salariés et de fonctionnaires.

Ces formations et ces actions de sensibilisation pourraient relever de la responsabilité sociale des entreprises et des administrations publiques.

<u>Recommandation n°12 :</u> Affermir les pouvoirs de l'Etat et ses prérogatives régaliennes en matière numérique pour assurer notre capacité à faire appliquer nos lois et à protéger nos concitoyens.

Avec l'arrivée des réseaux sociaux et des plateformes, nous avons changé d'ère. Le pouvoir d'influence de ces réseaux, dont les dirigeants sont désormais reçus comme des chefs d'Etat, est considérable.

Les membres de la CSNP considèrent que les enjeux démocratiques posés par ces acteurs sont trop importants pour que nos démocraties se laissent imposer sur leur territoire des règles qu'elles n'ont pas choisies.

Les réseaux sociaux et les grandes plateformes ont généralement leur siège en dehors du territoire de l'Union européenne et, cela pose très concrètement la question de notre souveraineté, de notre capacité à faire appliquer nos lois et de protéger nos citoyens.

Si nos partenaires européens ne sont pas complètement alignés sur nos positions, la CSNP appelle les autorités françaises à veiller à ce que notre droit national et les normes européennes soient respectés par les réseaux sociaux et les plateformes.

<u>Recommandation n°13 :</u> Allonger le délai de prescription à deux ans pour les actions de diffamation et d'injures commises en ligne.

Le droit de l'expression en ligne et ses limites sont gouvernés essentiellement par la loi du 29 juillet 1881 sur la liberté de la presse.

Historiquement, le délai de prescription qui était de trois mois, aujourd'hui d'un an, s'expliquait par les modalités de publication de la presse qui était limitée dans le temps et dans l'espace. Toutefois, ces modalités ne sont plus adaptées à l'ère d'internet. En effet, les publications sont illimitées dans le temps et dans l'espace.

Afin de réparer plus efficacement les abus de la liberté d'expression, en prenant en considération les effets potentiellement beaucoup plus graves des abus commis sur Internet et d'adapter le texte aux enjeux actuels, **la majorité des membres de la CSNP proposent de modifier l'article 65-3 de la loi du 29 juillet 1881 sur la liberté de la presse en portant le délai de prescription de ces infractions d'un an à deux ans.**

LISTE DES PERSONNES ET ENTITÉES AUDITIONNÉES ET RENCONTRÉES

ARCOM
M. Benoit LOUTREL et Mme Laurence PECAUT-RIVOLIER, membres du collège
Mme Lucile PETIT, Directrice des plateformes en ligne

CNIL
M. Thomas DAUTIEU, directeur de l'accompagnement juridique,
M. Bertrand PAILHES, directeur des technologies et de l'innovation,
Mme Chirine BERRICHI, Conseillère parlementaire

Direction Générale des entreprises
M. Loic DUFLOT, Chef de service de l'économie numérique
Mme Chantal RUBIN, Chef du Pôle régulation des plateformes numériques

Gendarmerie nationale
Colonel Vincent ROCHE, Commandant de groupement de la Gendarmerie nationale des Yvelines
Major Jessica DUBOIS, Commandant de la Maison de Confiance et de Protection des Familles des Yvelines
Adjudant-chef René COUESLAN Chef de la cellule prévention technique de la malveillance

Génération Numérique - M. Cyril DI PALMA, Délégué général

Lycée Bascan de Rambouillet,
M. Dominique PINCHERA, Proviseur
M. Mikaël HICETTE, Proviseur-adjoint
Mme Sara QUERTINIER, Proviseure-adjointe
Association Team Anti Harcèlement.

Maître Richard MALKA, Avocat

Parquet de Paris
Mme Laure BECCUAU, Procureure de Paris
M. Grégory WEILL, Procureur en charge du parquet national de lutte contre la haine en ligne
Mme Lisa-Lou WIPF, Vice-Procureure en charge de la section des mineurs

Mme Myriam QUEMENER, Magistrate

SNAPCHAT - Mme Sarah BOUCHAHOUA, Responsable des affaires publiques

Maitre Ilana SOSKIN, Avocate

TIKTOK
M. Eric GARANDEAU, Directeur des affaires publiques
Mme Sarah KHEMIS, Responsable Senior Affaires Publiques France

YUBO
Mme Sharone FRANCO, Directrice des affaires publiques
M. Marc-Antoine DURAND, Directeur des opérations