RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CONSEIL NATIONAL DE LA REFONDATION

CNR Numérique

Volet « Apaisement de l'espace numérique et lutte contre les violences en ligne »

Septembre 2023

Le mot du ministre

La recherche d'effectivité par la mobilisation du collectif

Le 22 novembre 2022, nous inaugurions le Conseil national de la refondation dans le numérique, dont l'axe dédié à l'apaisement de l'espace numérique et à la lutte contre les violences en ligne. L'idée d'apaisement s'est avérée essentielle pour aborder de manière constructive, positive et collective une vaste série de problèmes que nous subissons depuis trop longtemps : cyberharcèlement, agressions verbales, injures, violences sexistes et sexuelles, atteintes à l'intégrité des mineurs, etc.

Notre détermination pour lutter contre ces situations bien trop fréquentes est claire. Nous ne pouvons tolérer que, du fait de sa libre expression, de par son identité ou sa simple existence, une personne soit soumise ou exposée à des agressions, avec parfois des conséquences absolument dramatiques. Les mots comptent, les images heurtent et il n'est bien sûr rien de virtuel en la matière.

La France a été particulièrement motrice pour sécuriser notre environnement numérique. Elle a joué un rôle de premier plan dans l'adoption du règlement européen sur les services numériques, le *Digital Services Act*, dont la mise en œuvre se fera de manière progressive d'ici au mois de février prochain. Après plusieurs décennies au cours desquelles des acteurs majeurs comme les réseaux sociaux ont bénéficié d'une responsabilité juridique limitée, nous évoluons vers un renforcement du contrôle et de la responsabilité de ces acteurs.

Notre droit sera prochainement adapté dans les mois à venir. C'est une des vocations du projet de loi actuellement en débat au Parlement. Il reviendra alors à la Commission européenne et aux autorités nationales compétentes dont le coordinateur des services numériques, qui en France devrait être l'Arcom, de faire respecter ces nouvelles règles. Au vu des enjeux, il est apparu essentiel d'avancer sur des mesures fortes visant à sécuriser notre espace numérique, à protéger les publics les plus jeunes, les victimes de harcèlement et les consommateurs contre les faits d'escroquerie massifs dont nous faisons trop fréquemment l'objet. Le débat parlementaire en cours est l'opportunité de débattre de certaines de ces mesures à adopter.

Mais tout ne se jouera pas au niveau législatif. Beaucoup se fera dans la mise en œuvre. C'est pourquoi **la priorité donnée à ce CNR n'était pas de déboucher sur des obligations supplémentaires mais d'assurer l'effectivité du cadre réglementaire en**

vigueur en mettant sur pied un cadre de construction collective des remèdes les plus appropriés et en identifiant les ressorts concrets à activer pour faciliter l'implication et la protection de toutes et tous.

D'aucuns pourraient considérer les mesures contenues dans cette feuille de route comme frappées du coin du bon sens, voire s'étonner de leur inexistence à ce jour. Pourtant les travaux du CNR en ont révélé la nécessité. Loin des effets d'annonces ou des injonctions fondées sur des moyens hypothétiques, les mesures annoncées visent à instaurer et nourrir un cadre d'action durable.

Dans le cadre des travaux de ce CNR, de nombreuses administrations, associations, plateformes, entreprises et nombre de citoyens ont contribué à des échanges inédits. Jamais nous n'avions mis en place un tel cadre de discussions où enseignants, journalistes, lycéens, collégiens, streameuses… pouvaient interagir directement avec les représentants des réseaux sociaux et des autorités nationales dans un cadre d'écoute et de confiance. La formule a pu surprendre, mais elle a fonctionné. Les principaux réseaux sociaux ont fait preuve d'écoute, de nombreux mythes ont pu être débusqués tandis que des clefs de compréhension et donc d'amélioration ont pu être apportées en direct. Ce CNR a permis d'éprouver une méthode collective qui doit perdurer à l'avenir dans l'exercice de la régulation.

Nous devons avant toute chose permettre à l'ensemble des acteurs d'interagir en direct, de s'écouter et de se comprendre pour ensuite agir. L'apaisement de l'espace en ligne commence bien par cette phase d'écoute et d'attention des uns envers les autres, tous réunis dans la même pièce, dans un cadre de confiance, en se parlant jour après jour. C'est cette méthode que nous entendons instituer avant toute chose.

Cette méthode, les équipes de toutes les autorités publiques engagées dans le CNR l'ont éprouvée, le Conseil national du numérique, la Dilcrah, l'Arcom, la DGE, le PEReN, la DINUM, la DITP, la Pharos, la gendarmerie nationale, Cybermalveillance.gouv.fr, la CNIL, l'Education nationale, la Justice. Autour d'elles, une part importante de la société civile œuvrant contre les violences en ligne s'est rassemblée. Autant de personnes engagées au quotidien qui ont donné de leur temps pour répondre à un objectif politique majeur. Je tiens particulièrement à les en remercier. La recherche d'un environnement numérique apaisé est une priorité fondamentale de l'action de ce Gouvernement. Soyez assurés que nous y mettrons tous les moyens nécessaires.

Jean-Noël Barrot
Ministre délégué chargé de la Transition numérique et des Télécommunications

Sommaire

Introduction **7**

Que faire face à une situation que l'on estime anormale ? **10**

Quelques faits et chiffres **14**

I. VISIBILISER ***Partager les vécus et les actions portées*** **19**

Agréger les rapports et études réalisés 20

Créer un baromètre de l'apaisement de l'espace numérique 27

Générer un tableau de bord des actions portées 32

La parole aux acteurs **35**

II. PROTÉGER ***Mieux orienter les utilisateurs vers les dispositifs adaptés*** **47**

Approfondir notre connaissance du parcours utilisateur 51

Massifier les campagnes publiques d'information 53

La parole aux acteurs **57**

III. RASSEMBLER ***Porter les écosystèmes œuvrant à l'apaisement*** **63**

Soutenir les acteurs de la citoyenneté numérique 64

Instituer un forum d'échange dédié à l'apaisement de l'espace numérique 67

La parole aux acteurs **70**

ALLER PLUS LOIN ***18 propositions faites par les participants*** **79**

Éduquer et former le plus grand nombre 79

Améliorer la réponse pénale 82

Développer une atmosphère de confiance et de sécurité 85

Listes des entités et personnes contributrices ou participantes **89**

Introduction

Le Conseil national de la refondation a été initié par le président de la République le 8 septembre 2022. Il vise à rassembler l'ensemble des personnes intéressées autour de solutions concrètes améliorant le quotidien de toutes et tous. Dans ce cadre, le 22 novembre 2022, Jean-Noël Barrot, ministre délégué chargé de la Transition numérique et des Télécommunications, inaugurait le Conseil National de la refondation dédié au numérique (CNR Numérique). Au cours de ces six derniers mois, le CNR Numérique a travaillé à trois enjeux prioritaires faisant chacun l'objet d'une feuille de route :

- l'inclusion et l'accessibilité numériques ;
- les transitions numériques au travail ;
- l'apaisement de l'espace numérique et la lutte contre les violences en ligne.

Pour ce qui est de l'apaisement de l'espace numérique et la lutte contre les violences en ligne, objet du présent document, le travail a été réalisé par l'association de nombreuses autorités, associations, entreprises et citoyens déjà fortement mobilisés. Dans la poursuite de la philosophie du CNR, l'objectif était prioritairement de construire sur les initiatives existantes pour faciliter l'action de chacun et atteindre une meilleure protection des publics.

Tout au long des six derniers mois, des dizaines d'échanges avec des parties prenantes (usagers, plateformes, autorités, associations) ont été conduits quotidiennement. Des ateliers de plus grande dimension ont été organisés : le 12 janvier sur les signaleurs de confiance à l'initiative de l'Arcom et dans le cadre de l'Observatoire de la haine en ligne ; le 7 février à l'initiative du ministre délégué pour rassembler l'ensemble des acteurs du secteur et une centaine de collégiens et lycéens ; le 15 février 2022 pour réunir des utilisateurs, des représentants des plateformes et des autorités autour de la question du parcours de l'usager dans le signalement des contenus illicites ; le 22 mars 2022, à l'Assemblée nationale à l'initiative de Mme la députée Véronique Riotton sur l'exposition à la violence des femmes d'influence.

Ces échanges ont nourri une dynamique collective très constructive. Ils ont permis de faire émerger les actions initiées, les besoins et les idées qui permettent de nourrir une feuille de route lisible, efficace, qui ne soit pas fondée sur des projections, mais bien sur des actions à portée de main.

Les mesures annoncées, loin d'être incantatoires, offrent un chemin qui ne dépend pas de la libération d'une capacité de travail insoupçonnée de personnels, magistrats, policiers ou enseignants déjà très fortement mobilisés. Ces mesures ne sont pas non plus fondées sur une manne financière inespérée. Elles présentent des solutions

concrètes, en nombre sciemment limité, qui répondent à des attentes et s'appuient sur les expériences et les engagements des acteurs. Surtout, elles ont pour ambition de répondre aux besoins des citoyens et de soutenir les acteurs de terrain, que ce soit en mettant en avant leurs actions ou en structurant leur cadre d'intervention. Ce cadre structuré est précisément celui qui permettra l'émergence de nombreuses mesures au quotidien, offrant la réponse la plus adéquate aux exigences citoyennes.

Le CNR Numérique est intervenu à un moment clé dans l'histoire de la régulation des services numériques marqué par l'entrée en vigueur du règlement européen sur les services numériques et sa mise en application progressive. Un projet de loi sera bientôt débattu au Parlement afin d'adapter le droit national à ce règlement et de porter des mesures complémentaires répondant aux objectifs de protection des publics.

Il est donc prévu de longue date que de nouvelles règles soient progressivement mises en œuvre aux fins de l'apaisement de nos relations en ligne et sous peine de fortes sanctions. Beaucoup d'attendus, notamment sur la modération des contenus en ligne, devraient être ainsi couverts dans ce cadre.

Dans ce contexte, il a semblé utile de penser le CNR comme le lieu d'émergence de solutions pouvant accompagner la législation et la régulation tout en facilitant le travail des acteurs, et ce sur la base des nombreuses briques déjà existantes. Si toutes les questions sous-jacentes à l'apaisement de l'espace numérique n'ont pu être abordées dans le cadre de la présente concertation, le cadre d'action dessiné tant à travers la présente feuille de route, que dans le règlement européen des services numériques et le projet de loi visant à sécuriser et réguler l'espace numérique offrira le cadre pertinent pour ce faire. Ainsi, les travaux ont abouti à 7 mesures phares répondant à 3 objectifs principaux :

- **VISIBILISER : Partager les vécus et les actions portées**

  Mesure 1 – Agréger les rapports et études réalisés

  Mesure 2 – Créer un baromètre de l'apaisement de l'espace numérique

  Mesure 3 – Générer un tableau de bord des actions portées

- **PROTÉGER : Mieux orienter les utilisateurs vers les dispositifs adaptés**

  Mesure 4 – Approfondir notre connaissance du parcours utilisateur

  Mesure 5 – Massifier les campagnes publiques d'information

- **RASSEMBLER : Porter les écosystèmes œuvrant à l'apaisement de l'espace numérique**

  Mesure 6 – Soutenir les acteurs de la citoyenneté numérique

  Mesure 7 – Instituer un forum d'échanges multipartites

Les mesures présentées couvertes par ces trois axes entendent se rapprocher d'un point de rassemblement entre des acteurs de nature et aux objectifs très différents. C'est ce qui constitue leur force : elles peuvent participer d'une synergie fructueuse entre des acteurs variés et être ainsi porteuses de nombreuses améliorations tangibles.

Ces mesures ne sont certainement pas les seules devant être portées pour parvenir à l'apaisement de nos relations en ligne. Bien d'autres thèmes sont à aborder en amont, en aval ou en parallèle des dispositifs ici annoncés. Qu'il s'agisse de la façon dont les réseaux sociaux et autres plateformes en ligne sont conçus, des pratiques compulsives pouvant donner lieu à des comportements violents, des phénomènes sociaux sous-jacents, des questions éducatives, des problèmes généraux de mise en application de la loi. Mais ces champs d'action ne peuvent être le fruit d'une concertation de six mois au niveau national et entre de tels acteurs.

Les phénomènes observés sont multifactoriels et il faut bien prendre le problème par tous les bouts. C'est pourquoi, pour aller plus loin, une ultime partie de la feuille de route a pour vocation de rassembler 18 propositions faites par les participants au CNR Numérique et qui rejaillissent sur des cadres d'action plus étendus. Ces propositions n'en sont pas moins fondamentales et pourront alimenter les débats ou actions à venir. Elles s'organisent autour des 3 axes suivants :

- **Éduquer et former le plus grand nombre**
- **Améliorer la réponse pénale**
- **Développer une atmosphère de confiance et de sécurité**

Enfin, tout au long de ce CNR, la parole a été donnée aux acteurs pour comprendre et valoriser leurs actions. Afin de rendre compte de cette dynamique, une partie d'entre eux a été invitée à s'exprimer de manière libre et directe dans des encarts dédiés. Leurs propos n'engagent que leurs auteurs, tout comme ils ne sauraient être engagés par le contenu de la présente feuille de route. D'autres contributions pourront être ajoutées dans les semaines à venir pour celles et ceux qui en feraient la demande.

Une feuille de route pour

→ *Rendre compte de l'existant et clarifier les apports de la régulation à venir*

→ *Identifier 3 axes prioritaires regroupant 7 mesures structurantes*

→ *Prolonger le travail sur 3 axes complémentaires forts de 18 propositions*

→ *Donner la parole aux acteurs*

Que faire face à une situation que l'on estime anormale ?

Face à une situation que l'on estime anormale, il n'est pas toujours possible d'appliquer une qualification juridique stricte, mais cela ne doit pas empêcher une victime ou un témoin d'agir, si l'on estime de bonne foi qu'un contenu ou un comportement donné ne devrait pas exister, et devrait à l'inverse être réprimé.

Dans cette situation, une première chose à faire est de signaler le contenu sur le réseau social en suivant les indications fournies. Toutes les plateformes auront bientôt (février 2024) l'obligation de mettre en place un dispositif de signalement facile d'accès. Une fois le signalement envoyé à la plateforme, celle-ci devra en accuser réception et le traiter dans les meilleurs délais. Il sera également tenu d'informer l'utilisateur de la décision prise et des recours possibles si l'internaute n'est pas satisfait de la décision.

Sur les réseaux sociaux, lorsqu'un utilisateur souhaite signaler un contenu il peut le faire de plusieurs manières : depuis la publication ou le commentaire concerné (en cliquant sur les trois petits points par exemple ou en restant appuyé 3" sur la publication sur certains réseaux) ou à travers un formulaire dédié, généralement plus détaillé et permettant de préciser un peu plus les motifs du signalement ou encore de partager des pièces jointes. Néanmoins, en pratique, le signalement auprès des plateformes ne permet pas toujours de répondre à l'ensemble des cas rencontrés, notamment dans les cas de messages trop nombreux pour être signalés, mais pourtant bien constitutifs de harcèlement en ligne.

En plus des signalements auprès des plateformes, d'autres voies listées ci-après sont ouvertes selon que : le signalement sur le réseau social s'est avéré infructueux ; que la personne ait besoin d'être accompagnée juridiquement ou psychologiquement ; ou qu'elle souhaite déposer plainte, alerter ou mobiliser les autorités. Ce qui peut se faire par de nombreux moyens (formulaires dédiés, mail, téléphone, sms, tchat). Partager la situation vécue avec des professionnels est de manière générale une bonne chose.

Tout en respectant les règles de confidentialité et de protection des publics, chacun des services listés ci-dessous mènera les utilisateurs à bon port, au besoin en les redirigeant vers d'autres services et même si la qualification retenue par l'utilisateur n'est pas la bonne. Chacun de ces services fournit une ou plusieurs portes d'entrée selon la situation à laquelle les utilisateurs font face. Enfin, la plupart des dispositifs listés ici de manière succincte et non exhaustive apportent des ressources sur les conduites à tenir, que l'on soit utilisateur, parent, proche, victime ou témoin.

Recherche de dispositifs d'appui en cas de violences

Le site Service-public.fr fournit de nombreuses ressources sur les démarches à entreprendre auprès des autorités en cas d'agression ou de violence. Le site recense notamment sur une page dédiée l'ensemble des démarches utiles, des ressources et bonnes pratiques pour lutter contre le cyberharcèlement. Le site offre la possibilité d'échanger en ligne 24h/24 et 7 j/7 par messagerie instantanée avec un gendarme ou un policier lorsqu'il est victime ou témoin de faits de cyberharcèlement et de discrimination.

Assistance, diagnostic et signalement de comportements ou de contenus illicites

Ma Sécurité est la plateforme d'accompagnement des victimes dans leurs démarches, opérée par la police et la gendarmerie nationales. Le site, accessible également par application mobile, recense les informations à connaître en cas de problème : démarches utiles, fiches thématiques, etc. Il oriente directement vers les services, autorités et associations compétentes. Enfin, le site et l'application donnent accès à un outil de discussion instantanée avec un policier ou un gendarme 24h/24 et 7 j/7.

Pharos est le portail officiel de signalement des contenus illicites sur Internet. Violence, mise en danger des personnes, menace ou apologie du terrorisme, injure ou diffamation, incitation à la haine raciale ou discrimination, atteintes aux mineurs, le mot d'ordre est simple : je ne partage pas, je signale à Pharos !

Thésée est la plateforme de signalement pour les victimes d'escroqueries en ligne : piratage de messagerie, chantage, rançongiciels, arnaque sentimentale, sites de vente et petites annonces frauduleuses. Elle permet de déposer plainte à distance, sans se rendre au commissariat.

Arrêtonslesviolences.gouv.fr est une plateforme de signalement gratuite, anonyme et disponible 24h/24 qui assure un accueil personnalisé et adapté par un policier ou un gendarme aux victimes de violences sexuelles ou sexistes au travail, dans la rue, dans le cadre familial ou en ligne.

Cybermalveillance.gouv.fr est le guichet unique interministériel permettant d'orienter particuliers, entreprises, associations, collectivités victimes de tous types de malveillances en ligne. Le site fournit un outil de diagnostic qui oriente en quelques clics les utilisateurs vers les relais les plus pertinents. Il informe également les utilisateurs sur les menaces numériques et les moyens de s'en protéger.

Point de Contact est une association dédiée à l'analyse et à la transmission des signalements des utilisateurs. Après analyse des signalements qui lui sont transmis, l'association les répercute sur les plateformes ou hébergeurs et chez Pharos afin qu'ils soient pris en charge.

e-Enfance/3018 est l'association référente de protection de l'enfance en ligne et l'accompagnement à la parentalité numérique. Reconnue d'utilité publique, elle est le partenaire officiel du ministère de l'Éducation nationale dans la lutte contre le harcèlement entre élèves. Le 3018, opéré par l'association, est le numéro national de prise en charge des jeunes victimes de violences numériques. Gratuit, anonyme et confidentiel, le 3018 est accessible 7/7 de 9h à 23h, par téléphone, Tchat et via l'application 3018. En tant que signaleur de confiance, il dispose d'une procédure de signalement prioritaire pour obtenir la suppression de contenus ou comptes préjudiciables à un mineur en quelques heures.

Dépôt de plainte

Pré-plainte en ligne est un service opéré par le ministère de l'Intérieur qui permet d'effectuer une pré-déclaration en ligne pour des faits d'atteinte aux biens (vol ou escroquerie par exemple) ou certains faits à caractère discriminatoire par un auteur inconnu. Une fois la pré-déclaration remplie, la victime doit prendre rendez-vous au commissariat de police ou à la brigade de gendarmerie pour signer la plainte.

Informations et ressources pédagogiques

Je Protège Mon Enfant est la plateforme d'information et d'accompagnement à la parentalité numérique. Elle propose des outils, des conseils et des ressources pratiques pour mieux informer les parents sur l'exposition des enfants aux écrans et aux contenus potentiellement préjudiciables sur Internet.

Tralalere est une entreprise de l'ESS créatrice d'expériences numériques engageantes pour éduquer par et au numérique. Depuis 15 ans, Tralalere coordonne le Safer Internet France pour la Commission européenne et son programme national de sensibilisation Internet Sans Crainte.

Internet Sans Crainte est le programme national de sensibilisation des jeunes au numérique de la Commission européenne, opéré par Tralalere depuis 2008. Dans ce cadre, Internet Sans Crainte met à disposition des ressources en ligne pour sensibiliser aux pratiques numériques et aux dangers sur Internet et forme les médiateurs éducatifs à la sensibilisation des mineurs.

Le signalement auprès des plateformes

Le site de l'Arcom propose des liens vers les rubriques des conditions générales d'utilisation des principales plateformes (Facebook, Instagram, TikTok, Snapchat, Twitter, Twitch, Pinterest, Dailymotion, Bing, Jeuxvideo.com, BeRreal, Yubo, Wikipédia) et expliquant comment signaler.

L'ensemble du monde associatif

De nombreuses associations accompagnant les utilisateurs dans leurs démarches face à une situation difficile fournissent un travail d'une importance particulière et souvent bénévole. Sans pouvoir toutes les citer, on compte parmi elles : Stop Homophobie, SOS Homophobie, la Licra, la Ligue des droits de l'Homme, #jesuislà, StopFisha, Génération Numérique, Féministes contre le cyberharcèlement, Respect Zone, SOS Racisme et bien d'autres encore.

Quelques faits et chiffres

Les échanges dans le cadre du CNR Numérique ont mis en lumière l'ampleur et la diversité des formes de violences exercées en ligne, qu'il s'agisse de diffamation, de harcèlement, d'expression de haine, d'usurpation d'identité, de piratage, de diffusion non consentie de photos et de vidéos intimes, de révélation d'informations personnelles, de menaces, de raids numériques. Si ces violences sont de plus en plus visibles du grand public et sont de mieux en mieux comprises, il est plus difficile de se représenter la dimension du problème ou encore le travail quotidien d'apaisement de l'espace numérique réalisé par les associations, les autorités, les plateformes et les institutions judiciaires. Les quelques faits et chiffres suivants[1] ont vocation, de manière partielle, à les mettre en lumière auprès du grand public ; avec, en trame de fond, la difficulté permanente à s'accorder sur la licéité des contenus et comportements en cause.

→ Les violences et la haine en ligne nous concernent toutes et tous et prennent des formes bien différentes.

- 41 % des Français déclarent avoir subi des cyberviolences et 31 % admettent en avoir commis[2]. Les plus jeunes sont particulièrement affectés par ces violences : 87 % des jeunes (18-14 ans) y ont déjà été confrontés[3].

- Une enquête conduite par l'association Féministes contre le cyberharcèlement avec Ipsos et publiée en novembre 2022 fait apparaître que « parmi les répondant·es de l'enquête auprès des victimes on retrouve en majorité des femmes (84 % des répondant·es) ainsi que des personnes discriminées en raison de leur identité de genre et leur orientation sexuelle (43 %)[4] ».

- Les violences ont des impacts concrets sur la santé physique et psychique des victimes. Selon la même étude, 80 % des victimes de cyberharcèlement rapportent un impact sur leur santé mentale et 88 % ont eu des troubles anxieux et dépressifs. Chez les jeunes adultes, le cyberharcèlement est un

[1] Les actions portées par les réseaux sociaux ayant participé aux échanges sont égrainées tout au long de cette feuille de route dans une recherche d'équilibre. En effet, tous ne peuvent être cités à chaque fois. Les ressources concernant chacun d'entre eux sont le plus souvent référencées et accessibles en ligne.

[2] Féministes contre le cyberharcèlement, Enquête « Cyberviolence et cyberharcèlement : état des lieux d'un phénomène répandu », novembre 2021.

[3] *Idem*

[4] *Idem*

facteur déterminant dans l'émergence de troubles lourds (insomnie, alimentation, dépression) et 49 % des victimes ont déjà pensé au suicide[5].

- Une étude publiée en 2021 par l'Economist Intelligence Unit fait apparaître que 38 % des femmes ont fait l'objet personnellement d'une forme de violence en ligne, 65 % ont pu témoigner de ce qu'une de leur proche avait subi une telle violence et 85 % ont pu assister à l'exercice de violences sur des femmes[6].

- La même étude fait apparaître que les faits de violence sont souvent commis de façon combinée : diffamation, harcèlement, haine, usurpation d'identité, piratage, diffusion non consentie de photos et de vidéos intimes, révélation d'informations personnelles, menaces, raids numériques. Étant précisé que souvent les agressions se poursuivent dans l'espace tangible : menaces, injures, atteintes physiques et agressions sexuelles.

- La plateforme Pharos a enregistré plus de 237 000 signalements en 2020. Plus de la moitié d'entre eux concerne des escroqueries et extorsions, 8 % concernent des discriminations[7].

- En 2022, la personnalité qualifiée de la CNIL puis l'Arcom ont examiné 82 754 demandes de retrait de contenus à caractère terroriste ou à caractère pédopornographique émises par la plateforme Pharos[8].

- En 2022, l'association de signalement Point de Contact a reçu et traité plus de 40 000 signalements pour des contenus illicites en ligne (pédocriminalité, haine en ligne, etc.).

- Cybermalveillance.gouv.fr est le service de prévention et d'assistance aux particuliers, entreprises et collectivités pour les cybermenaces (arnaque, piratage, harcèlement) auxquelles ils peuvent être confrontés. En 2022, Cybermalveillance.gouv.fr a reçu plus de 280 000 demandes d'assistance[9]. Les situations de cyberharcèlement représentent la 5e raison pour laquelle Cybermalveillance.gouv.fr est sollicitée par les particuliers.

- Le 3018, numéro national pour les violences en ligne sur mineurs, opéré par l'association e-Enfance/3018, est disponible 7 jours sur 7 de 9h à 23h. Il a reçu

[5] e-Enfance / 3018, Plus d'1 jeune adulte sur 2 a déjà été victime de cyberharcèlement, novembre 2022.
[6] Economist Intelligence Unit, Measuring the prevalence of online violence against women, mars 2021.
[7] Selon des chiffres communiqués par Pharos sur son site Internet.
[8] Arcom, Rapport d'activité de la personnalité qualifiée, 18 avril 2023
[9] Cybermalveillance.gouv.fr, Rapport d'activité 2022.

25 000 appels et fait supprimer 10 000 comptes ou contenus préjudiciables en 2022.

- Le Pôle national de lutte contre la haine en ligne (souvent appelé Parquet numérique) a été saisi de plus de 1000 procédures pour des faits de haine en ligne en deux années d'exercice[10].

→ Le signalement des contenus illicites sur Internet est utile.

- Tandis que 7 jeunes sur 10 ont déjà été exposés à du contenu choquant sur internet ou sur les réseaux sociaux, seulement 1 jeune sur 4 signale un contenu choquant ou haineux ou l'auteur de ce contenu auprès de l'administrateur du site ou du réseau social[11].
- Pourtant, Pharos traite les signalements d'utilisateurs pour des contenus illicites en moins de trois heures environ. Les principales associations signaleurs de confiance, telles que Point de Contact, traitent les signalements des utilisateurs en moins d'une journée.
- À la réception des appels (via téléphone, tchat ou l'application 3018), les écoutants du 3018 accompagnent et analysent les demandes des victimes, rassemblent les preuves des violences pour ensuite les transmettre aux réseaux ou plateformes concernés et obtenir la suppression de comptes ou contenus.

→ L'anonymat sur les réseaux sociaux n'est pas le principe.

- Dans le cadre d'enquêtes judiciaires, les forces de l'ordre interagissent avec les plateformes, que ce soit par le biais d'une demande d'entraide pénale internationale ou non, pour obtenir les informations accessibles juridiquement et techniquement concernant l'identité des auteurs de violences en ligne.

→ De nombreux acteurs (autorités, associations, plateformes) contribuent quotidiennement à l'apaisement de l'espace numérique.

- Le taux de prévalence représente le pourcentage estimé de contenus illicites sur une plateforme. En 2022, Instagram estimait que 0,01 % à 0,02 % des

[10] Selon des chiffres communiqués par le pôle dans le cadre des échanges avec le CNR Numérique.

[11] Génération Numérique, Enquête sur les contenus choquants accessibles aux mineurs, asso-generationnumerique.fr, février 2023. A noter qu'ils étaient 1 sur 3 selon l'étude réalisée l'année précédente. Voir Génération Numérique, Enquête sur les contenus choquants et le complotisme, mars 2022.

contenus mettait en avant un discours haineux. 93,9 % des contenus modérés ont été détectés par Instagram avant d'être retirés[12].

- Entre autres organisations et à titre indicatif, e-Enfance/3018 sensibilise 200 000 enfants, jeunes, parents et professionnels par an aux bonnes pratiques sur Internet et les réseaux sociaux. Génération Numérique éduque à la citoyenneté environ 350 000 enfants, adolescents et adultes tous les ans.
- À l'échelle globale et sur le dernier semestre 2021, Twitter a retiré plus de 5 millions de contenus, suspendu près d'1,3 million de comptes et agi sur plus de 4 millions d'entre eux[13]. Ces chiffres sont en nette augmentation depuis 2018 et couvrent globalement toutes les thématiques liées à l'apaisement de l'espace numérique.
- Pour la France, au dernier trimestre 2022, TikTok annonce avoir supprimé 63,2 % des contenus illicites avant que ceux-ci ne soient visionnés[14].
- À partir du 28 août 2023, les très grandes plateformes (dont font notamment partie Youtube, Instagram, Facebook, Snapchat, Twitter et TikTok) devront faire appliquer les dispositions du règlement sur les services numériques : mettre en place des dispositifs de signalement clairs et accessibles pour les utilisateurs, évaluer les risques sur leurs plateformes et prendre des mesures de réduction des risques, être transparents sur leurs efforts et leurs règles de modération.
- De manière générale, quant aux statistiques relatives à la modération, le texte du DSA permettra aux régulateurs (Commission européenne et autorités nationales) de demander des interfaces de programmation d'application, API) pour accéder aux informations pertinentes et demander à des services d'expertise comme le nouveau centre européen pour la transparence algorithmique (l'ECAT) et au Pôle d'expertise de la régulation numérique (le PEReN) de les analyser.

[12] Données déclaratives. Des données complémentaires à ce sujet sont disponibles dans les rapports de transparence d'Instagram.

[13] Données déclaratives. Pour plus d'informations à ce sujet, se référer au centre de transparence der Twitter.

[14] Données déclaratives. Pour plus d'informations, se référer aux rapports de transparence de TikTok.

I. VISIBILISER

Partager les vécus et les actions portées

Lorsque nous sommes en ligne, nous pouvons avoir des expériences très contrastées selon qui nous sommes et ce que nous faisons. Avoir pleinement conscience des situations vécues et des actions portées pour les éviter est une première étape pouvant mener à une compréhension et une qualification commune des violences subies pour, à terme, y apporter une meilleure réponse. De nombreux témoignages, rapports et études s'avèrent être d'une grande richesse à cet égard, mais restent nécessairement partiels et encore trop épars. Une agrégation des ressources disponibles s'avère alors nécessaire (mesure 1). À quoi s'ajoute la nécessité de rendre compte des vécus et des actions portés grâce, d'une part, à un baromètre (mesure 2) et, d'autre part, à un tableau de bord dédiés à l'apaisement de l'espace numérique (mesure 3).

Agréger les rapports et études réalisés

Les rapports de transparence des réseaux sociaux et les évaluations de la Commission européenne

En application du droit européen et depuis de nombreuses années, les plateformes en ligne, dont les principaux réseaux sociaux, sont tenues de retirer les contenus illicites publiés par les utilisateurs. Elles sont également tenues de publier des rapports de transparence sur leurs activités de modération rendant ainsi compte de la quantité de contenus sur lesquelles elles sont intervenues.

La Commission européenne opère un suivi détaillé des activités de modération des plateformes et précise le contenu de ces rapports de transparence. En effet, le Code de conduite pour lutter contre les discours haineux illégaux diffusés en ligne, initié en 2016 par la Commission européenne, établit des lignes directrices pour la modération des contenus par les plateformes. La Commission évalue régulièrement l'application du Code de conduite[15] par les plateformes et compare leurs efforts de modération. Dans le cadre de la mise en œuvre du règlement sur les services numériques, adopté en fin d'année 2022 et actuellement en cours de mise en œuvre, les obligations des plateformes se verront renforcées.

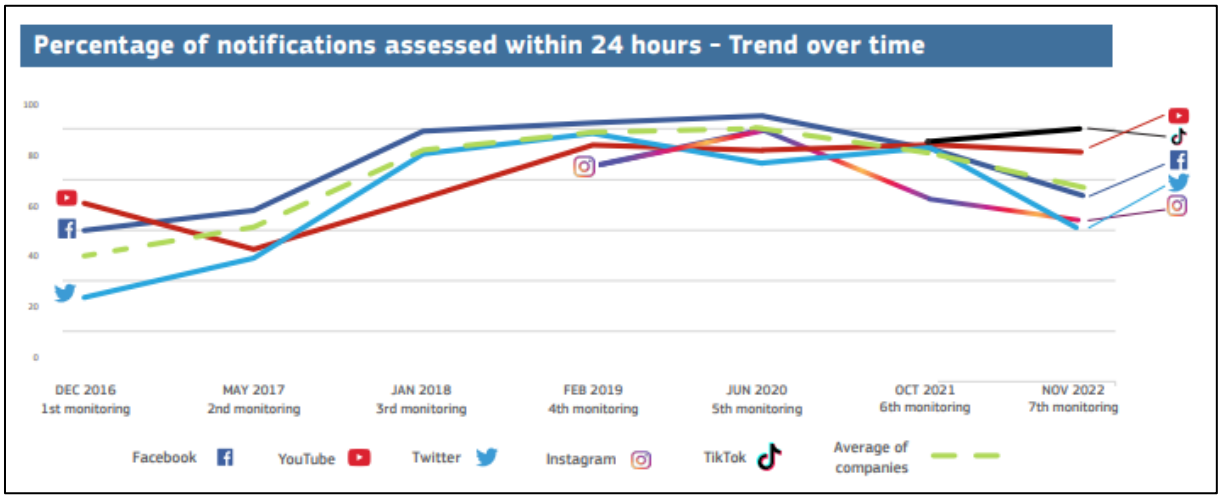
Qu'est-ce que la modération des contenus sur les réseaux sociaux ?

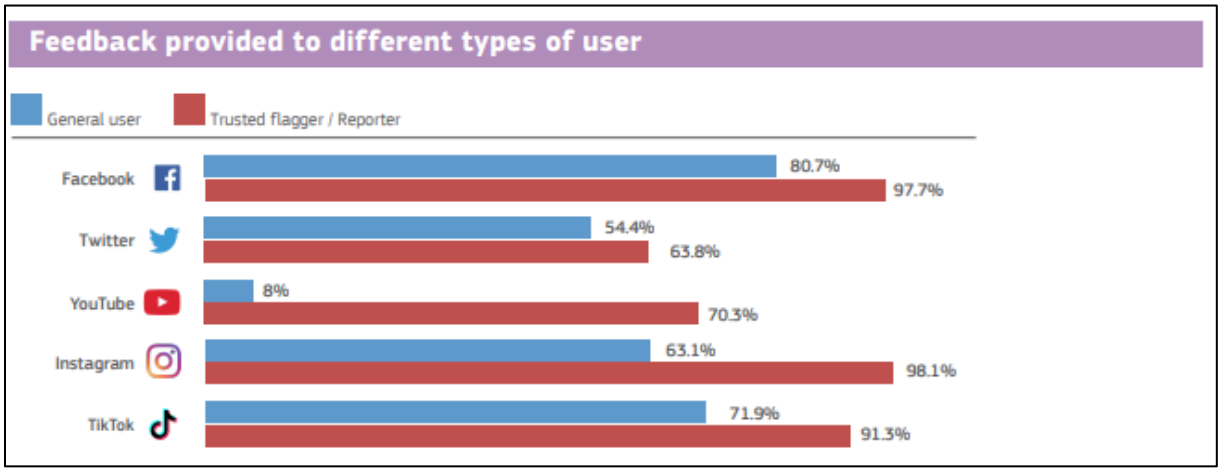
La modération est l'activité par laquelle un réseau social définit et applique les règles à suivre sur son réseau social, qu'elles émanent de la loi ou des règles d'utilisation des réseaux sociaux en cause. En vertu de règles applicables en France depuis l'adoption de la loi pour la confiance dans l'économie numérique du 21 juin 2004, les services en ligne que l'on qualifie d'hébergeurs — une qualification encore appliquée à ce jour aux réseaux sociaux pour leurs activités principales — ont l'obligation de retirer des contenus lorsqu'ils ont connaissance de leur caractère manifestement illicite.

Cette connaissance peut leur être apportée par le signalement des utilisateurs ou par décision de justice, par exemple suite à une procédure en référé, une procédure d'urgence traditionnelle dont une déclinaison existe spécifiquement en matière de communication au public en ligne. Le règlement sur les services numériques (*Digital Services Act*) approfondit les obligations des hébergeurs en matière de modération, notamment pour ceux qualifiés de plateformes. Entre autres obligations, toutes les plateformes devront informer l'utilisateur de la décision prise sur son signalement et lui indiquer les voies permettant de contester la décision prise.

[15] Commission européenne, "Countering illegal hate speech online : 7th evaluation of the Code of Conduct", novembre 2022

Le code de conduite européen précité et déjà mis en œuvre par les principaux réseaux sociaux a pour objectifs de responsabiliser les plateformes dans la modération des contenus illicites et d'assurer un suivi de cet exercice de modération année après année. Dans ce cadre, la Commission européenne publie régulièrement des évaluations des activités de modération par les plateformes permettant rendre compte de manière indépendante des efforts fournis. Ainsi, la septième évaluation de la mise en œuvre du code de conduite publiée en novembre 2022 compare l'évolution de l'efficacité de la modération des plateformes en rendant compte du pourcentage de signalements traités dans les 24 heures suivant leur notification. La septième évaluation compare également les politiques de modération des plateformes en fonction du retour fourni au signalant.





Source : Commission européenne, « Factsheet - 7th monitoring round of the Code of Conduct », novembre 2022

Dans la poursuite des exigences portées au niveau européen à travers les codes de conduite ou encore en droit national à travers la mise en œuvre de la loi pour la confiance dans l'économie numérique du 21 juin 2004, les plateformes sont tenues à un certain effort de transparence. Ainsi les plateformes sont notamment tenues de rendre publics au moins une fois par an des rapports de transparence concernant leurs activités de modération et contenant des informations sur leur activité de modération. Ces rapports, plus ou moins riches, contiennent des chiffres produits par les plateformes à partir de leurs activités ou à partir d'audits extérieurs.

Ainsi, certains réseaux sociaux mettent en avant un chiffre qui est celui du taux de prévalence. Tel que décrit par Meta, « la prévalence prend en considération toutes les vues de contenus sur Facebook et Instagram et mesure le pourcentage estimé des vues qui concernent des contenus en infraction. » Par exemple, au dernier trimestre 2022, la prévalence du harcèlement sur Facebook, tel que calculé par le groupe, était entre 0,07 % et 0,08 %[16].

Le taux de proactivité représente le pourcentage de l'ensemble des contenus sur lesquels la plateforme est intervenue (retrait ou dissimulation du contenu, etc.) et qui ont été détectés avant qu'un utilisateur ne signale le contenu. Ce taux vise à mesurer l'efficacité des outils de détection et de modération des contenus des plateformes. Ainsi, au dernier trimestre 2022, 61 % des contenus traités par Meta étaient détectés par la plateforme, quand 39 % des contenus traités étaient signalés par des utilisateurs et associations.

De manière générale, la transparence des plateformes vis-à-vis de leurs efforts de modération est primordiale pour assurer une confiance entre les plateformes, les autorités et surtout les utilisateurs. C'est pourquoi, en anticipation de l'adoption du règlement européen sur les services numériques, l'article 6-4.I.3° de la loi pour la confiance dans l'économie numérique impose aux opérateurs de plateforme de décrire entre autres choses et « en termes clairs et précis leur dispositif de modération visant à détecter, le cas échéant, à identifier et à traiter ces contenus, en détaillant les procédures et les moyens humains ou automatisés employés à cet effet ainsi que les mesures qu'ils mettent en œuvre affectant la disponibilité, la visibilité et l'accessibilité de ces contenus[17] ».

De leur côté, de nombreuses associations publient des études et analyses sur le traitement des contenus illicites en ligne et la situation de certains publics. Leur publication permet de visibiliser les vécus des utilisateurs et d'objectiver des situations qui pourraient sinon se voir discréditées car jugées subjectives.

[16] De plus amples détails sont disponibles ici.

[17] Pour une mise en œuvre récente de cette obligation, voir l'ordonnance n°90382 rendue par la Cour de cassation le 23 mars 2023 dans une affaire opposant plusieurs associations à Twitter.

Les études réalisées par la société civile

Le monde associatif est riche d'enquêtes portant sur les causes touchant de nombreuses catégories d'utilisateurs. Une première chose sera de rassembler les informations existantes sur les phénomènes observés. Cela permettra d'informer le public sur la situation, de rendre honneur au travail réalisé par les associations engagées contre les violences en ligne et de construire des actions en faveur des causes concernées.

Ci-dessous, nous donnons à voir pour illustration uniquement et sans aucune visée exhaustive, trois études dont les résultats sont récents et portent sur la question du cyberharcèlement, la question de la haine en ligne ainsi que sur l'exposition des plus jeunes à certains contenus. Au premier titre pourra être évoquée l'étude réalisée par l'association **Féministes contre le cyberharcèlement** avec l'institut de sondage Ipsos (voir encart en fin de partie). L'immense avantage de cette étude réside dans le fait que la méthode employée répond aux exigences les plus strictes en la matière. Elle fait alors apparaître des résultats importants rappelés ci-dessous sur le vécu en ligne des femmes.

Source : Féministes contre le cyberharcèlement, Cyberviolence et cyberharcèlement : état des lieux d'un phénomène répandu, novembre 2021

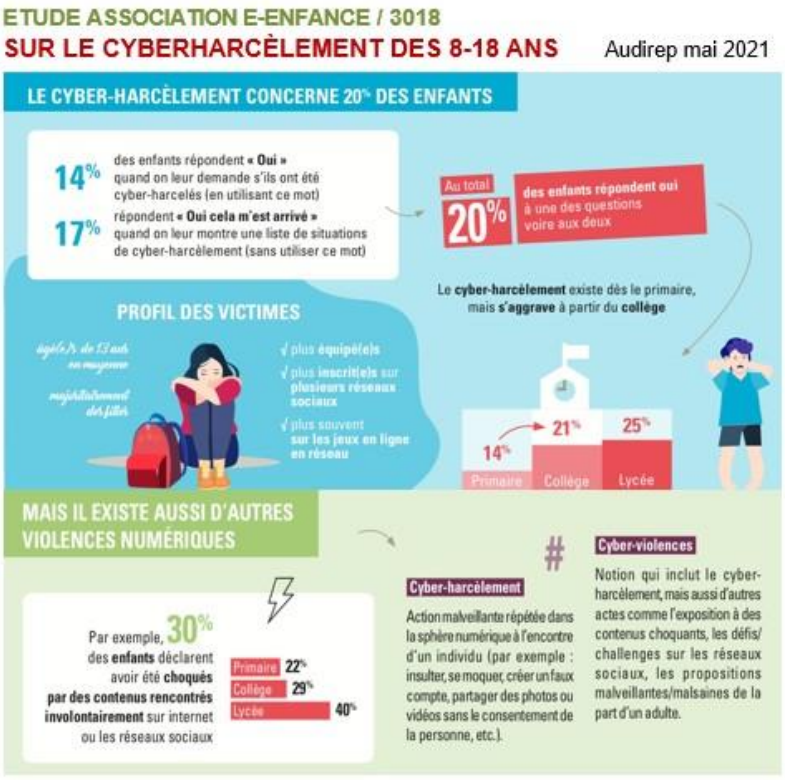
L'enquête annuelle menée par **Génération Numérique** sur l'exposition des jeunes aux contenus choquants[18] est une autre enquête riche en conclusions sur le rapport au numérique des populations les plus jeunes. Cette enquête, réalisée sur des jeunes âgés de 11 à 18 ans, permet de prendre conscience de l'ampleur de l'exposition des jeunes aux contenus choquants en ligne (scènes de violences, propos racistes, propos injurieux ou haineux liés à une religion) et des comportements que ces jeunes adoptent lorsqu'ils y sont confrontés.

Selon l'enquête, 7 jeunes sur 10 ont déjà été exposés à du contenu choquant sur internet ou sur les réseaux sociaux, notamment du contenu particulièrement traumatisant pour les populations les plus jeunes : des scènes de guerre, de torture et de violence (pour 26 % des répondants). Confrontés à ce type de contenus, 23 % des répondants affirment en parler à un adulte et seulement 1 jeune sur 4 signale le contenu choquant ou haineux ou l'auteur de ce contenu auprès de l'administrateur du site ou du réseau social.

Source : Génération Numérique, Enquête sur les contenus choquants accessibles aux mineurs, asso-generationnumerique.fr, 2023.

Dans la même veine, l'étude[19] réalisée en 2021 par l'association e-Enfance/3018 met en lumière que le cyberharcèlement existe dès le primaire et s'aggrave tout au long de la scolarité. 20 % des 8-18 ans en ont été victimes de cyberharcèlement, 25 % pour les lycéens et les victimes de cyberharcèlement sont en majorité des femmes.

[18] Génération Numérique, Enquête sur les contenus choquants accessibles aux mineurs, asso-generationnumerique.fr, 2023.
[19] Etude d'e-Enfance/3018 et de la Caisse d'Epargne sur le cyberharcèlement des jeunes adultes, 8 novembre 2022.



Enfin, l'étude[20] réalisée par l'IFOP pour Gamertop en 2023 se penche particulièrement sur le cas des violences sexistes et sexuelles dans le milieu du jeu vidéo. 53 % des joueuses qui ont répondu à l'enquête affirment avoir été victime ou témoin au moins une fois d'une situation de sexisme en ligne. De nombreuses formes de sexisme ont été recensées : remarques désobligeantes sur le physique, propos obscènes et commentaires à connotation sexuelle, menaces d'agressions sexuelles, etc. Confrontées à ces violences, de nombreuses joueuses (40 %) sont alors contraintes de dissimuler leur genre en ligne voire même d'arrêter le jeu en ligne.

Si ces enquêtes se fondent sur le ressenti et le vécu des populations interrogées, l'étude « Cartographie de la haine en ligne : étude du discours haineux en France » publiée par l'Institute for Strategic Dialogue[21] en 2020 adopte une méthodologie alternative qui mériterait d'être complétée et poursuivie par un examen approfondi. Cette étude analyse les dynamiques et l'ampleur des discours haineux en France grâce à des outils d'analyse de données sur les réseaux, utilisant l'apprentissage automatique, le traitement du langage naturel et l'analyse quantitative. Elle recense près de 7 millions de cas de discours haineux en ligne contre les femmes, les personnes de la communauté LGBTQ, les personnes handicapées et les communautés arabes françaises. Il en ressortirait que 19 % des comptes haineux les plus actifs présentent un comportement automatisé ou voisin. L'étude relève également que les types de

[20] Gamertop, « Quand sexisme et jeux vidéo font (encore) bon ménage – Une enquête exclusive de l'IFOP pour Gamertop », 26 avril 2023.
[21] Institute for Strategic Dialogue, "Cartographie de la haine en ligne : étude du discours haineux en France", 2020

discours haineux se recoupent : à l'instar des discriminations dans l'espace tangible, la haine en ligne est intersectionnelle, ce qui suppose de l'analyser en tant que phénomène systémique.

Les différentes études relatives aux comportements illicites et haineux en ligne sont complémentaires dans leurs approches et leurs objets d'étude et méritent d'être visibles en un point unique. Cela permettra de faciliter la comparaison entre les approches retenues par les acteurs, notamment pour parvenir à une compréhension et une qualification commune des phénomènes à l'œuvre — ce qui n'est pas le cas à ce jour — et ainsi de permettre un dialogue sur la base des constats partagés. Le rassemblement de ces études devra permettre de nourrir un dialogue entre parties prenantes sur le sens et l'amélioration des indicateurs statistiques, pour faciliter la compréhension du phénomène et mieux apprécier les efforts de modération des plateformes. Un tel travail est actuellement en cours au PEReN et pourra ainsi être communiqué prochainement.

Enfin, l'ensemble des informations chiffrées pouvant être mises à disposition par les autorités publiques (police, gendarmerie, parquet, juridictions, etc.) pourraient être rassemblées. Ainsi, pourraient être mieux compris à la fois les phénomènes en cause et la chaîne de traitement des cas portés à l'attention des autorités. Les points de fragilité dans le dispositif global pourraient alors être mieux identifiés.

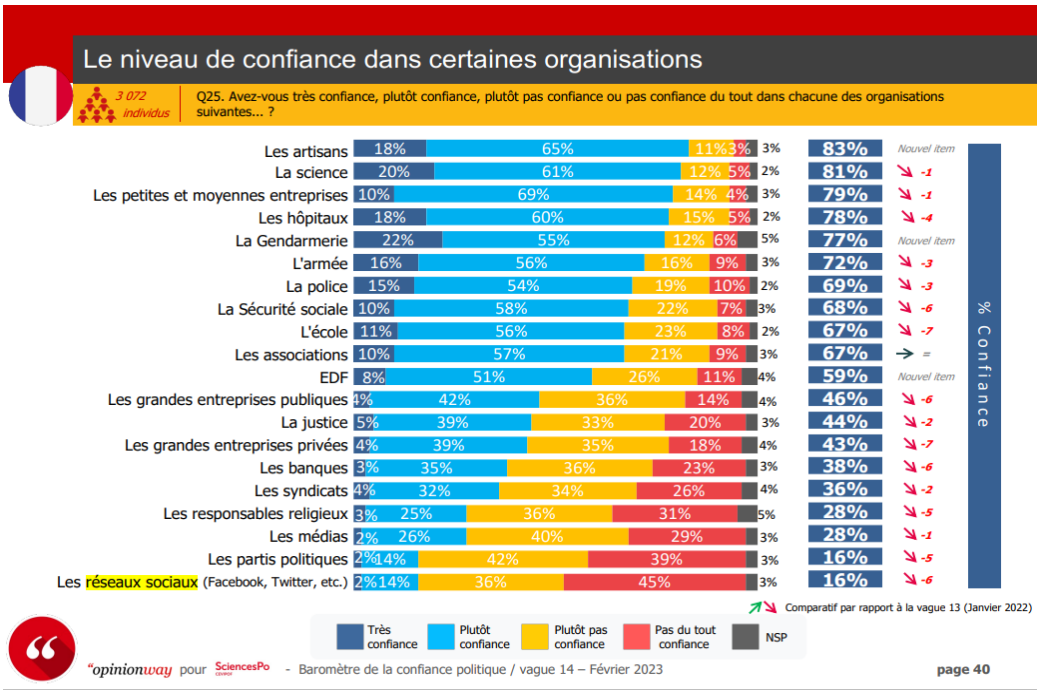
Mesure 1 – *Les études et rapports sur les comportements illicites en ligne, leur modération et leur traitement seront rassemblés sur un site dédié.*

Créer un baromètre de l'apaisement de l'espace numérique

Les études et rapports produits à ce jour guident utilement l'action publique en apportant une visibilité d'intérêt général sur les problématiques qu'elles abordent. Or, les rapports de transparence ne prennent pas le problème sous l'angle du vécu des utilisateurs. De tels travaux dépendent quant à eux le plus souvent de la capacité à agir des associations et ne peuvent couvrir l'ensemble des problématiques liées à nos communications en ligne. Ainsi émerge la nécessité de confier à l'ensemble des autorités intéressées la construction d'un baromètre sur l'apaisement de l'espace numérique en lien avec des instituts de recherche et le monde associatif.

Les baromètres existants

Un premier exemple de ce type est le **Baromètre de la confiance politique** du Centre de recherches politiques de Sciences Po (CEVIPOF). Question éminemment subjective, la confiance y est plus ou moins objectivée grâce à l'application d'une méthodologie rigoureuse, éprouvée par de nombreuses vagues de sondage année après année. Grâce à ce baromètre, et avec toutes les réserves nécessaires, il apparaît par exemple que les Français feraient particulièrement confiance dans les institutions régaliennes, dans la science, l'artisanat, mais pas du tout dans les « réseaux sociaux ». En ce sens, 81 % des répondants déclarent n'avoir « pas du tout » ou « plutôt pas » confiance dans les réseaux sociaux. Beaucoup de biais peuvent s'introduire dans le processus, mais les résultats renseignent tout de même sur une tendance lourde.

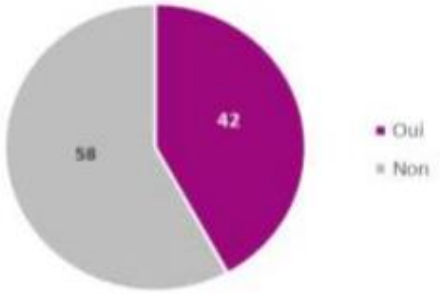


Source : Sciences Po, Baromètre de la confiance politique, sciencespo.fr, février 2023

Sur cette base, l'étude du vécu des Français en ligne pourrait être approfondie grâce à des questions portant sur les sentiments de sécurité, de confiance, d'enrichissement, de plaisir, de découverte. Ce rapport aux réseaux sociaux pourrait aussi être décliné par types d'usages et par réseau social. Tous les réseaux n'ont pas la même vocation, tous les Français n'en ont pas le même usage. Apporter plus de détails dans le rendu de la perception des Français de leur expérience en ligne peut être intéressant.

Le **Baromètre du numérique**[22] réalisé par le Credoc et piloté par le CGE, l'ANCT, l'Arcep et l'Arcom couvre un grand nombre de questions relatives à l'accès et aux usages du numérique des Français. Il fournit des éléments d'analyse et de suivi fondamentaux pour la conduite de l'action publique. Il est d'ailleurs à observer qu'en l'état le Baromètre du numérique contient quelques informations utiles sur les questions intéressant l'apaisement de notre vie en ligne. Ainsi, à l'initiative de l'Arcom, l'édition 2022 a fait apparaître que 87 % des sondés jugeaient les interfaces de signalement des plateformes facilement accessibles et que 85 % des participants les jugeaient simples d'utilisation. Pourtant, seuls 4 répondants sur 10 affirment avoir déjà utilisé un dispositif de signalement, ce qui permet de contextualiser le sentiment d'accessibilité des dispositifs de signalement des répondants.

Graphique 178
Les réseaux sociaux (Facebook, Twitter, Snapchat, Instagram, etc.) et les plateformes de partage de vidéos (YouTube, Dailymotion, etc.) ont mis en place des dispositifs permettant de signaler des comptes ou des contenus inappropriés. Avez-vous déjà utilisé un de ces dispositifs de signalement ?
- Champ : ensemble des internautes de 12 ans et plus, en % -



Source : CREDOC, Baromètre du numérique, 2022

Il apparaît également que les pratiques de signalement de comptes et de contenus inappropriés varient grandement en fonction du profil du signalant : alors que dans les populations les plus jeunes (entre 12 et 39 ans), la majorité a déjà signalé un compte ou un contenu, la proportion de signalants décroît fortement avec l'âge.

Ces questions mériteraient d'être approfondies et enrichies. Sur le signalement, de nombreuses questions pourraient être posées. Quelle est l'efficacité perçue ? Pour quel type de problème ont-ils signalé ? Quels dispositifs de signalement connaissent-ils ? Les utilisateurs connaissent-ils leur finalité ? Comment apprécient-ils leurs interfaces ? Quel a été le résultat ?

[22] CREDOC, Baromètre du numérique, credoc.fr, 2023.

Comme évoqué précédemment, le règlement européen sur les services numériques adopté en octobre 2022 impose aux plateformes de mettre en place des dispositifs de signalement faciles d'accès et d'utilisation. Elles devront indiquer aux utilisateurs la décision retenue à la suite de leur signalement et les orienter vers des voies de recours internes et externes. Sonder les usagers sur la pertinence des dispositifs existants sera instructif pour assurer que la mise en œuvre des nouvelles obligations va dans la bonne direction.

Néanmoins, le Baromètre du numérique ne peut accueillir de trop nombreuses questions sur une thématique donnée sans atteindre un seuil limite de personnes interrogées. Ce qui confirme que les questions qui se posent sur l'apaisement de l'espace numérique doivent bien faire l'objet d'un questionnaire spécifique.

Les consultations menées sur le site du CNR

Deux consultations publiques réalisées depuis le site du CNR ont confirmé l'intérêt d'approfondir certaines questions. Tout en étant limitées d'un point de vue méthodologique, ces consultations ont posé la question aux personnes intéressées de savoir quelle était leur connaissance des dispositifs de signalement existants.

La deuxième consultation en ligne réalisée dans le cadre du CNR Numérique s'intéressait à la popularité des plateformes de signalement ou d'assistance. Chez une population semble-t-il familière du numérique, Pharos apparaîtrait comme la plateforme de signalement la plus populaire avec 47 % des répondants qui en ont déjà entendu parler. À côté de quoi 32 % des répondants ont entendu parler de Cybermalveillance.gouv.fr. Tandis qu'une part non négligeable des répondants (41 % d'entre eux) n'ont jamais entendu parler de Pharos ni de Cybermalveillance.gouv.fr.

Au-delà des réponses obtenues, le questionnaire a enfin été l'occasion de recueillir des recommandations pour améliorer la protection des mineurs dans l'espace numérique. Près de 48 % des participants appellent à la formation et à la sensibilisation des plus jeunes, notamment dans le milieu scolaire. 30 % des participants pensent qu'il est nécessaire d'accompagner les parents, afin qu'ils protègent mieux leurs enfants en ligne.

Déployer un baromètre dédié à l'apaisement numérique permettra d'approfondir de nombreuses questions et de guider la conduite de l'action publique. Sa régularité fournira un rendez-vous à l'ensemble des acteurs, permettra de mesurer le chemin parcouru comme celui restant à parcourir et de donner alors les orientations pour les années à venir en actionnant les leviers les plus pertinents. Cet exercice s'avérera aussi particulièrement utile pour guider les acteurs de la régulation en complément de l'exercice à venir dans le cadre de la mise en œuvre du règlement européen sur les services numériques.

La complémentarité d'un baromètre avec la mise en œuvre du règlement sur les services numériques

Cet exercice d'objectivation complétera utilement la qualification des phénomènes à l'œuvre dans le cadre de la mise en place du cadre de régulation à venir, un exercice délicat requérant d'accorder des visions parfois divergentes. En effet, un des problèmes auquel nous sommes collectivement confrontés est que les phénomènes observés ne sont pas qualifiés de la même façon. Là où en tant que citoyen nous pouvons voir des faits de violence, la loi verra des faits de discrimination, là où telle personne verra un droit à la parodie, tel acteur verra une atteinte à tel droit ou liberté.

Ces questions se posent tous les jours aux plateformes et aux autorités. Elles rendent le travail de modération souvent très délicat et requièrent une grande connaissance, à la fois des règles applicables et des modes d'expression sur les réseaux.

La divergence de qualification appliquée aux phénomènes observés induit aussi que lorsque chacun des acteurs communique sur la modération ou du signalement, il applique nécessairement une grille de lecture qu'il aura préalablement établie, étant précisé qu'il faut aussi distinguer ce qui ressort de la loi de ce qui ressort des atteintes au règlement de la communauté. Publier un propos donné peut selon les cas être illégal ou uniquement contraire au règlement d'utilisation d'un réseau social ; ce qui modifie la grille d'appréciation de chaque acteur et ainsi les résultats communiqués.

Enfin, dans le cadre de la régulation à venir, les plus grandes plateformes devront justifier avoir mis en œuvre les moyens nécessaires à l'atténuation des risques systémiques qu'ils véhiculent. Tout comme les plus grands réseaux sociaux, les autres plateformes devront quant à elles donner suite aux signalements des utilisateurs. Leurs décisions devront parvenir aux utilisateurs concernés qui pourront le cas échéant faire l'objet de recours devant des organes dédiés. Les signaleurs de confiance désignés publieront des rapports annuels rendant compte des divergences d'appréciations ou de traitement entre les plateformes et eux. L'ensemble de ces processus exigent nécessairement de qualifier les phénomènes à l'œuvre d'un point de vue juridique.

Le baromètre de l'apaisement numérique indiquera pour sa part les phénomènes auxquels les utilisateurs sont les plus sensibles ainsi que leur degré de satisfaction et de connaissance. Il pourra nourrir les échanges d'une autre perspective et orienter utilement le travail de l'ensemble des acteurs, plateformes, autorités ou associations. Son pilotage, en lien avec les autorités concernées, pourrait être confié au coordinateur pour les services numériques en France, dont le rôle devrait être dévolu à l'Arcom, selon le projet de loi « Sécuriser et réguler l'espace numérique ».

Mesure 2 *—Un baromètre annuel de l'apaisement de l'espace numérique sera créé.*

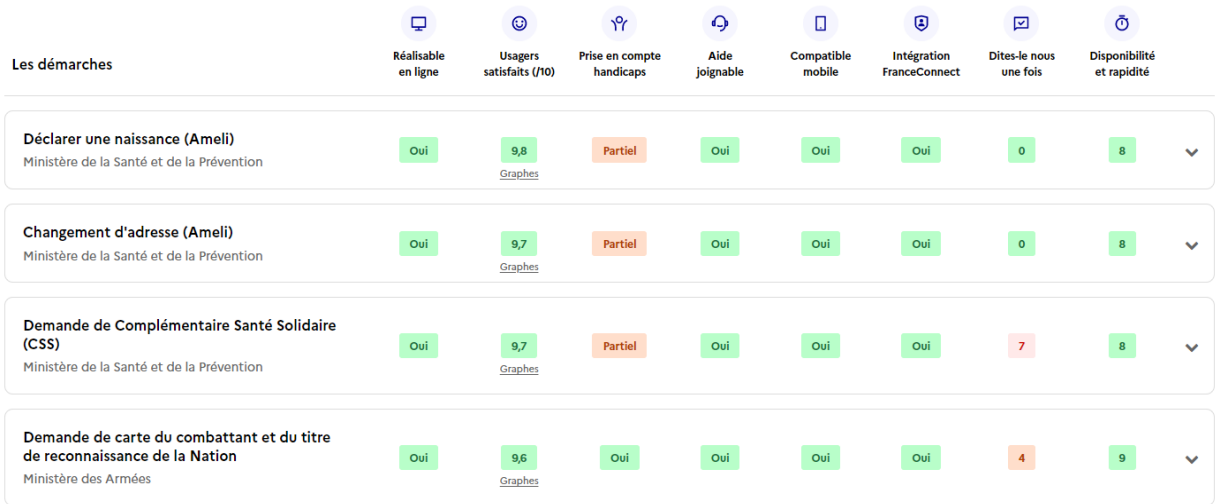
Générer un tableau de bord des actions portées

Si objectiver le ressenti des utilisateurs est important, il importe tout autant de rendre compte des actions conduites par les acteurs concernés autour de l'apaisement de l'espace numérique. Une des grandes vertus des réunions organisées dans le cadre du CNR Numérique fut la capacité offerte aux acteurs de faire connaître à un public plus large les actions qu'ils conduisent et d'entrer ensuite dans un dialogue.

Dans les encarts ci-après, certains réseaux sociaux rendent compte de leur fonction de modération ainsi que des actions de sensibilisation et des campagnes qu'ils ont mises en place. Ces démarches sont complétées par les nombreuses actions portées par la société civile et les autorités publiques. Démultiplier ces actions et donc les moyens mis à disposition renforcera la confiance mutuelle entre la société civile organisée, les plateformes, les utilisateurs et les autorités.

Outre le fait que les acteurs du signalement tels que Point de Contact ou Pharos ne sont pas toujours connus du public, les modes de signalement sur les plateformes ne sont pas non plus toujours bien compris ou utilisés à bon escient. Mettre en avant les dispositifs existants et leurs qualités sera une manière d'orienter les acteurs vers des dispositifs toujours plus optimaux mais aussi un moyen d'informer les utilisateurs.

Pour mettre en visibilité les actions entreprises, les outils du type tableau de bord sont particulièrement utiles. Les autorités publiques ne sont d'ailleurs pas étrangères à ce type de dispositifs. Parmi les tableaux de bord existants, on pourra relever notamment l'Observatoire de la qualité des démarches en ligne qui rassemble les 250 démarches phares de l'État pour leur appliquer des critères de qualité. Ce tableau de bord, consultable par tout un chacun, permet d'assurer un suivi de l'accessibilité et de la facilité d'utilisation des démarches en ligne.



Les démarches	Réalisable en ligne	Usagers satisfaits (/10)	Prise en compte handicaps	Aide joignable	Compatible mobile	Intégration FranceConnect	Dites-le nous une fois	Disponibilité et rapidité
Déclarer une naissance (Ameli) Ministère de la Santé et de la Prévention	Oui	9,8 Graphes	Partiel	Oui	Oui	Oui	0	8
Changement d'adresse (Ameli) Ministère de la Santé et de la Prévention	Oui	9,7 Graphes	Partiel	Oui	Oui	Oui	0	8
Demande de Complémentaire Santé Solidaire (CSS) Ministère de la Santé et de la Prévention	Oui	9,7 Graphes	Partiel	Oui	Oui	Oui	7	8
Demande de carte du combattant et du titre de reconnaissance de la Nation Ministère des Armées	Oui	9,6 Graphes	Oui	Oui	Oui	Oui	4	9

Source : Observatoire de la qualité des démarches en ligne, observatoire.numerique.gouv.fr.

D'autres tableaux de bord peuvent être mentionnés à titre d'exemple, avant tout pour montrer la malléabilité d'un tel outil :

- Le tableau de bord du *New Deal* mobile de l'Arcep[23], assure un suivi trimestriel de la mise en œuvre des obligations des opérateurs et de l'amélioration de la couverture mobile.
- Le baromètre des résultats de l'action publique[24] a été créé en 2021 pour rendre visibles les résultats des politiques prioritaires du Gouvernement.
- L'indice de l'économie et de la société numériques (DESI) agrège les indicateurs des performances numériques de l'Europe dans de nombreux domaines (capital humain, connectivité, intégration de la technologie numérique, services publics numériques) et permet d'assurer une comparaison entre les différents pays européens.

Un tableau de bord dédié à l'apaisement de l'espace numérique permettra d'apprécier de manière objective les avancées réalisées par les acteurs, de les faire connaître, mais également de diffuser les meilleures pratiques afin qu'elles puissent guider les actions des uns et des autres. D'ailleurs, le règlement européen sur les services numériques donne à la Commission européenne la compétence d'établir les bonnes pratiques en matière de signalement[25]. Un tableau de bord rendant compte des pratiques des acteurs permettra d'orienter au mieux un tel travail tout en mettant en miroir les évolutions des plateformes avec les travaux engagés par la société civile. À ce dernier titre, un catalogue des formations et actions territoriales entreprises par la société civile pourra être d'une grande utilité et participer au soutien des acteurs de la citoyenneté numérique (cf. Mesure 6).

Qui plus est, un point souvent relevé par les participants est l'absence d'homogénéité ou de lisibilité des catégories de signalement. Le tableau de bord permettra d'initier l'harmonisation des critères et catégories de signalement sur les plateformes, étant précisé que la recherche de cohérence doit aussi s'appliquer au secteur public.

De manière générale, il s'agit de capitaliser sur ce qui est fait pour faire connaître ce qui existe pour aller toujours un cran plus loin, sans se limiter à critiquer ce qui est mal fait. À ce titre, certains dispositifs de signalement rapides ne sont pas tous connus (rester appuyé 3 secondes sur une vidéo sur certains réseaux) tandis que d'autres sont plus visibles (bien identifiés sur fond rouge). D'autres améliorations pourraient alors

[23] Arcep, « Suivi du New Deal mobile : indicateurs réseaux et services mobiles, derniers chiffres T4 2022 », mis à jour le 13 avril 2023

[24] Direction interministérielle de la transformation publique, « Le baromètre des résultats de l'action publique ».

[25] En ce sens, l'article 35 du règlement sur les services numériques prévoit que la Commission peut définir des bonnes pratiques et recommander des mesures possibles aux fournisseurs de très grandes plateformes en ligne en vue de l'atténuation des risques systémiques posés par ceux-ci.

émerger comme par exemple la facilitation de l'établissement des preuves, la généralisation du signalement de contenus en masse, ou encore le signalement de plusieurs comptes de manière simultanée.

Le tableau de bord des mesures prises pour veiller à l'apaisement de l'espace numérique pourra enfin recueillir les mesures prises par les plateformes au titre de la mise en œuvre du règlement européen sur les services numériques. Ainsi, il permettra de rendre visibles et intelligibles les fruits de la régulation au niveau européen dont les atouts ne sont pas forcément tangibles sinon pour l'utilisateur. Réciproquement, il permettra enfin de mettre en exergue d'éventuels manquements à agir et qu'il s'agira de résoudre afin de maintenir un niveau de confiance suffisant.

Un tel tableau de bord pourra inclure de nombreuses catégories qui seront identifiées au fil de l'eau par les acteurs mais qui pourraient graviter autour de thèmes comme :

- La facilité du signalement (accessibilité, temps de réponse, etc.)
- Les dispositifs de modération (moyens déployés pour la France, recours aux dispositifs d'intelligence artificielle et impact, gouvernance de la modération : utilisateurs ou employés, etc.)
- Déploiement de dispositifs de prévention (messages aux utilisateurs, campagnes, etc.)
- Redirection vers des dispositifs de signalement ou de plainte gouvernementaux

Mesure 3 —*Un tableau de bord des actions conduites pour l'apaisement de l'espace numérique rendra compte des actions portées par les acteurs publics et privés.*

La parole aux acteurs

Le règlement sur les services numériques

Une présentation réalisée par l'Arcom

Les plateformes numériques (réseaux sociaux, plateformes de partage de vidéos…) permettent aux internautes d'échanger tous types d'informations. Elles occupent désormais, de ce fait, une place de choix et disposent d'un pouvoir important dans l'espace informationnel public. Elles ont considérablement fait évoluer les espaces et les formes d'expression et d'échange, ainsi que les mécanismes d'information et de formation de l'opinion publique. En constante mutation, elles offrent ainsi une myriade de possibilités en matière de débat démocratique, de créativité ou encore d'innovation. Elles véhiculent toutefois également des risques préexistants qui y trouvent des modalités de diffusion et d'amplification nouvelles : désinformation, fraude, haine, mise en danger des personnes…

Le régime de responsabilité limitée des hébergeurs, qui s'applique à ces plateformes et va de pair avec leur interdiction de surveillance généralisée des contenus, n'était plus à même, à lui seul, d'apporter une réponse adaptée à ces enjeux. Il fallait donc faire émerger une régulation adaptée qui prenne en compte le rôle des plateformes en matière de circulation des informations sur leur service de par leurs outils de recommandation et leurs fonctionnalités sociales. Des initiatives nationales ont vu le jour, notamment en France où le législateur a consacré l'existence des plateformes en ligne en les définissant dans la loi pour une République numérique du 7 octobre 2016.

En 2018, la loi a imposé à ces acteurs un devoir de responsabilité dans la lutte contre la manipulation de l'information : ils étaient désormais tenus de déployer des moyens pour œuvrer à cette lutte, en fournissant aux utilisateurs un mécanisme de signalement, des explications sur leurs systèmes de recommandation de contenus ou encore des informations sur les personnes ayant financé la promotion de contenus liés à un débat d'intérêt général. Trois ans plus tard, le Parlement français a complété ces obligations de moyens d'un volet portant sur la lutte contre la haine en ligne.

Chargée de veiller à la mise en œuvre de ces obligations, l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom) a développé un dialogue exigeant avec les grandes plateformes en les poussant davantage chaque année à améliorer les mesures mises en œuvre et la transparence de leurs actions et de leur fonctionnement vis-à-vis du public, dans le strict respect de la liberté d'expression des utilisateurs.

Le règlement européen sur les services numériques (RSN) s'inscrit dans cette logique. Il instaure un nouveau régime de responsabilité des intermédiaires numériques fondé sur des obligations de moyens et un devoir de vigilance. Les fournisseurs de services intermédiaires (ensemble plus large englobant les plateformes en ligne) doivent lutter

contre les contenus et comportements illicites sur leur service et garantir un environnement sûr et prévisible à leurs utilisateurs, notamment aux consommateurs.

Les apports du RSN sont multiples. Tout d'abord, il crée un cadre harmonisé à l'échelle européenne, permettant à l'Union de parler d'une seule voix à des acteurs numériques d'une envergure internationale. Pour cela, il impose des règles unifiées et crée un dispositif assurant une coordination multilatérale et bilatérale étroite entre les États membres et la Commission européenne. Ensuite, il instaure une régulation asymétrique, avec des obligations proportionnées à la nature des activités du fournisseur de service intermédiaire et à son impact sur la circulation des informations sur son service : plus cet impact est important, plus ses obligations sont contraignantes.

En particulier, les très grandes plateformes en ligne et les très grands moteurs de recherche (ceux qui sont utilisés par au moins 10 % de la population de l'Union, soit 45 millions de citoyennes et citoyens européens) sont désormais tenus responsables des risques « systémiques » que représente leur service sur les sociétés. Sous le contrôle d'auditeurs indépendants et de la Commission européenne et des États membres, ils doivent, chaque année, identifier ces risques et prendre des mesures pour les atténuer. Parmi ces risques que représentent les plateformes et leurs usages, le RSN identifie notamment :

- leurs effets négatifs sur l'exercice des droits fondamentaux, le discours civique, les processus électoraux et la sécurité publique ;
- leurs risques pour la santé publique et les personnes, en particulier les mineurs ;
- la diffusion de contenus illicites ;
- la protection des personnes (dont les mineurs), notamment des consommateurs.

Ils doivent également lutter contre les contenus trompeurs et mensongers, et en particulier la désinformation.

Mesure inédite, le RSN permet aux chercheurs, dans certaines conditions, d'accéder aux données de ces grands opérateurs pour participer à la détection des risques systémiques et à l'évaluation des mesures d'atténuation prises en conséquence.

Le RSN s'applique aussi plus largement à tous les services intermédiaires fournis au sein de l'Union, incluant les services dits « de simple transport » (tels que les fournisseurs d'accès à internet) et ceux dits « de cache » (réseau de diffusion de contenu ou, en anglais, *content delivery network* (CDN)). Tous se voient tenus de coopérer avec les autorités pour traiter les demandes liées à des contenus illicites, et désigner un point de contact pour ces mêmes autorités ainsi que pour les utilisateurs dans l'Union. Leur politique de modération doit être clairement exposée dans leurs conditions générales et faire l'objet d'un rapport annuel public. Parmi eux, les services d'hébergement doivent en outre permettre aux utilisateurs de leur signaler facilement

tout contenu illicite et, en cas d'action de modération, ou de non-action à la suite d'un signalement, fournir à l'utilisateur concerné les motivations de leur décision. Il leur revient également d'informer les autorités s'ils ont connaissance d'une menace pour la sécurité ou la vie des personnes.

Les plateformes en ligne doivent déployer des moyens supplémentaires, en offrant des voies de recours internes aux utilisateurs contre leurs décisions de modération (ou de ne pas agir à la suite d'un signalement) ou en participant à des procédures de règlement extrajudiciaire des litiges. Les comptes des utilisateurs abusifs doivent être suspendus de façon proportionnée et transparente. Les interfaces des plateformes ne doivent pas viser à tromper les utilisateurs et doivent être transparentes en matière de publicité et de systèmes de recommandation. Enfin, les plateformes prennent des mesures pour protéger les mineurs qui les utilisent.

Lorsqu'elles ont une activité de place de marché (mise en relation de vendeur professionnel avec des consommateurs), les plateformes en ligne doivent également garantir la traçabilité des vendeurs professionnels et permettre l'information des consommateurs, notamment ceux qui auraient été amenés à acheter un produit illégal sur la plateforme.

Ainsi, le public est placé au centre de ce vaste dispositif de régulation et d'encadrement de l'activité des plateformes. Pour assurer l'efficacité de ce dernier, le RSN confie un rôle privilégié à la société civile : les entités désignées « signaleurs de confiance » par les États membres verront leurs signalements traités de façon prioritaire par les plateformes.

Dans la perspective de l'adaptation du RSN en droit français, l'Arcom pourrait se voir confier un rôle de régulateur et de coordinateur français des services numériques. Elle s'y prépare d'ores et déjà en collaboration avec les autorités publiques françaises et européennes, des fournisseurs de services, du monde académique et de la société civile.

Le PEReN

Créé en 2020, le Pôle d'Expertise de la Régulation Numérique (PEReN) est un centre d'expertise de pointe en matière de science des algorithmes et des données. Il accompagne l'ensemble des administrations publiques, services de l'État et autorités indépendantes, qui conçoivent, mettent en œuvre et évaluent la régulation des plateformes numériques. Il s'investit également dans des projets de recherche à caractère exploratoire ou scientifique.

Aujourd'hui, les plateformes en ligne occupent une place fondamentale dans notre vie (numérique) quotidienne. Notre usage des systèmes de recherche et de recommandation ou encore des réseaux sociaux en est l'illustration : outils omniprésents et devenus incontournables, ils reposent le plus souvent sur des technologies algorithmiques. Malheureusement, au-delà de connecter numériquement entre eux des milliards d'utilisateurs, les très grandes plateformes numériques peuvent également devenir des espaces virtuels pour la désinformation, les fausses croyances, les incitations à la violence et le harcèlement.

Les réseaux sociaux sont devenus le principal espace virtuel dans lequel les personnes expriment leurs opinions et dans lequel, trop souvent, elles peuvent également être agressées. Beaucoup de personnes se sentent libres d'insulter et d'attaquer d'autres utilisateurs dans le confort d'un relatif anonymat et souvent sans se soucier des conséquences d'agressions qui, si elles sont perpétrées dans un espace virtuel, peuvent cependant avoir des effets bien réels. Malgré le sentiment diffus que le cyberharcèlement et les attaques envers les minorités sont extrêmement présents dans les réseaux sociaux aujourd'hui, quantifier ces phénomènes reste une tâche difficile car les plateformes ne sont souvent pas aussi transparentes qu'elles peuvent l'annoncer : de telles analyses nécessitent en outre une connaissance technique très spécifique et une évaluation statistique des phénomènes.

C'est pourquoi il est nécessaire de relever les défis techniques inhérents à la régulation des plateformes en ligne, et ce conformément aux nouvelles modalités de cette régulation qui prévoit d'associer pouvoirs publics, institutions de recherche et société civile. Comprendre l'univers de la donnée et des algorithmes est un prérequis indispensable pour analyser le fonctionnement des plateformes numériques, et aider à la mise en place de leur régulation dans le cadre européen (DSA, DMA) et national. C'est une des missions essentielles du PEReN et c'est dans ce but qu'il s'associe et interagit avec ses partenaires nationaux et européens pour fournir aux régulateurs une expertise technique supplémentaire leur permettant d'exercer pleinement leurs compétences de régulation des plateformes numériques.

En collaboration avec le CNR et la DILCRAH, le PEReN réfléchit aux modalités d'une étude technique et quantitative sur la prévalence de discours haineux sur les réseaux sociaux, qui pourra s'appuyer sur les techniques à l'état de l'art en matière d'anonymisation, de traitement automatique du langage et d'apprentissage profond pour analyser les contenus publiés sur les réseaux sociaux, à une échelle statistique et sans prendre connaissance des contenus individuels, afin d'alimenter les travaux des acteurs compétents.

Féministes contre le cyberharcèlement

Créé en janvier 2016, Féministes contre le cyberharcèlement est un collectif féministe intersectionnel constitué en association loi de 1901 depuis 2017 et mobilisé contre les violences faites via les outils numériques aux femmes, aux filles et aux personnes LGBTQI+, notamment lorsqu'elles sont issues de groupes minorés. L'association a pour objectif de sensibiliser au phénomène des cyberviolences, d'orienter les victimes et de les informer sur les recours possibles.

Les violences en ligne sont un phénomène nouveau, en constante évolution sur lequel il n'existe que peu de données. Ce qui ne se mesure pas n'existe pas, c'est pourquoi il nous paraît essentiel de conduire des enquêtes permettant de quantifier les cyberviolences et de documenter le parcours des victimes afin de susciter une prise de conscience du caractère massif du phénomène et de ses ressorts spécifiques.

Les données que nous avons recueillies grâce aux enquêtes « Cyberviolence et cyberharcèlement : état des lieux d'un phénomène répandu » et « Cyberviolence et cyberharcèlement : le vécu des victimes », conduites à notre demande par IPSOS, dressent un état des lieux alarmant : 41 % des Français·es déclarent avoir subi des cyberviolences et 31 % admettent en avoir commis. Les violences en ligne sont répandues et ciblent en particulier les jeunes, les femmes et les personnes issues de groupes minorés. Elles ont de lourdes conséquences sur la vie et la santé des victimes — jusqu'à la tentative de suicide pour plus d'une victime sur 10, et restent pourtant largement minimisées et impunies.

La lutte contre ces violences repose en majorité sur les victimes, qui, faute de recours satisfaisants en matière de signalement et de procédure judiciaire, développent des stratégies d'autodéfense qui restreignent leur liberté d'expression. Par ailleurs, le niveau d'information du public demeure très faible : 69 % des victimes rapportent ne pas avoir su comment réagir à une cyberviolence et 81 % se déclarent mal informées sur les plateformes d'aide.

Au vu de cet état des lieux, notre association appelle les pouvoirs publics à mettre en place de grandes campagnes nationales d'information et de prévention, une plateforme d'écoute et d'orientation destinée à l'ensemble des victimes de cyberviolences — quel que soit leur âge, un observatoire des cyberviolences de genre permettant de systématiser le recueil de données et la publication d'analyses sur le sujet, ainsi qu'un plan national de formation à destination du personnel éducatif, social et de santé, du corps juridique et des forces de police, afin d'améliorer le parcours des victimes et leur accès au droit.

Génération Numérique

Bien que les parents soient généralement rassurés que leurs enfants soient à la maison, dans leur chambre, il est nécessaire de leur rappeler que les mondes numériques accessibles grâce aux outils (smartphone, tablette, ordinateur) qu'ils leur donnent ne sont pas plus sécurisés que la rue. Les enfants sont largement exposés à des contenus qui les choquent : qu'il s'agisse de contenus violents, haineux, porno… les internautes sont très largement susceptibles d'être confrontés à ce genre d'images, de vidéos ou de propos. Il est impératif que les adultes aient conscience de la réalité de ces mondes numériques afin qu'ils puissent contribuer à éduquer leurs enfants en toute connaissance de cause. Les campagnes médiatiques d'information sont malheureusement trop rares pour aider à cette prise de conscience. De plus, les angles sont souvent très anxiogènes (ce qui n'est pas le cas de la campagne Je Protège Mon Enfant).

Un des principaux soucis que nous relevons est que les mineurs participent peu au signalement de ces contenus car ils estiment que cela ne sert à rien : les mineurs signalent principalement sur les plateformes qui hébergent ces contenus problématiques. Or, les mineurs estiment qu'ils manquent d'information quant aux raisons des décisions qui sont prises par les plateformes. À notre avis, il serait très pédagogue que les plateformes explicitent leur gestion des signalements afin que les internautes apprennent, au fur et à mesure de leurs signalements, ce qui est autorisé ou interdit. C'est la meilleure manière d'apprendre à mieux contribuer à la modération des contenus en ligne.

Florence Hainaut, journaliste, réalisatrice du documentaire #SalePute

La première fois que j'ai été harcelée via Internet, c'était par un auditeur de Pure FM, une radio de la RTBF pour laquelle je travaillais. C'était en 2009, et le service juridique de la RTBF m'a dit qu'il ne pouvait rien faire parce que c'était mon Facebook personnel. Le collègue à qui mon harceleur écrivait pour dire des horreurs sur moi a refusé de le bloquer parce que — sic — « ça le faisait rire ». On m'a demandé pourquoi je lui avais répondu, en premier lieu. Puis pourquoi j'acceptais des auditeurs comme amis Facebook. Puis pourquoi je racontais tant de choses sur Facebook.

À l'époque je travaillais en petit matin à la radio. Cela veut dire que je sortais de chez moi à 3 heures du matin. Pendant plusieurs semaines, j'avais un couteau sur moi. Cette toute première expérience m'a appris quelque chose de fondamental ; face au harcèlement, j'étais seule.

Puis en 2015, me voilà catapultée à la présentation de l'émission politique du dimanche sur la RTBF. Alors que j'étais insultée de manière constante et que je m'en

insurgeais régulièrement sur les réseaux sociaux, je n'ai reçu — dans mon milieu professionnel — aucun soutien, ni public, ni même discret. Ma hiérarchie m'a demandé d'arrêter d'en parler sur Twitter, mes collègues directs ont fait semblant de rien, ou m'ont dit de ne pas répondre. C'est, ai-je beaucoup entendu, le revers de la médaille. Je trouve néanmoins étonnant que mes confrères n'aient pas à porter la même médaille.

J'ai quitté la RTBF en 2016 pour devenir freelance. J'ai travaillé pour une émission d'humour politique et les choses se sont aggravées. Puis je suis devenue très vocale sur les questions de genre et d'égalité et c'est devenu pire. Et puis j'ai écrit, dans le journal Le Soir une carte blanche sur le port du foulard par les étudiantes en supérieur et c'est devenu l'enfer. En 2021, avec Myriam Leroy, j'ai réalisé un documentaire sur la cyberviolence misogyne et comme prévu on l'a payé cher. Un blogueur a entrepris de débunker les chiffres du documentaire et de « prouver » que nous avions menti. Un président de parti a partagé son article.

De quoi aurais-je eu besoin ? D'une lecture adéquate du phénomène que constitue la cyberviolence. De chiffres qui prouvent que ce que je vis est réel. Alors peut-être que mon expérience aurait pu s'inscrire dans un schéma politique indéniable, et donc analysée pour ce qu'elle est vraiment.

Or il n'existe rien ou si peu. L'étude la plus importante à ce jour vient d'être menée par le collectif « Féministes contre le cyberharcèlement ». Une autre, « The chilling » met avant l'étendue du problème pour les femmes journalistes et les dangers que fait peser cette menace sur nos paroles de professionnelles.

Mais où sont les chiffres officiels ? Ils ne sont pourtant pas très difficiles à collecter. Mais quand ils le sont, il manque souvent une toute petite donnée : le genre des agresseurs. Qui harcèle qui ? Et donc, pourquoi ?

Dans une résolution datant du 17 avril 2018, le Parlement européen souligne l'importance de recenser les problèmes que pose internet lorsqu'il est utilisé pour commettre des délits, proférer des menaces ou perpétrer des actes de harcèlement ou de violence à l'encontre des femmes ; et invite instamment les décideurs politiques à apporter une réponse appropriée à ces questions. Et depuis, que s'est-il passé ?

Internet est un lieu où les femmes — qui sont encore aujourd'hui peu mises en avant dans les médias traditionnels — peuvent prendre la parole, s'organiser, faire connaître leur travail, s'épancher, parler. Découvrir ensemble que leurs expériences douloureuses ou humiliantes sont universelles. Se mobiliser.

Aucun #metoo, aucun réveil tardif sur la question des violences et du harcèlement n'aurait été possible sans cette formidable caisse de résonance que constituent les réseaux sociaux. Et c'est bien parce qu'ils sont un formidable lieu de galvanisation qu'ils sont également un formidable terrain de chasse.

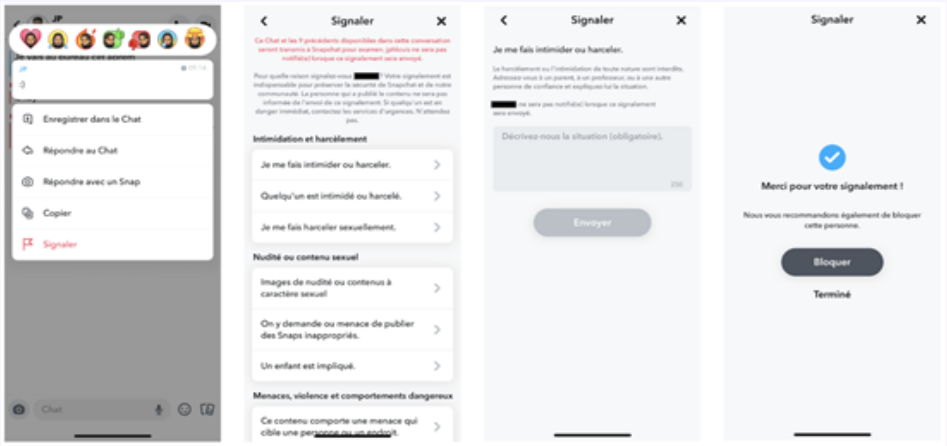
Snapchat

La lutte contre les cyberviolences repose sur un engagement quotidien, qui nous oblige tous, plateformes, associations, administrations et internautes, à agir sans délai. Nous saluons ainsi les travaux menés dans le cadre du Conseil National de la Refondation du Numérique pour penser ensemble à un espace numérique plus sûr.

Snapchat a pour objectif de reproduire les interactions quotidiennes que nous pouvons avoir entre amis proches et familles. Les plateformes ne devant pas se résoudre en une compétition entre utilisateurs, la conception de Snapchat assure un rempart structurel contre tout risque de viralité.

Ces engagements se retrouvent dans la partie privée de l'application, où toute relation doit être réciproque, et tout enregistrement d'écran est immédiatement notifié. Les groupes, restreints en nombre, ne peuvent être visibles que par leurs membres. Les amitiés pouvant évoluer, l'outil *Friend Check Up* invite l'utilisateur à s'assurer que sa liste d'amis est composée de personnes connues et avec lesquelles il souhaite rester connecté.

La lutte contre le cyberharcèlement est cruciale pour protéger la santé mentale et physique des victimes. Nous prenons des mesures immédiates contre les comportements abusifs, pouvant aller jusqu'au bannissement des auteurs. Aussi, nous accordons une grande importance au signalement et invitons tout Snapchatter, victime ou témoin de comportements préjudiciables, à le notifier. Notre dispositif, facilement accessible sur l'ensemble de notre plateforme, présente dans un jargon clair les différents motifs de signalement et invite l'utilisateur à fournir des éléments contextuels afin de guider nos modérateurs. Conscient des potentielles pressions sociales, nous leur rappelons que celui-ci est confidentiel, et en cas de danger imminent, la nécessité de contacter au plus vite les forces de l'ordre et/ou une personne de confiance. Ces signalements peuvent être réalisés par nos partenaires associatifs, dans le cadre de notre programme *signaleurs de confiance*, et pour lesquels nous traitons leurs notifications en priorité.



En parallèle, nous mettons en place des outils de prévention afin de promouvoir un environnement sain et respectueux. Notre portail Here For You, généré par des mots clés liés à la santé mentale, propose ainsi des contenus de sensibilisation renvoyant vers nos partenaires de confiance, comme E-Enfance. Des campagnes en fil rouge rappellent également les ressources existantes, comme le 3018 ou le 3114. Pensé et travaillé avec nos experts, notre Centre Parental permet par ailleurs à tout parent d'avoir des conversations constructives et ouvertes avec son adolescent, tout en protégeant leur autonomie et vie privée. Celui-ci est accompagné de notre Guide parental, qui accompagne les parents sur Snapchat.

Compte tenu de l'évolution des pratiques, et de l'apparition de nouveaux phénomènes, nous repensons quotidiennement notre engagement afin de nous adapter aux nouvelles pratiques et aux évolutions technologiques, pour apporter plus de sécurité sur notre plateforme.

Meta

Si les réseaux sociaux offrent de multiples opportunités aux utilisateurs comme l'accès à l'information ou la mobilisation autour de causes qui leur sont chères, ils peuvent également y être confrontés à la publication de contenus offensants.

La sécurité des utilisateurs constitue une priorité absolue pour Meta. Notre politique en matière d'intimidation et de harcèlement interdit ce type de contenus, que nous supprimons dès que nous en avons connaissance et nous désactivons les comptes récidivistes.

Notre action repose sur trois piliers :

- Nos standards de la communauté définissent ce qui peut être publié ou non sur nos plateformes. Accessibles à tous les internautes, ils font l'objet d'un rapport de transparence trimestriel, dans lequel nous indiquons notamment le nombre de contenus traités avant ou après signalement, et le taux de prévalence.
- Nos investissements sont sans précédent en matière de sécurité et de sûreté, à hauteur de 16 milliards de dollars en cinq ans. 40 000 personnes sont dédiées à cette mission dans le monde. Parmi elles, les modérateurs analysent les contenus nécessitant la compréhension de contextes spécifiques. Parce que la modération à grande échelle ne peut reposer uniquement sur l'action humaine, nous avons développé des modèles d'intelligence artificielle de pointe, capables d'identifier une vaste majorité de contenus en infraction. Nous avons open-sourcé une partie de ces technologies à travers l'outil HMA pour permettre à d'autres plateformes d'en bénéficier.
- Enfin, nous avons développé des outils pour permettre aux utilisateurs de mieux contrôler leur expérience en ligne. Cela comprend le filtrage des commentaires et des messages privés injurieux sur la base de « Mots masqués », ou encore la restriction de contacts non sollicités. Les outils de signalement permettent d'améliorer nos systèmes automatisés et de remonter les contenus qui leur échappent. C'est pourquoi nous proposons de nombreuses catégories de signalement, accessibles depuis n'importe quel contenu.

Nous savons que l'impact émotionnel de l'intimidation et du harcèlement peut être plus important sur les mineurs. Ainsi, les comptes des 13-18 ans sont privés par défaut à l'inscription, et ils ne peuvent être contactés sur Instagram par des adultes qu'ils ne suivent pas.

Par ailleurs, Meta travaille étroitement avec des experts français et internationaux, psychologues, créateurs, associations, et forces de l'ordre, afin de :

- traiter en priorité les signalements que ces tiers de confiance nous remontent ;
- améliorer les outils existants pour permettre à chacun d'avoir le contrôle de son expérience ;
- mettre en place des campagnes pour rappeler que ces outils existent mais aussi promouvoir les comportements responsables en ligne ;
- contribuer aux efforts partagés de l'industrie et proposer des solutions globales à travers par exemple le programme StopNCII pour empêcher le partage d'images intimes volées.

Meta est convaincu que ça n'est qu'ensemble que ce défi pourra être relevé, dans une dynamique de responsabilité partagée entre les acteurs publics, les forces de police et de justice, les entreprises, les associations et experts, et les utilisateurs.

Google

Google est honoré d'avoir été associé aux différents travaux et groupes de travail du Conseil National de la Refondation (CNR) Numérique et de pouvoir soumettre la présente contribution sur le harcèlement dans l'espace numérique. La mission de Google est de permettre à chacun de pouvoir accéder à une information de qualité dans un monde numérique responsable, où la bonne modération des contenus illicites et dangereux est partie intégrante. Il s'agit là d'un élément essentiel de notre devoir envers nos utilisateurs et partenaires, et nous sommes pleinement engagés à contribuer à rendre l'espace numérique plus responsable.

Nous investissons constamment dans des équipes ou des outils techniques et technologiques permettant de lutter contre toute forme de contenus illicites sur nos produits. Nous incluons ces informations dans notre rapport de transparence accessible en ligne, dédié aux questions de retraits des contenus et sécurité en ligne

Nous avons mis en place des mécanismes de signalement simplifiés permettant à tout utilisateur de porter à notre connaissance tout contenu qui serait contraire aux règles de droit français ou même aux conditions d'utilisation du produit concerné. À titre d'exemple, au cours du dernier trimestre 2022, YouTube a retiré pour la France plus de 43 000 vidéos, et environ 6 % l'ont été pour cause de harcèlement ou cyberintimidation… Google et YouTube font de la lutte contre le cyberharcèlement une priorité. Au-delà de règles et d'outils dédiés, notamment liés à la modération des commentaires sur nos plateformes, nous travaillons avec les acteurs institutionnels et associatifs pour sensibiliser le plus grand nombre à ces sujets — en voici quelques exemples :

Nous soutenons depuis plusieurs années la campagne « Non au harcèlement » du ministère de l'Éducation nationale. L'année dernière, le spot campagne a aussi fait l'objet d'une amplification sur YouTube, à travers un *masthead* dédié (bannière vidéo s'affichant directement sur la page d'accueil de YouTube). À travers cette amplification, la vidéo a récolté 223 000 vues. Nous avons par ailleurs rappelé sous la vidéo les numéros 3018 et 3020. Nous soutenons l'association e-Enfance/3018 depuis plusieurs années, à travers Google.org, la branche philanthropique de Google (nous avons notamment soutenu le lancement du programme Les Super Héros du Net). Le 3018 est par ailleurs *trusted flagger* sur YouTube, et nous avons un canal de communication ouvert en permanence pour les écoutants du 3018 qui peuvent solliciter notre aide pour les situations qu'ils n'arrivent pas à résoudre directement avec nos formulaires en ligne. Enfin, l'association bénéficie aussi de crédits publicitaires sur le moteur de recherche pour mettre en avant le 3018 dans les résultats de recherche.

Nous déployons, avec nos partenaires, des campagnes de communication dédiées à la sécurité en ligne. Ainsi, durant le mois d'avril, nous avons édité un supplément magazine, distribué à plus de 900 000 exemplaires en complément de magazines (M Le Mag, Le Figaro Magazine, L'Obs, Elle, Psychologies magazines, etc.). En page 10 de ce guide, Justine Atlan, directrice générale d'e-Enfance/3018, répond à une interview sur le thème « Comment lutter contre le cyberharcèlement ».

Nous avons également soutenu la série *Résotuto*, proposée par Lumni, 20 tutos destinés aux ados et visant à les interroger sur leurs usages d'Internet des réseaux sociaux (ces tutos abordent notamment le sujet du cyberharcèlement). Tous les détails sur la série sont disponibles sur ce lien.

Enfin, au-delà de ces initiatives, Google est également membre de l'association Point de Contact dont l'objet est d'analyser et de relayer les signalements effectués par les internautes. Point de Contact comme d'autres associations luttant contre les violences en ligne (LICRA, CRIF, Stop homophobie) sont membres du programme Trusted Flaggers de YouTube permettant notamment un traitement prioritaire de leurs signalements.

II. PROTÉGER

Mieux orienter les utilisateurs vers les dispositifs adaptés

Il est fréquent qu'une personne ayant fait l'objet d'une agression en ligne ou qui en est témoin se trouve démunie, soit parce qu'elle ne connaît pas les comportements à adopter, les liens à suivre, les autorités ou associations à contacter, soit parce que les actions entreprises ont été dépourvues d'effet. Pour prendre les décisions permettant d'accompagner au mieux les victimes, proches et témoins, nous devons approfondir notre connaissance de leur parcours utilisateur (mesure 4). Pour prévenir, former et orienter, des campagnes massives d'information seront déployées (mesure 5).

Le vécu des victimes face aux procédures

Partir du vécu des victimes et des témoins est primordial dans la lutte contre la haine et les violences en ligne. Lorsque l'utilisateur fait face à un contenu ou un comportement illicite, une multitude de démarches s'ouvrent à lui sans que chacune puisse nécessairement répondre à la diversité de ses attentes : besoin de retrait ou de blocage de contenu immédiat, soutien psychologique, accompagnement juridique. Les frustrations qui en découlent doivent être comprises et accueillies. Il existe ainsi une responsabilité et un intérêt collectifs à ce que l'utilisateur soit guidé au mieux dans ses démarches pour qu'il puisse s'adresser au bon interlocuteur et sache quoi en attendre.

Retour sur l'atelier organisé le 22 mars 2023 sur les violences en ligne faites aux femmes

Dans le cadre du Conseil national de la refondation, un atelier dédié à la question de la haine subie par les femmes en ligne a été organisé le mercredi 22 mars par le Conseil national du numérique et la Délégation Interministérielle à la Lutte contre le Racisme, l'Antisémitisme et la Haine anti-LGBT+, à l'initiative de Mme la députée Véronique Riotton, présidente de la délégation aux droits des femmes et à l'égalité des chances entre les hommes et les femmes de l'Assemblée nationale. Cet événement a été placé sous le patronage et introduit par M. Jean-Noël Barrot, a accueilli la participation de Mme Isabelle Lonvis-Rome, ministre déléguée auprès de la Première ministre, chargée de l'Égalité entre les femmes et les hommes, de la Diversité et de l'Égalité des chances, de Mme Marlène Schiappa, Secrétaire d'État auprès de la Première ministre, chargée de l'Économie sociale et solidaire et de la Vie associative, ainsi que des députés Prisca Thevenot et Paul Midy. Il a permis de donner la parole aux femmes médiatisées victimes de violences en ligne, de laisser libre court à un dialogue multipartite entre autorités, plateformes, femmes d'influence, associations et entreprises ainsi que de faire émerger des pistes d'action pour collectivement améliorer la lutte contre ce phénomène.

La haine à l'encontre des femmes médiatisées, un phénomène d'ampleur toujours banalisé

L'échange conduit lors de l'atelier a mis en lumière, par la force des témoignages, l'ampleur et la diversité des formes de harcèlement que subissent les femmes sur leurs réseaux sociaux. À ce titre, une enquête conduite par l'association Féministes contre le cyberharcèlement avec Ipsos et publiée en novembre 2022 fait apparaître que « parmi les répondant·es de l'enquête auprès des victimes on retrouve en majorité des femmes (84 % des répondant·es) ainsi que des personnes discriminées en raison de leur identité de genre et leur orientation sexuelle (43 %). »

Par ailleurs, ces violences prennent souvent des formes multiples (surveillance illégale, messages haineux, injures, diffamation, usurpation d'identité, révélation

d'informations personnelles mettant en danger les victimes, diffusion non consentie de photos et de vidéos intimes, etc.) et évoluent rapidement au gré des progrès techniques et de l'émergence de nouvelles fonctionnalités sur les plateformes. Cela suppose une adaptation constante des victimes pour signaler ces violences, des plateformes et des autorités afin de qualifier et de sanctionner ces nouvelles formes de haine, ainsi que des associations pour accompagner au mieux les victimes. L'ampleur du harcèlement et la viralité des contenus haineux sur les plateformes exposent les femmes médiatisées à de véritables « raids numériques ». La multitude des agresseurs est bien souvent difficile à appréhender par les autorités et expose les femmes médiatisées à des violences continues sur le long terme.

Ces violences ont des conséquences visibles et concrètes sur la santé psychique et physique des femmes qui les subissent, ainsi que sur leurs relations interpersonnelles. 88 % des victimes de violences en ligne souffrent ou ont souffert de troubles anxieux et dépressifs : crises de panique, insomnies, baisse d'estime de soi, etc. De nombreuses victimes ont déjà eu des pensées suicidaires ou ont tenté de mettre fin à leurs jours. En outre, les violences génèrent un sentiment d'insécurité, d'autant plus lorsque les victimes sont également harcelées dans l'espace tangible. Les violences subies par les femmes médiatisées expriment des phénomènes bien plus systémiques que circonscrits aux réseaux : les messages de haine relayés sur les réseaux constituent une caisse de résonance des agressions et discriminations qui s'expriment également en dehors des réseaux. Ce qui implique de penser les politiques publiques de lutte contre la haine de manière globale.

En dépit d'une sensibilité de l'opinion publique aux violences sexistes et sexuelles depuis #MeToo, les violences en ligne affectant les femmes continuent d'être banalisées, voire niées. Les femmes entendues ont partagé le sentiment d'être culpabilisées pour les violences vécues : le « tu n'aurais pas dû sortir ainsi » s'exprime également en ligne. Ce qui consiste une forme d'acceptation de ces violences et un renversement de la charge de culpabilité. Par ailleurs, la haine en ligne s'exprime également dans les messageries privées. Ce phénomène confronte les victimes à une haine décomplexée, dans une sphère où elles se retrouvent isolées, et ce jusque dans leurs outils de travail (boîtes mail ou messageries privées).

La persistance des violences sexistes et sexuelles en ligne interroge enfin la perception par la population de la place des femmes dans l'espace public. Ces violences, qui s'expriment de manière systémique, ont pour effet de stigmatiser, de rendre illégitime et de mettre sous silence la parole des femmes médiatisées, ainsi renvoyées à la sphère privée. Elles empêchent la participation de toutes et tous à l'espace public et *in fine*, la construction de la société égalitaire.

Les échanges ayant eu lieu dans le cadre du CNR ont fait apparaître une double difficulté du point de vue de l'utilisateur : une certaine inconnue quand ce n'est pas un doute exprimé par les participants sur l'utilité et les modalités du signalement ou du dépôt de plainte et le manque de lisibilité des outils disponibles.

À tel point qu'il existe un désintéressement pour ces voies de recours et que des stratégies de contournement en viennent à devoir être mises en place. Des femmes ayant subi de violences sexistes et sexuelles en ligne témoignent en ce sens des stratégies mises en place : clôturer l'accès à sa messagerie privée, engager un modérateur professionnel, bloquer et limiter la visibilité des contenus problématiques, s'autocensurer en évitant de parler des « sujets qui fâchent ». Autant de stratégies qui constituent une charge mentale et souvent une bride injustifiée à la liberté d'expression.

Enfin, le manque de signalement des contenus préjudiciables par les utilisateurs tient aussi aux difficultés rencontrées par les utilisateurs. Les dispositifs et les critères de signalement varient d'une plateforme à l'autre. Les catégories des dispositifs de signalement ne sont pas toujours les mêmes. Ils peuvent ne pas être intuitifs ou accessibles à l'ensemble des publics. Le signalement exige de devoir interagir avec les commentaires problématiques. Il n'est souvent pas possible de signaler une multitude de commentaires à la fois. Et surtout l'incertitude décourage : « que devient notre signalement une fois qu'il est envoyé ? ».

Dès lors, l'outil de signalement fait encore pour beaucoup l'objet de mésusages : relativement aux signalements portant sur des contenus qui méritent d'être signalés, le signalement reste très souvent utilisé pour exprimer un désaccord ou pour nuire à une personne donnée, afin de réduire sa visibilité sur le réseau. Parfois les associations sont touchées par ce type de comportement abusif provenant de personnes malveillantes. Ce qui peut laisser certaines associations penser que les algorithmes de classement donneraient une visibilité moindre à leurs publications qu'à celles des personnes dont elles entendent dénoncer les comportements.

Assurer une plus grande transparence sur les procédés algorithmiques conduisant à diminuer la visibilité de certaines publications (par exemple les publications ayant été signalées, comme le font certains réseaux sociaux) semble nécessaire à deux égards : tout d'abord pour rendre compte de la réalité des conséquences réelles données au signalement, hormis la suppression du contenu ; ensuite pour en préserver certains acteurs devant être protégés, comme les associations œuvrant à l'intérêt général.

En parallèle du signalement sur les réseaux sociaux ou plateformes dédiées, des progrès ont été faits pour améliorer la prise en charge des victimes de violences en ligne ou encore le dépôt et le traitement de leur plainte. Mais ces progrès se heurtent aux contraintes structurelles des missions régaliennes, à commencer par le manque de personnel (voir Pour aller plus loin), et ce pour endiguer tout sentiment d'impunité.

Approfondir notre connaissance du parcours utilisateur

Pour répondre aux besoins des utilisateurs, il convient d'abord d'identifier les attentes, incompréhensions et usages de chacun et chacune, probablement selon le type d'utilisateur concerné et le type de situations auxquelles elle risque de faire face. Ce qui implique de mener des études comme celles mentionnées précédemment, mais également de comprendre par des études de terrain indépendantes le parcours des personnes confrontées à des situations de violence.

Si l'on prend le cas d'un utilisateur exposé à un contenu offensant ou qu'il juge illicite, il est possible que la personne ne trouve pas le moyen de signaler de manière efficace. Les utilisateurs n'ont pas tous le même degré de connaissance des outils disponibles, en quoi ils consistent, comment la confidentialité est assurée, etc. La personne concernée n'a pas toujours connaissance des relais dont elle peut bénéficier dans le monde associatif ou encore auprès des autorités publiques. Ces situations sont d'autant plus difficiles à appréhender lorsque les utilisateurs sont victimes de raids numériques, impliquant des milliers d'agressions en ligne, ce qui complexifie les démarches pour les victimes. De nombreuses initiatives pour faire connaître les moyens disponibles existent mais pas nécessairement sur tous les sujets et pas nécessairement partout.

Rien par exemple n'indique à une personne le parcours qu'elle peut suivre pour se faire aider en dehors de la plateforme. Une piste serait d'étudier la question d'un renvoi des utilisateurs vers d'autres acteurs (par ex. Cybermalveillance.gouv.fr, Masecurite.fr, soutien psychologique, autorités pour dépôt de plainte, signaleurs de confiance) après leur signalement d'un contenu sur une plateforme. Sachant que si cette idée est louable, des acteurs ont partagé la crainte que ce renvoi soit à l'origine d'une confusion des genres dans le parcours de l'utilisateur, ce qui est également à prendre en compte.

En attendant, lorsque l'utilisateur cherche un remède hors des réseaux sociaux, il est possible de supposer que le chemin le plus direct pour l'utilisateur est de faire une recherche sur un moteur de recherche. Mais il apparaît alors que des sites comme Cybermalveillance.gouv.fr arrivent en fin de page de résultats lorsque l'on pose une question générique telle que « que faire en cas d'agression sur les réseaux sociaux ? ». L'utilisateur aura peut-être tendance à aller sur le premier site public, souvent le site Service-public.fr dont les pages très riches orientent vers certaines procédures en lien avec le cyberharcèlement, bien que les dispositifs évoqués couvrent d'autres types de comportements illicites et sans renvoyer non plus aux dispositifs associatifs. En réponse à la recherche « on m'a injuriée en ligne », la personne sera là aussi orientée également vers le site service-public.fr où Pharos est accessible en quelques clics.

Ces quelques exemples très partiels n'emportent aucune qualité méthodologique, mais témoignent au contraire de la nécessité qu'il y a d'appliquer une méthodologie

sérieuse sur l'analyse du parcours utilisateur afin de définir les remèdes les plus appropriés. Peut-être qu'une action à entreprendre est de favoriser l'apparition de l'outil de diagnostic très performant du site Cybermalveillance.gouv.fr.

Comment alors coller au mieux au parcours de l'utilisateur pour améliorer sa connaissance des outils existants et l'aiguiller vers les dispositifs de soutien, de signalement ou de plainte en quelques clics seulement ? L'expertise pour ce faire réside chez les plateformes, des sociétés spécialisées mais aussi au sein de l'État, tant au sein de la Direction interministérielle de la transformation publique (DITP) que de la Direction interministérielle du numérique (DINUM). Ces directions comportent des experts qui s'intéressent au comportement de l'utilisateur et à la manière dont il doit être intégré dans la réflexion et la conduite de politiques publiques plus efficaces.

En juin 2022, en partenariat avec la DITP et la DINUM, la DILCRAH a initié une démarche collaborative de promotion du civisme en ligne dans l'univers du jeu vidéo et de l'e-sport. Ce travail de co-construction a réuni pendant plusieurs mois, des acteurs publics et privés, issus de l'écosystème du jeu vidéo, de l'e-sport, du numérique, de la lutte contre la haine en ligne, de la recherche ainsi que des joueuses, des joueurs, des étudiantes et des étudiants. L'objectif était de co-créer des outils pour lutter contre la toxicité en ligne et préserver l'expérience de jeu. Dans un premier temps, un travail de diagnostic[26] a été effectué par l'équipe de sciences comportementales de la DITP, avec les trois objectifs suivants :

- identifier les déterminants du comportement toxique dans les jeux vidéo ;
- recommander des leviers pour lutter contre les comportements toxiques ;
- établir des principes et des conseils pratiques pour la création et la diffusion d'un code de modération commun.

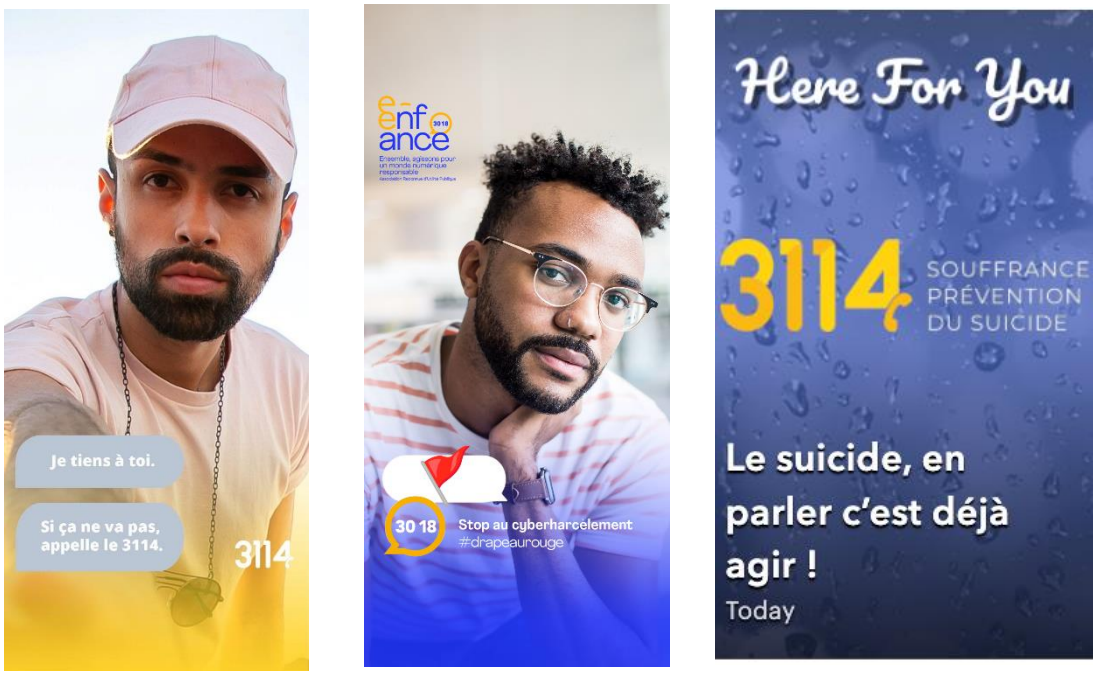
Dans un second temps, les participantes et participants se sont mobilisés sur une série d'ateliers pour proposer des solutions justes, et notamment des campagnes en ligne autour d'un code de modération des joueurs (dont un tutoriel). Cette action innovante est pérennisée dans le cadre du plan 2023-2026 de lutte contre le racisme, l'antisémitisme et les discriminations liées à l'origine[27].

Mesure 4 – *Une étude indépendante sera conduite sur le parcours des victimes et témoins de contenus enfreignant les règles applicables.*

[26] DITP, Rapport de diagnostic : civisme et jeux vidéo, publié le 13 octobre 2022
[27] DILCRAH, Plan national de lutte contre le racisme, l'antisémitisme et les discriminations liées aux origines 2023-2026, janvier 2023

Massifier les campagnes publiques d'information

Que ce soit en collaboration avec d'autres acteurs, privés ou publics, ou de manière autonome, les réseaux sociaux créent des campagnes de sensibilisation. La plupart ont également créé des espaces et documents dédiés à l'apprentissage aux bons usages, souvent en mobilisant des associations pour leur rédaction. Mais il apparaît nécessaire d'aller au-delà.



Source : Extraits de campagnes de sensibilisation diffusées par le réseau social Snapchat

En novembre 2021, dans le cadre de la Journée nationale de lutte contre le harcèlement scolaire, l'association e-Enfance/3018 a mené deux campagnes de sensibilisation simultanées sur Snapchat et TikTok. L'objectif : rappeler les règles de sécurité et de bienveillance en ligne[28]. Sur TikTok, une page était entièrement dédiée à la campagne, avec une mise en avant sur l'onglet « Découverte » pour renforcer sa visibilité. Elle hébergeait un quiz, des liens, des conseils, une vidéo de témoignages ainsi qu'un clip de sensibilisation réalisé par le ministère de l'Éducation nationale[29].

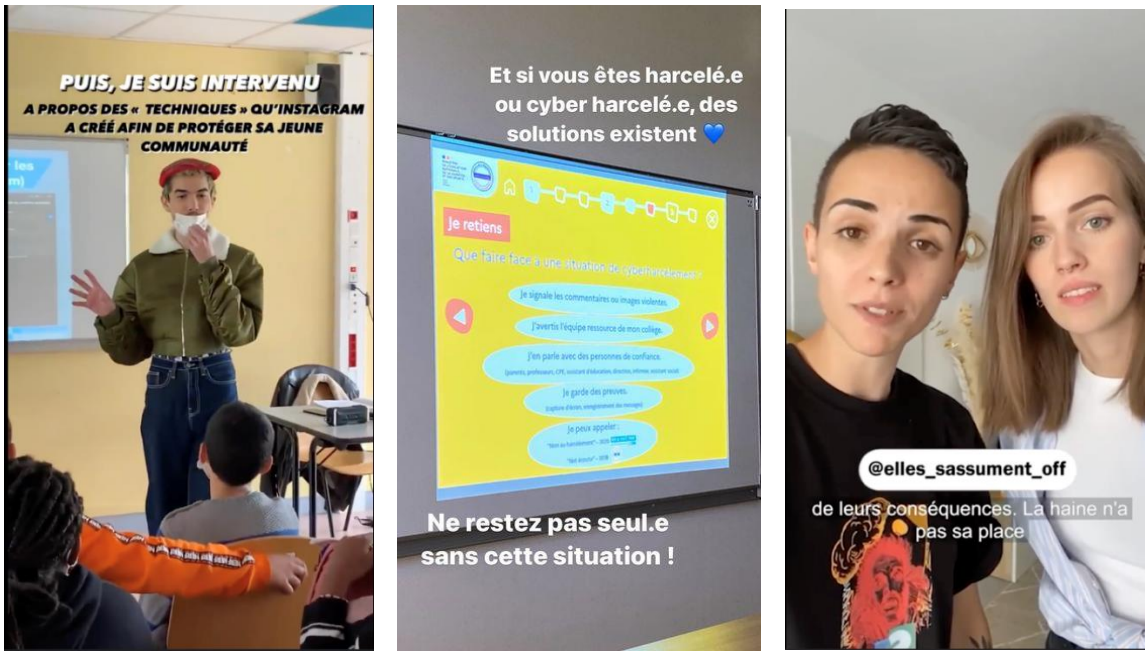
En 2022, l'association e-Enfance/3018 a développé d'autres campagnes dont, en août, une campagne d'affichage nationale visant à faire télécharger par les jeunes l'application 3018 pour briser leur solitude face au cyberharcèlement. Celle-ci a pris

[28] Cyberharcèlement : l'association e-Enfance / 3018 lance une campagne de sensibilisation sur TikTok et Snapchat, Le Figaro, 18 novembre 2021

[29] Ministère de l'éducation, Campagne de sensibilisation Non au harcèlement 2021-2022, Youtube, vidéo publiée le 19 novembre 2021.

place dans les gares SNCF et s'est prolongée en septembre dans les centres commerciaux. Elle a été diffusée également sur les réseaux sociaux jeunes.

Parmi les campagnes portées par le groupe Meta[30], la campagne #LePoidsdesMots, opérée par Génération Numérique, a été réalisée avec 12 créateurs de contenu sur Instagram pour sensibiliser les audiences des créateurs aux dangers du harcèlement en ligne. La campagne sur les réseaux sociaux s'est ensuite traduite dans la rue, où environ une centaine de milliers de jeunes ont pu être formés.



Source : Extraits de contenus réalisés par des créateurs de contenu dans le cadre de la campagne #LePoidsdesMots, lancée par Génération Numérique avec le soutien d'Instagram

Parmi les actions de sensibilisation réalisées hors ligne, Google a édité un supplément magazine portant sur les bonnes pratiques de parentalité numérique, distribué à plus de 900 000 exemplaires en complément de magazines (M Le Mag, Le Figaro Magazine, L'Obs, Elle, Psychologies magazine, etc.).

En parallèle, de grandes campagnes de sensibilisation nationale ont été portées par les autorités publiques sur la question du cyberharcèlement en lien avec la protection de la jeunesse. Ce fut le cas encore récemment avec la campagne Je Protège Mon Enfant dont la vocation est de sensibiliser le plus grand nombre aux bonnes pratiques

[30] Pour des illustrations de campagnes passées, voir par exemple celles conduites avec ou au bénéfice de e-Enfance / 3018, RespectZone, Elues locales, la Licra. La période des élections françaises de 2022 a également fait l'objet de campagnes de sensibilisation des utilisateurs pour lutter contre la diffusion de fausses informations. Voir par exemple Meta, « Elections françaises 2022 : une série d'initiatives dédiées sur Facebook, Instagram et WhatsApp pour aider les citoyens à lire et à décrypter l'information en ligne », 16 février 2022.

de la parentalité numérique[31]. La campagne portée par Cybermalveillance.gouv.fr contre le cyberharcèlement[32] et réalisée en coopération avec l'Institut National de la Consommation consistait quant à elle en un spot télévisé visant à sensibiliser aux dangers du cyberharcèlement chez les jeunes et à partager les bonnes pratiques face au cyberharcèlement.

Nous avons désormais besoin d'une coordination entre ces initiatives (cf. partie III) ainsi que de campagnes d'informations massives et générales sur les comportements à adopter en ligne, à la fois pour ne pas être auteurs de méfaits, être informés des bonnes pratiques. Il s'agit d'œuvrer comme dans certains environnements à risque ou au sujet de nombreux biens de consommation : des messages d'avertissement sont ainsi dispensés sur produits alimentaires, les autoroutes, les plages publicitaires télévisuelles. Dans cette perspective, différentes voies complémentaires sont à emprunter.

Des campagnes publiques seront portées de manière récurrente par les autorités compétentes en coopération avec le Service d'information du Gouvernement. Ce dispositif aura pour avantage d'informer l'entièreté de la population, de marquer le caractère prioritaire des messages portés, et potentiellement d'engager la conversation entre les auditeurs ou téléspectateurs d'un même message. À la manière des nombreuses campagnes annuelles visant à sensibiliser à la sécurité routière (« Sam ! Celui qui conduit ne boit pas ») ou des campagnes dédiées au jeu en ligne, ce dispositif aura vocation de porter les connaissances nécessaires auprès du plus grand nombre et à partager des bonnes pratiques sur Internet.

Cette démarche pourra être nourrie par une communication clarifiant le rôle de chacune des entités listées de manière non exhaustive dans la partie *Que faire face à une situation illicite ?* du présent document (pp. 10 à 13).

En lien étroit et dans la poursuite des efforts qu'elles ont engagés, les plateformes pourront être mobilisées, par la voie législative au besoin, afin d'assurer le financement et la diffusion de messages définis en lien avec les associations et les autorités. Cela aura pour avantage de fournir aux utilisateurs une information dédiée, adaptée aux réseaux sociaux notamment, mais surtout de les informer directement dans l'environnement concerné, à savoir le réseau social. Les plateformes partagent déjà des informations concernant leurs politiques de modération et de sensibilisation au signalement, mais le plus souvent dans leurs rubriques « Aide »[33].

---

[31] Campagne nationale de sensibilisation à la parentalité numérique pour un usage raisonné des écrans par les enfants, février 2023.

[32] Cybermalveillance.gouv.fr, "Cyberharcèlement chez les jeunes : comment réagir ?", YouTube, vidéo publiée le 24 octobre 2022.

[33] A titre d'exemple, Google met à disposition, à l'instar d'autres plateformes, des informations portant sur leur politique de signalement et de modération dans leur rubrique « Aide ».

Il serait intéressant de privilégier une intégration permanente de l'information dans le flux de la plateforme. L'objectif est de fournir une information permanente, simple et accessible, là où il faut et quand il faut. En effet, nous ne sommes pas tous égaux face à une situation ou dans un environnement donné et la capacité qu'offrent les supports numériques d'adapter les informations fournies à différents publics est intéressante.

Pendant la crise du Covid-19, les plateformes se sont mobilisées pour dispenser une information pertinente sur le traitement de l'information en nous invitant à tel ou tel comportement[34]. Il serait intéressant de prolonger l'expérience ou du moins la réflexion autour des phénomènes de haine en ligne par exemple. Des dispositifs d'informations préventifs pourraient être déployés lorsque certains mots ou types de contenus sont détectés automatiquement (« Es-tu sûr de vouloir publier ceci ? », « Lis avant de repartager », « Ce message semble enfreindre telle règle. Le cas échéant, il est passible de telle sanction »).

Ces mesures permanentes permettraient de faire la lumière sur les fonctionnalités offertes par les plateformes. Des tutoriels simples, rapides et accessibles (en langue française et facilement identifiables) sur ce qui est à signaler, pourquoi signaler, comment signaler pourraient être régulièrement promus sur la plateforme, comme par exemple le renvoi depuis les pages de signalement des réseaux sociaux vers les pages dédiées de Cybermalveillance.gouv.fr. Enfin, un questionnaire récurrent et évolutif pourrait avoir à être rempli à échéances régulières sur les principales plateformes et réseaux sociaux pour nous assurer d'un bon niveau de compréhension des comportements à adopter ou non.

Ces dispositifs, s'ils ne résultent pas de l'action autonome des plateformes, pourraient faire l'objet de mesures législatives ou réglementaires visant à une information éclairée des utilisateurs. À ce titre, il est à observer que de nombreuses pratiques à risques font déjà l'objet d'informations légales aux consommateurs et utilisateurs, des gâteaux apéritifs à l'alcool en passant par la circulation routière et les jeux d'argent. La dernière campagne de l'Autorité nationale des jeux, « T'as vu, t'as perdu »[35] vise à sensibiliser les joueurs aux risques des jeux d'argent en ligne.

Mesure 5 – *Des campagnes publiques d'information au public seront déclinées sur les réseaux sociaux et les médias traditionnels.*

[34] Par exemple de lire les documents partagés.

[35] Autorité nationale des jeux, « L'Autorité nationale des jeux lance une campagne de prévention intitulée « T'as vu, t'as perdu » », 14 novembre 2022

La parole aux acteurs

Cybermalveillance.gouv.fr

Cyberharcèlement, usurpation d'identité, escroquerie sentimentale, hameçonnage, piratages, etc. Perceval, Pharos, Thésée, etc. Les menaces sont multiples, les solutions parfois difficiles à identifier. C'est pour cette raison que l'État a créé en 2017 la plateforme Cybermalveillance.gouv.fr, voulue comme le guichet unique de lutte contre les cybermenaces, et ce pour les particuliers, les collectivités et les entreprises (hors OIV et OSE).

Depuis sa création, Cybermalveillance.gouv.fr accompagne les victimes en permettant, à toute victime que ne saurait définir ce qu'elle subit, de réaliser un « parcours d'assistance ». En quelques questions, l'incident est qualifié, avec une définition précise ainsi que la conduite à tenir lorsque l'on est victime. Par exemple sur le cyberharcèlement, nous expliquons, entre autres, qu'il est nécessaire d'en parler à un tiers de confiance, de conserver les preuves, de signaler les contenus illicites auprès des plateformes de réseaux sociaux (avec les liens de signalement pour les plus répandues), de déposer plainte, et de contacter les services du 3018 ou du 3020. Le service permet également, pour les menaces qui le nécessiteraient, une mise en relation avec des prestataires de proximité en capacité d'accompagner les victimes sur les aspects techniques de la réponse. La plateforme renvoie enfin vers le bon service lorsque l'État a mis en place une réponse spécifique pour une cybermalveillance précise.

De nombreux contenus de sensibilisation sont également disponibles sous différentes formes : guides, fiches pratiques, et autres vidéos car la prévention reste clé pour se prémunir des cyberattaques.

Depuis sa création, le trafic est en constante augmentation, ce qui démontre l'intérêt de la démarche et de la centralisation de la réponse, dans un monde où les cybermenaces sont en croissance permanente : 1,2 M de visiteurs en 2020, 2,4 en 2021, et 3,8 M en 2022.

Et parce que la cybermalveillance concerne l'ensemble de la société civile, les administrations et les entreprises, la réponse doit être collective. Le dispositif est ainsi porté par le Groupement d'Intérêt Public (GIP) ACYMA, composé de 62 membres issus du secteur public comme des Ministères, du privé et du domaine associatif, et qui contribuent chacun à sa mission d'intérêt général, dans une démarche d'accompagnement des victimes qui s'inscrit dans la logique du « guichet unique » de Cybermalveillance.gouv.fr.

Pharos

Depuis près de quinze ans qu'elle s'emploie à ce qu'Internet demeure fréquentable, la plateforme d'harmonisation d'analyse et de recoupement des signalements PHAROS peut témoigner que l'expansion du web — et subséquemment des médias sociaux — est allée de pair avec un accroissement, en nombre comme en intensité, des comportements odieux.

Toutefois, la place gagnée dans la vie quotidienne parce qu'il est usuel de regrouper sous le terme de « réseaux » est désormais telle que même les victimes de harcèlement numérique n'imaginent que rarement de s'en désinscrire, en dépit des expressions de profonde cruauté auxquelles elles ont pu être exposées.

Le succès foudroyant de ces nouveaux modes de communication pourrait donner à croire que ceux qui les opèrent sont devenus les dépositaires d'une forme de service public ce qu'infirme pourtant la demande insistante des internautes pour une plus grande régulation, laquelle demande confortant les pouvoirs publics dans leur rôle autant qu'elle les oblige.

Il convient néanmoins de prendre acte que la chose commune peut de nos jours procéder d'une hybridation mêlant à un niveau jamais atteint des considérations propres à la sphère privée à d'autres, originellement inhérentes à la sphère publique.

Dans ce contexte, l'expérience vient corroborer l'idée selon laquelle la préservation de notre environnement numérique est l'affaire de toutes et tous, de sorte qu'importent tant les actions individuelles que celles des organisations (associations, entreprises ou administrations).

Ceci n'allège nullement la charge qui incombe aux états dans la lutte contre les manifestations d'animosité en ligne et, s'agissant d'une problématique dont la plasticité le dispute à la complexité, les met perpétuellement au défi de parvenir à se montrer adaptatifs tout en menant une démarche régalienne cohérente.

Bien que fort nombreux, les signalements en rapport avec des contenus haineux reçus par PHAROS (quelque 18 000 durant l'année 2022, plus de 23 000 en 2021) ne sauraient constituer le seul socle sur lequel la plateforme doit s'appuyer pour appréhender le phénomène et fonder son action. À cet égard, l'augmentation régulière de ses facultés proactives et le renforcement des liens noués avec diverses structures de toutes tailles et de toutes natures — près d'une centaine de conventions d'ores et déjà conclues avec des organisations privées ou publiques — s'avèrent fondamentaux.

CyberNeTic

Le projet de recherche CyberNeTic vise à formaliser des questionnements scientifiques autour du cyberharcèlement pour comprendre les nouvelles formes d'expression de la cyberviolence, à identifier les comportements spécifiques qui leur sont attachés et à proposer à la gendarmerie nationale, partenaire privilégié, des dispositifs numériques innovants qui renouvellent les méthodologies d'intervention et de prévention en matière de cyberharcèlement.

C'est dans ce contexte particulier que la Division du Renseignement Criminel de la Gendarmerie Nationale, la Section Opérationnelle de Lutte contre les Cybermenaces de la Gironde ainsi que l'université Bordeaux Montaigne (axe Communication Organisation et Sociétés du laboratoire du MICA) se sont associés pour porter une dynamique de cybersécurité qui cherche à renforcer les compétences des gendarmes dans l'assistance aux victimes de cybermalveillance.

L'objectif premier est de pouvoir faire émerger du sens pour l'environnement stratégique en identifiant la nature des pratiques de cyberharcèlement, les phénomènes d'engrenage qui se démarquent dans la mise en place de ces processus cybermalveillants, les stratégies d'influence et de manipulation empruntées dans les discours de prédation, etc.

Du point de vue de la méthode, l'analyse de différentes situations de cyberharcèlement — notamment au travers de conversations entre mis en cause et victimes — permet de proposer une interprétation étayée de l'émergence du phénomène social dans différents contextes d'origine (porno divulgation, arnaque aux sentiments, usurpation d'identité, commentaires haineux, piratage de données personnelles, vigilantisme numérique, etc.). La recherche propose également comme livrables à la Gendarmerie Nationale des dispositifs numériques innovants tant en interne qu'en externe (fiches techniques, tutoriels vidéos, jeu vidéo, site internet de sensibilisation à l'hygiène informatique, application professionnelle pour accompagner les gendarmes dans la perquisition numérique, etc.).

Alors que les progrès technologiques rendent de plus en plus complexes les opérations de perquisition et de recueil de la preuve numérique, celle-ci demeure indispensable à la manifestation de la vérité et peut s'avérer préjudiciable si elle venait à manquer au débat pénal. C'est la raison pour laquelle le projet CyberNeTic développe actuellement un projet d'application aidant les forces de l'ordre de au recueil de preuves numériques. Ce dispositif a vocation à être partagé sur l'ensemble du territoire.

Brigade numérique de la Gendarmerie nationale

Dans un souci de modernisation et d'amélioration du contact avec les citoyens, la gendarmerie nationale a décidé de s'engager dans une démarche de proximité numérique, en créant la brigade numérique le 27 février 2018.

La brigade numérique permet à la population d'accéder et d'échanger avec la gendarmerie (hors cas d'urgence) dans l'espace virtuel (tchat) en tout temps et à partir de tout lieu. Appartenant au commandement de la gendarmerie dans le cyberespace et située à Rennes (35), elle s'intègre pleinement dans la police de sécurité du quotidien. Fonctionnant 24h/24 et 7 j/7, cette structure est composée de 33 gendarmes spécifiquement formés, (en majorité des officiers de police judiciaire) dont 28 remplissent la fonction d'opérateur.

Pour la gendarmerie nationale, la brigade numérique est en charge du fonctionnement de l'offre de service « Ma Sécurité » via le site internet et l'application mobile et de la plateforme numérique d'accompagnement des victimes (PNAV). Les opérateurs échangent et répondent pour toutes les questions relatives à la sécurité de manière générale, aux victimes ou témoins de violences conjugales sexuelles et sexistes (arretonslesviolences.gouv.fr), de cyberharcèlement et de discrimination.

L'expérience acquise de la relation à l'usager permet d'attester de la réelle efficacité ce mode d'échanges par tchat, un contact numérique qui répond à des réels besoins de la société et où l'humain est la clé de voûte. L'opérateur de la brigade numérique permet à un usager de créer une relation individualisée avec la gendarmerie et de bénéficier d'un accompagnement personnalisé. Cependant, le parcours de l'internaute peut être bloqué ou freiné tellement il existe de plateformes, d'applications mobiles et de numéros d'appel. La recherche d'une simplification des accès aux aides numériques devrait permettre d'améliorer encore l'efficacité du service public.

Enfin, ces dernières années témoignent d'une augmentation très importante des faits de cyberharcèlement (pour les faits connus), un phénomène de société qui ne cesse de s'amplifier. Ces atteintes se traduisent parfois par la diffusion massive de messages de haine dans des temps très courts ayant pour objectif ou effet d'atteindre la personne, sa fonction ou son activité professionnelle sans pour autant avoir d'effets immédiats sur les conditions de vie ou la santé physique ou mentale de la victime (constitution de l'infraction pénale au sens de l'article 222-33-2-2 du code pénal). Face à la fulgurance de ces atteintes, la recherche d'une action rapide devrait pouvoir permettre l'arrêt de ces cyberviolences et de protéger la victime en amont de conséquences sur ses conditions de vie ou sa santé.

StopFisha

L'association Stop Fisha lutte quotidiennement contre le cybersexisme et les cyberviolences sexistes et sexuelles en accompagnant des victimes, signalant des contenus illicites et sensibilisant le plus grand nombre à ces fléaux en plein expansion.

Être destinataire de propos à connotation sexuelle ou sexiste, c'est le quotidien des femmes dans la rue. C'est aussi, et même davantage, le quotidien des femmes en ligne.

Le constat est là : malgré les efforts mis en œuvre, nous ne parvenons pas à mettre un terme à la commission des infractions sur Internet. Trop souvent même après une condamnation pénale, l'envoi de messages haineux continue. Les cyberviolences sont tellement tolérées que celles et ceux qui en sont la cible s'entendent souvent dire qu'ils devraient quitter les réseaux sociaux, ce qui n'a d'autre effet que d'en faire peser la responsabilité sur la victime.

Aussi, dans les plus grosses affaires de cyberharcèlement, on ne retrouve devant le tribunal correctionnel, et seulement des années plus tard, qu'une dizaine de personnes quand les potentiels auteurs de l'infraction se comptent par milliers. Le traitement judiciaire de ces affaires est défaillant et nourrit un insupportable sentiment d'impunité.

Les cyberviolences, par leur nombre et leur viralité, sont des infractions de masse. Il est temps d'en prendre la mesure et de changer d'approche dans la façon dont notre justice pénale les appréhende. Et face aux infractions les plus courantes, nous avons une réponse : l'amende-forfaitaire, une sanction pénale prononcée sans procès, par un policier, un gendarme ou un agent public habilité qui constate une infraction déterminée.

C'est cette logique qui, face au trop grand nombre de comportements dégradants à connotation sexuelle ou sexiste dans la rue, a conduit à créer la contravention d'outrage sexiste surnommée « *harcèlement de rue* ».

S'il a été initialement pensé pour protéger les femmes de situations intimidantes, hostiles ou offensantes dans la rue, ce texte doit aujourd'hui s'appliquer sur Internet et l'utilisation d'un service de communication au public en ligne devenir une circonstance aggravante. Ce d'autant que sur Internet, la preuve de l'outrage sexiste ne posera plus de difficulté et cette contravention, devenue depuis peu un délit, trouvera toute son utilité.

L'amende-forfaitaire permettra, avec l'essentielle collaboration des plateformes et le déploiement de « *cyberpatrouilleurs* », de toucher les auteurs de propos sexistes en ligne chez eux, et de les sanctionner sans délai. Les « *sales putes* » sur Internet, comme dans la rue, ne doivent plus être tolérés.

III. RASSEMBLER

Porter les écosystèmes œuvrant à l'apaisement

De très nombreuses autorités, plateformes, associations ainsi que de nombreux citoyens agissent au quotidien pour l'apaisement de notre espace numérique. Leurs efforts sont considérables et méritent d'être soutenus. Ce soutien ne doit en aucun cas consister en un remplacement ou une centralisation. C'est pourquoi il est proposé d'intervenir à un niveau amont et de penser l'animation et la coordination des réseaux avant toute chose. Cela vaut tant pour les acteurs qui œuvrent pour le développement d'une citoyenneté numérique de manière générale (mesure 6) que pour ceux œuvrant directement à l'apaisement de l'espace numérique et dont l'action collective mérite d'être encouragée (mesure 7).

Soutenir les acteurs de la citoyenneté numérique

Fournir les clefs de compréhension et d'action à l'ensemble des publics est le point de dénouement de beaucoup des problèmes que nous rencontrons en ligne. Dans cet exercice, il importe que chaque acteur reste sur ses fondamentaux. Le rôle de l'école n'est pas celui des plateformes, tout comme celui de la société civile n'est pas celui des autorités. Dans cette idée, l'école apparaît comme le lieu de la transmission des fondamentaux de la citoyenneté, les plateformes celui de l'information concrète sur les conduites à tenir, la société civile celui de l'expression et de l'accompagnement des publics et les autorités celui de la prévention et de la bonne application de la loi.

Nécessairement, nos relations dans l'espace numérique ont un lien avec la façon dont on perçoit nos comportements et nos relations en dehors de cet environnement. C'est pourquoi il est toujours difficile de dissocier des apprentissages dédiés à la vie numérique de ceux dédiés à notre façon d'être en société. Ainsi la lutte contre les violences, l'éducation à la sexualité et aux relations affectives, l'esprit critique, la compréhension des médias et de l'information, les apprentissages qui peuvent permettre d'interagir et d'exprimer des sentiments ou des idées de manière pacifique sont autant de remèdes aux maux que l'on peut rencontrer en ligne.

Tout aussi naturellement, l'environnement numérique fournit une architecture à nos relations sociales et les modèle. Nous pouvons d'ailleurs observer que nos relations ne sont pas les mêmes sur tous les réseaux sociaux. Comprendre le fonctionnement de notre environnement numérique, les rouages des réseaux sociaux, les dynamiques qui animent certains acteurs sont autant de connaissances essentielles. Leur transmission passe par des disciplines telles que l'économie, l'informatique, la sociologie et les relations internationales appliquées au numérique.

Des dispositifs éducatifs déjà riches

Beaucoup de ces apprentissages figurent déjà dans les cursus d'apprentissage de l'Éducation nationale. Des complications peuvent être rencontrées pour que ces enseignements soient pleinement dispensés, mais la cause est entendue. Ce qu'il s'agit de rechercher est bien plus l'effectivité et la pertinence des enseignements promus que l'imposition de nouvelles lignes dans les cursus allant du primaire au secondaire. Sans oublier que les dispositifs déclinés ne peuvent pas tout : l'intime et l'empathie exigent parfois de sortir des cadres établis.

Pour ce qui concerne la lutte contre les phénomènes les plus néfastes, le ministère de l'Éducation nationale et de la Jeunesse agit notamment au travers de la mission chargée de la prévention des violences en milieu scolaire, l'instauration de nombreux programmes dédiés, mais aussi au travers d'enseignements dispensés aux élèves.

Les dispositifs éducatifs

Tout d'abord, les élèves suivent tout au long de leur cursus un enseignement moral et civique, dont une partie est dédiée aux questions d'égalité et du respect d'autrui. De plus, l'éducation à la sexualité vise à apporter des connaissances scientifiques et à cultiver des comportements responsables, valorisant le respect d'autrui.

PIX est la plateforme d'évaluation en ligne et de certification des compétences numériques, à destination des élèves du milieu éducatif et des étudiants de l'enseignement supérieur. Au-delà de la validation des compétences numériques, PIX propose depuis novembre 2022 des parcours de sensibilisation aux élèves dès la classe de 6e au bon usage des outils numériques et des réseaux sociaux ainsi qu'aux dérives et aux risques liés à ces outils.

Le Réseau Canopé est un opérateur du ministère de l'Éducation nationale et de la jeunesse. Il a pour mission de former les enseignants tout au long de leur carrière et en particulier aux outils numériques. Pour cela, il met à disposition des ressources en ligne, notamment sur la lutte contre les violences en milieu scolaire (contre le harcèlement et les discriminations). La plateforme Canotech, opérée par le réseau Canopé, met à disposition des enseignants des cours en ligne sur de nombreuses thématiques et notamment sur les sujets liés aux violences en milieu éducatif. Le Centre pour l'éducation aux médias et à l'information (Clemi) est chargé de l'éducation aux médias et à l'information dans l'ensemble du système scolaire français. Le site du Clemi met à disposition des enseignants des ressources (vidéos, ouvrages, contenus) permettant de favoriser par les élèves une meilleure compréhension des médias et des usages numériques.

Enfin, le GIP Trousse à projets met à disposition des parents des ressources sur la parentalité numérique, en ligne via la mallette des parents sur le site dédié de l'Éducation nationale.

S'il est essentiel de fournir ces apprentissages dans le cadre scolaire pour assurer le partage de fondamentaux à des publics particulièrement exposés ainsi que pour former les citoyens de demain, les problématiques liées à l'environnement en ligne ne sont pas le seul fait des plus jeunes. Et ils n'en sont pas non plus les seuls destinataires. Lorsque sont commis des faits de violence à l'encontre des femmes, lorsqu'il s'agit de protéger les enfants et donc de dispenser les informations pertinentes aux parents ou lorsque des personnes sont prises à parti en raison d'une expression politique, nous nous trouvons face à des problèmes sociétaux majeurs qui exigent une compréhension et un apprentissage qu'il est indispensable et urgent de fournir en dehors de l'école.

En dehors du parcours scolaire au sens strict, une myriade d'initiatives contribue à la diffusion d'un savoir sur le numérique, sur ses risques, ses opportunités et sur les comportements à adopter. Ces initiatives se déclinent partout en France grâce à

l'action d'un nombre incalculable de structures. Si ces organisations sont nombreuses, elles ne sont pas toutes bien identifiées et existent souvent grâce à des démarches volontaires, parfois bénévoles. Leur pérennité et leurs productions dépendent ainsi de la force de volontés ne bénéficiant pas d'un cadre structurant ou d'un soutien étatique coordonné. Fournir un tel cadre permettrait de mettre en visibilité, orienter et soutenir l'ensemble des productions et actions conduites. Tout l'enjeu est de savoir comment capitaliser sur les dynamiques d'acteurs sans les affaiblir, mais les nourrir et les rendre plus efficientes. Pour cela, il semble pertinent de penser la coordination des ressources et initiatives, plutôt que de chercher à les unifier ou les centraliser.

En effet, le recours à des sites officiels ou des institutions dédiées n'est pas toujours privilégié parmi les personnes devant être informées. Ainsi le dossier de presse associé à la récente campagne de sensibilisation à la parentalité numérique faisait apparaître que lorsqu'il s'agit de « recevoir des conseils concrets, [les parents se tournent] principalement vers les acteurs de proximité, comme les professionnels de santé (38 %) et les enseignants (25 %) et sont 33 % à privilégier un site internet officiel qui rassemble les bonnes pratiques en matière de parentalité numérique[36]. » Ce phénomène ressort tout autant des consultations tenues sur le site du CNR : les apprentissages au numérique passent beaucoup par la pratique ou par les proches, rarement par des institutions ou cursus dédiés[37]. Ce qui encourage à capitaliser sur les professionnels et organismes de proximité et donc à renforcer leur formation.

Ainsi, l'État pourra fournir un appui organisationnel à la création d'une plateforme de ressources, constituante du socle de cette connaissance partagée, regroupant les ressources fournies par et accessibles à toutes les parties prenantes. Ensuite, une coordination des acteurs de la citoyenneté numérique pourra aussi être organisée en s'appuyant sur le maillage local (associations, entreprises à impact, éducation nationale et populaire, structures de médiation, collectivités).[38] Enfin, joint à un dispositif d'évaluations, un soutien financier et logistique pourra être apporté.

Mesure 6 – *Un plan de soutien aux acteurs de proximité de la citoyenneté numérique sera engagé.*

---

[36] Voir le dossier de presse de la campagne Je Protège Mon Enfant.

[37] La 2e consultation en ligne réalisée dans le cadre du CNR numérique fait ressortir que 92% des contributeurs disent avoir déjà accompagné un proche dans des démarches en ligne.

[38] A l'image du travail de Génération numérique ou d'Internet Sans Crainte qui organisent de nombreuses formations auprès des personnes adultes sur les pratiques numériques des jeunes afin de mieux les accompagner dans leurs usages.

Instituer un forum d'échange dédié à l'apaisement de l'espace numérique

Non sans écho avec d'autres initiatives présentes ou passées, les enceintes de discussion créées dans le cadre du CNR Numérique ont donné à voir ce que pouvait être un forum rassemblant l'ensemble des personnes concernées. Lorsque sont réunies dans la même pièce des autorités, entreprises, associations, citoyens, influenceurs, joueurs en ligne, il se passe des choses profitables à tout un chacun. Des informations sont partagées, des mythes sont déconstruits, des solutions émergent, des relations se nouent. En bref, les problèmes sont mieux appréhendés par la formation d'un collectif animé vers un objectif commun.

Un premier constat qui a donc émergé de la période de temps offerte par le CNR est l'utilité de disposer de forums d'échanges animés par des acteurs indépendants et orientés vers la construction collective de solutions à des problèmes renvoyant à une responsabilité collective. Cette dynamique s'est inscrite dans le sillage des activités de l'observatoire de la haine en ligne animé par l'Arcom, avec cette particularité de pouvoir mobiliser des personnes utilisatrices des réseaux. Ainsi, les acteurs, et notamment les autorités et représentants de plateformes, ont pu échanger avec des parents, gameuses, lycéens, influenceuses, journalistes, personnalités politiques, etc.

Il serait utile de s'assurer que de telles expériences ne restent pas ponctuelles et donc d'assurer l'existence de tels temps d'échanges réguliers entre l'ensemble des acteurs. Cela permettrait notamment d'avoir une vue en temps réel des évolutions de pratiques et puis surtout garder des liens étroits entre tous. Mais il sera important que tous se sentent concernés et obligés à participer à ces échanges réguliers.

Une vaste part du tissu associatif dédié à l'apaisement de l'espace numérique nourrit des relations constantes avec les autorités ou les plateformes. Cela permet à la fois aux plateformes de fournir les informations nécessaires à la compréhension du fonctionnement des plateformes et aux associations de fournir des clefs de compréhension des phénomènes à l'œuvre, que ce soit sur ou hors des plateformes. Mais là encore, nous nous trouvons dans une situation où il existe relativement peu de mutualisation.

Une structuration de l'écosystème associatif autour des signaleurs de confiance est portée par la Délégation Interministérielle à la lutte contre le racisme, l'antisémitisme et la haine anti-LGBT (DILCRAH) dans son Plan national contre le racisme, l'antisémitisme et les discriminations liées à l'origine. Ainsi a été créé un portail autour de l'association Point de Contact, permettant de fédérer les acteurs associatifs autour d'une structure, qui assure le dialogue et le partage de bonnes pratiques avec les plateformes.

Qu'est-ce qu'un signaleur de confiance ?

L'exercice de la régulation dans le cadre du règlement sur les services numériques apportera des changements au long cours. Dans la poursuite d'efforts déjà engagés par certaines plateformes, des entités publiques ou privées dénommées signaleurs de confiance seront désignées au sein de chaque État membre par le coordinateur des services numériques, et seront responsables devant lui. Indépendantes des plateformes et comme toute association ou individu, ces entités détectent et signalent des contenus illicites aux plateformes. Ainsi, leurs signalements bénéficient du fait de leur sérieux, de leur expertise et de la confiance acquise, d'un traitement prioritaire.

Comme le font bien apparaître certains réseaux sociaux, des autorités et associations bénéficient déjà des accès suivants :

- Un formulaire de signalement dédié
- Des informations sur les décisions prises suite aux signalements opérés
- L'examen prioritaire des contenus signalés
- L'occasion d'échanger régulièrement avec la plateforme à propos des catégories de contenus illicites et des bonnes pratiques de signalement
- Des formations en ligne occasionnelles[39].

Si certaines associations et autorités bénéficient déjà d'un accès dédié, la reconnaissance en droit du statut de signaleurs de confiance constitue une véritable innovation, puisque le travail des associations devient partie intégrante du travail de régulation des plateformes. En effet, avec le règlement sur les services numériques, les signaleurs de confiance devront réaliser des rapports annuels sur le nombre de signalements effectués et l'efficacité de leurs démarches. Ils devront enfin être indépendants des plateformes.

Les échanges entre les plateformes, les autorités et la société civile pourraient avantageusement être mutualisés au sein d'un espace de dialogue commun. Un tel forum pourrait être l'occasion de créer des sessions d'échanges réciproques entre les personnes travaillant au sein des plateformes et le monde associatif. Dans un tel cadre, peuvent être imaginées des sessions de travail collectif dédiées à la formation des modérateurs sur les phénomènes sociaux nationaux, à l'amélioration des dispositifs de signalement, à la formation des associations aux bonnes pratiques de signalement, etc.

Demain, cette structuration sera essentielle pour accompagner la mise en œuvre de la régulation de l'ensemble des connaissances et actions portées par le tissu associatif.

[39] Notamment et à l'image de bien d'autres plateformes, le réseau social YouTube propose le programme YouTube Trusted Flagger d'où les éléments ici rapportés sont repris.

Il importe à ce titre de démultiplier les occasions de rencontres entre acteurs visant à faire émerger un dialogue apaisé et des propositions de solutions pour lutter contre la haine en ligne. Un tel cadre devra également assurer la rencontre avec le monde de la recherche et faire témoigner des personnes utilisatrices. Ainsi, il sera possible de parvenir à une plus grande implication de la société et à une mise en réseau de l'ensemble des parties intéressées autour de la régulation. Les collaborations directes entre chercheurs, associations et plateformes peuvent être intéressantes. Le forum pourrait en outre nourrir ses travaux des résultats du baromètre évoqué ci-avant.

De manière générale, impliquer les personnes en charge de la modération et du design des interfaces des principales plateformes peut aussi être instructif aussi bien pour elles que pour les personnes travaillant dans la société civile ou pour les autorités publiques. Sachant que de nombreuses plateformes accueillent des modérateurs bénévoles que ce soit sur des chaînes, des salons ou des groupes et mettent à leur disposition de nombreux outils. Réunir la société civile, les autorités et les communautés de modérateurs permettra de croiser et d'enrichir les pratiques des uns et des autres.

Depuis 2020, administrations, réseaux sociaux et société civile trouvent déjà un espace de dialogue multilatéral régulier au sein de l'Observatoire de la haine en ligne piloté par l'Arcom, qui l'a réuni environ 40 fois en 3 ans, que ce soit en format plénier ou en groupe de travail thématique. Le forum pourrait être l'émanation de cette structure à laquelle il serait donné un périmètre plus large, à savoir celui de l'apaisement de l'espace numérique.

Mesure 7 – *Un forum d'échange dédié à l'apaisement de l'espace numérique sera institué.*

La parole aux acteurs

Mission chargée de la prévention des violences en milieu scolaire

Ministère de l'Éducation nationale et de la jeunesse

Le cyberharcèlement est pleinement intégré à la politique de lutte contre le harcèlement menée par le ministère de l'Éducation nationale et de la Jeunesse (MENj).

Face à la montée de ce phénomène, le MENJ a créé une cellule dédiée à la lutte contre le cyberharcèlement en avril 2022 : la cellule de lutte « CyberNah », intégrée à la Mission chargée de prévention des violences en milieu scolaire (MPVMS) de la Direction générale de l'enseignement scolaire (DGESCO).

Cette cellule accompagne les académies sur la problématique du cyberharcèlement, organise avec le pôle harcèlement de la MPVMS les différents temps forts de la politique de la lutte contre le harcèlement (prix Non au harcèlement, journée NAH, Safer internet day, etc.) et développe des liens avec des partenaires institutionnels internes et externes autour des questions du cyberharcèlement dont notamment l'association e-Enfance/3018).

Le programme pHARe accorde une place importante à la lutte contre le cyberharcèlement et s'articule de la manière suivante :

les situations sont prises en charge par les équipes ressources (5 personnes en circonscription et 5 par collège) qui ont été formées à cette question, un volet pédagogique avec 10h d'apprentissage par an pour les élèves, du CP à la 3e, via des supports pédagogiques différents sur l'empathie, le cyber : ateliers de prévention au cyberharcèlement, à l'hyper-connexion, aux fake news ; intégration du « safer internet day » dans le programme pHARe ; mise en place d'un parcours pédagogique par cycle (cycle 2 Parcours « compétences psychosociales », cycle 3 Programme « empathic », cycle 4 Parcours « numérique ») ;

- un module de formation « ambassadeurs-collégiens » dédié au cyberharcèlement dans pHARe ;
- utilisation des campagnes qui ont remporté le prix spécial cyber pour sensibiliser les élèves au cyberharcèlement ;
- un prix spécifique vidéo dédié dans le cadre du concours annuel Non Au Harcèlement (NAH).

Pix

Face aux enjeux d'éducation au numérique et, en particulier, pour sensibiliser à la lutte contre le cyberharcèlement, les discours de haine et les contenus illicites en ligne, le ministère de l'Éducation nationale et de la Jeunesse a mandaté le GIP Pix pour élaborer un dispositif menant à la délivrance d'une attestation de sensibilisation au numérique, pour les élèves de 6e.

Ce dispositif repose sur deux parcours de tests sur la plateforme pix.fr :

- un parcours « Protection et Sécurité numérique » contenant un focus sur le cyberharcèlement et sa prévention (avec des questions portant sur les obligations légales pour les mineurs sur les réseaux sociaux, la connaissance des numéros d'écoute et de signalement, les moyens d'action pour réagir face à une situation de cyberharcèlement, etc.)

- un parcours « Initiation aux compétences numériques » permettant de poser les premiers jalons de culture numérique pour permettre aux élèves, non seulement d'être mieux armés face aux risques et dérives que le numérique peut représenter, mais aussi pour tirer pleinement parti de ses opportunités.

Ces deux parcours sont passés durant les deux premiers trimestres de l'année scolaire. Ils viennent en appui aux actions de sensibilisation portées par les enseignants et permettent aussi de créer un moment privilégié en classe pour échanger et débattre sur des sujets comme le cyberharcèlement.

En fin d'année scolaire, afin de valoriser les compétences acquises à l'issue de ces deux parcours, une attestation de sensibilisation au numérique adossée à la plateforme Pix sera alors remise aux élèves des classes de 6e par leur établissement.

Ce dispositif est le fruit d'un travail de terrain préalable auprès de 118 établissements volontaires. Il a permis de co-construire et d'améliorer le contenu pédagogique des parcours et d'en assurer l'adéquation avec les élèves de 6e. Dès 2024, chaque élève de 6e bénéficiera du dispositif.

De plus, chaque année, tous les élèves de collèges et lycées bénéficient de parcours de tests adaptés à leur niveau d'enseignement traitant entre autres, des enjeux numériques comme l'acquisition d'un regard critique sur les contenus en ligne, la sensibilisation aux dangers d'Internet et l'utilisation responsable des nouvelles technologies.

CNIL

La Commission nationale de l'informatique et des libertés (CNIL) offre un service de renseignement multicanal (postal, électronique, téléphonique), ouvert aux particuliers ainsi qu'aux entreprises, administrations et associations. Il permet de prendre connaissance de ses obligations et de ses droits en matière de protection des données personnelles.

En parallèle, la CNIL a fait de l'éducation au numérique, notamment des jeunes, une action prioritaire. Dans ce cadre, elle produit des ressources pédagogiques adaptées, se rend dans des établissements scolaires, anime un collectif d'acteurs engagés et travaille avec le ministère de l'Éducation nationale à la formation des enseignants.

Au fil du temps, ces relations avec des publics aux profils et aux niveaux de connaissance variés ont permis de faire évoluer la manière dont la CNIL communique. Elle a diversifié ses contenus sur son site web cnil.fr et a adapté sa manière de rédiger ses courriers et autres productions écrites. L'objectif est d'être plus compréhensible et plus accessible pour permettre à chacun de connaître la loi.

En effet, si plus de 83 % des ménages français possèdent un ordinateur et 96 % un téléphone portable, rares sont ceux qui connaissent la réglementation et notamment leurs droits *Informatique et Libertés*.

De récentes campagnes publicitaires utilisant la protection des données comme argument concurrentiel sont cependant le signe d'un intérêt réel et croissant des consommateurs pour le sujet.

C'est pourquoi la CNIL entend renforcer ses actions pour sensibiliser le grand public sur ses droits et lui donner les outils pour maîtriser ses données. C'est un véritable enjeu de société au regard de l'usage de plus en plus massif des données dans toutes les activités humaines. Maitriser ses données pour protéger sa vie privée devient une compétence indispensable à acquérir.

Parce qu'il est essentiel de s'appuyer sur celles et ceux qui sont au contact de la population chaque jour, la CNIL souhaite développer ses réseaux pour informer et protéger. Lieux d'accès au droit, de paroles, d'accompagnement, d'échanges : la richesse des organisations locales constitue un terreau fertile au développement d'espaces de partage et de sensibilisation, afin d'être au plus près des enjeux quotidiens des publics.

Parcourir ces derniers kilomètres pour toucher nos concitoyens s'avère indispensable pour la CNIL. Par l'écoute et le dialogue, la réalisation d'ateliers sur le terrain, la production et la diffusion de ressources adaptées, elle entend leur rendre un pouvoir qu'ils possèdent déjà mais ne connaissent pas toujours.

Point de Contact

Point de Contact, association loi 1901, propose différents outils permettant aux internautes de signaler anonymement, gratuitement et simplement les contenus choquants potentiellement illicites en ligne afin d'en obtenir le retrait auprès des hébergeurs et plateformes numériques, tant en France qu'à l'international.

L'association s'érige comme un pont opérationnel entre les acteurs privés et les institutions publiques dans la lutte contre les contenus illicites sur Internet tels que les violences et exploitations sexuelles de mineurs, la provocation à la haine ou encore les contenus à caractère terroriste, entre autres. Elle est reconnue comme « tiers de confiance » auprès des grandes plateformes, hébergeurs, et fait le lien avec les autorités nationales de police et de gendarmerie : Point de Contact est le premier signalant professionnel auprès de PHAROS. L'association s'investit également pour informer, sensibiliser et responsabiliser les internautes sur les contenus et les comportements répréhensibles en ligne et œuvre à valoriser et faire reconnaître le travail d'analyste.

Forte de son expertise depuis plus de 20 ans dans la lutte contre les violences numériques, Point de Contact appuie la nécessité de rationaliser les processus de signalement, pour faciliter l'orientation des utilisateurs, et fluidifier les relations entre les différentes parties prenantes publiques et privées. Grâce au développement de technologies et de relations partenariales opérationnelles fortes, Point de Contact tend à :

- Harmoniser les processus (formulaires, catégories d'infractions par exemple) avec les plateformes et autorités, et fluidifier les échanges via des outils automatisés de communication (API).
- Orienter au mieux les signalants vers les différents acteurs pertinents selon leur situation, en développant un module d'orientation qui sera directement rattaché aux outils de signalements, pour répondre au plus près des besoins des internautes.
- Rationaliser et assurer la coopération opérationnelle et stratégique entre les acteurs, associatifs, privés et publics en devenant notamment guichet unique de signalement des contenus haineux (dans le cadre du nouveau plan national de lutte contre le racisme, l'antisémitisme et les discriminations liées à l'origine), pour fluidifier le traitement des signalements fait à PHAROS. Ceci pourrait s'étendre à d'autres infractions entrant dans le champ de compétences de Point de Contact.

Enfin, il semble essentiel de voir sanctuariser un budget d'intervention pour les acteurs impliqués dans la lutte contre les contenus choquants rencontrés en ligne. Allouer des budgets conséquents et durables, pour permettre de pérenniser l'action et assurer de continuer à protéger au mieux les internautes face à l'évolution constante des pratiques numériques.

e-Enfance/3018

L'Association e-Enfance (reconnue d'utilité publique) protège les mineurs sur internet depuis 2005. Acteur de prévention, elle sensibilise 200 000 enfants, jeunes, parents et professionnels par an. Missionnée par la Commission européenne depuis 2008 (programme Safer Internet), elle opère la helpline française 3018, numéro court national pour assister les jeunes victimes de violences numériques. Le réseau INSAFE des helplines européennes a ainsi été précurseur du modèle des « signaleurs de confiance », avant le que le DSA ne le consacre.

En France, plus qu'une simple plateforme de signalement, le 3018 est un service grand public qui prend en charge immédiatement les situations des enfants et adolescents victimes de violences en ligne, de manière globale et transverse. Les écoutants sont accessibles 7 jours sur 7, de 9 h à 23h, par téléphone, Tchat, Messenger et via l'application 3018 (dotée d'un coffre-fort pour enregistrer puis envoyer de façon confidentielle les preuves de violences numériques subies). Une équipe de 20 professionnels psychologues, juristes et spécialistes des outils numériques, intervient à la demande des appelants jeunes victimes et leur entourage (parents ou professionnels).

Depuis 2010, le 3018 est devenu « signaleur de confiance » auprès d'une vingtaine de plateformes et réseaux sociaux. Cela signifie que le 3018 bénéficie d'un accès direct aux services de modérations des plateformes, afin de leur demander la suppression de tout compte ou contenu préjudiciable à un mineur. Cette procédure accélérée de signalements contextualisés, alliée à une longue et forte coopération quotidienne, permet le retrait en 24 à 72 heures dans 95 % des cas, voire en moins d'1 heure de contenus type violation de contenus intimes d'enfants et d'adolescents. Dans le même temps, en France le 3018 a signé des conventions avec les principaux acteurs institutionnels impliqués, afin de garantir un traitement prioritaire et coordonné aux situations des jeunes victimes et leur orientation (dépôt de plainte, suivi psychologique, etc).

L'efficacité du service fait déjà ses preuves, le 3018 est devenue une best-practice européenne pour la modélisation des « signaleurs de confiance » locaux prévus par le DSA. Et elle sera améliorée par sa systématisation, notamment en termes de transparence et d'harmonisation, voire d'automatisation. Mais il est nécessaire aujourd'hui de renforcer leurs moyens pour les pérenniser et pour garantir la qualité de leur service et leur indépendance. Et dans un monde où l'impact du numérique a pris une telle ampleur notamment sur le développement et la santé des jeunes, il est indispensable de faire savoir que ce service innovant et efficace, conçu pour les enfants et les adolescents (et leurs parents) existe. Ainsi, toutes les parties prenantes doivent participer à la promotion des helplines, partout, tout le temps et par tous leurs meilleurs moyens, hors ligne et en ligne.

Mais créer un environnement apaisé pour les adolescents sur les réseaux sociaux suppose au préalable de pouvoir les « identifier » en tant que mineurs. La vérification de l'âge est la clé de voûte de la protection de l'Enfance sur Internet. C'est la condition sine qua non pour pouvoir leur garantir leurs droits spécifiques, d'agir comme d'être protégés. Ainsi repérés ils pourront bénéficier de paramétrages et de fonctionnalités ad hoc en ligne, en cohérence avec leurs droits hors ligne. C'est pourquoi dans ce cadre, il nous permet indispensable, pour leur garantir un environnement numérique adapté et sécurisé, que les comptes/profils de mineurs comportent tous un « safe button », visible et accessible, qui renvoie directement à la helpline du réseau INSAFE du pays concerné (en France le 3018). Et de la même façon que le contrôle parental a été rendu obligatoire dans tout outil numérique, l'application 3018 — et celles de ses homologues helplines européennes — doit être obligatoirement embarquée par défaut.

Tralalere

Depuis 15 ans, Tralalere coordonne le Safer Internet France et opère Internet Sans Crainte, le programme national de sensibilisation des jeunes au numérique de la Commission européenne. Notre mission est d'outiller les éducateurs et les parents pour leur permettre d'accompagner les enfants et les adolescents dans des usages éclairés et responsables des écrans.

Nous constatons que le cyberharcèlement est en tête des préoccupations des parents comme des jeunes. Ce thème est celui pour lequel nous avons le plus de ressources, une trentaine. Nous proposons par exemple le programme « Vinz et Lou stoppent la violence » pour sensibiliser les 7-11 ans au cyberharcèlement avec des vidéos et des parcours numériques. Nous avons aussi développé des outils qui permettent de travailler le vivre ensemble, l'empathie, l'égalité, l'altérité, car ces compétences sont clés pour éviter et désamorcer les situations de violence. Nous proposons également une offre de formation professionnelle et l'animation d'ateliers de sensibilisation. Nous travaillons depuis 4 ans avec les services de l'Éducation nationale pour construire des outils pour les classes. Nos outils de prévention des violences en ligne sont disponibles dans la plateforme pHARe.

Nous constatons que les actions de sensibilisation aux cyberviolences portent majoritairement sur l'identification du harcèlement et les moyens d'action. Cette démarche est essentielle mais elle n'est pas suffisante pour travailler en amont les causes du harcèlement.

La prévention est clé pour une approche complète et plus en amont du problème :

- Travailler l'empathie, l'altérité, l'acception et le respect de soi et des autres dès le plus jeune âge. Ces compétences psychosociales devraient être intégrées aux programmes scolaires et faire l'objet d'un temps dédié.
- La prévention des cyberviolences passe aussi par une bonne connaissance du droit en ligne. La plupart des jeunes et des parents que nous rencontrons n'ont pas connaissance des lois qui encadrent leurs pratiques numériques et des responsabilités qui leur incombent. Une meilleure information en amont des jeunes, comme de leurs responsables légaux, pourrait éviter certaines situations dramatiques.
- Dans certains espaces, en ligne et hors ligne, la parole haineuse se banalise. Il n'est pas facile pour certains d'identifier et qualifier une parole haineuse. Il est essentiel de développer des supports qui permettent de sensibiliser aux discriminations, aux mécanismes des discours de haine pour apprendre à les repérer et savoir les déjouer. Et d'intégrer et généraliser dans les réseaux sociaux et messageries en ligne, des outils de détection de la parole haineuse et des messages de prévention pour les utilisateurs.

- Repenser le parcours utilisateur sur les réseaux sociaux pour intégrer des messages de prévention sur les bonnes pratiques, les droits et devoirs en ligne au fil de son utilisation. Les professionnels aux contacts des jeunes confrontés à une situation de cyberharcèlement ne sont aujourd'hui pas suffisamment formés aux mécanismes des cyberviolences. Former ces professionnels est clé pour repérer les situations plus en amont et mieux accompagner auteurs, témoins et victimes.

Lucie Ronfaut, journaliste, autrice de la newsletter #Règle30

Je m'appelle Lucie Ronfaut, je suis journaliste et je me spécialise dans les questions de société et d'inclusion dans le numérique. Par exemple, j'ai réalisé un documentaire intitulé « La solitude du modo », qui interroge des modérateurs et modératrices pro et amateur·es. Un cas m'a particulièrement marqué : celui d'une autrice féministe qui était tellement submergée de haine qu'elle a dû embaucher une modératrice personnelle. C'est elle qui regarde ses messages à sa place pour signaler et supprimer le pire.

Je considère qu'internet c'est la vraie vie, et que ce qui se passe dans la rue a autant d'importance que ce qui se passe en ligne. Concrètement, on est dans une situation où des femmes n'ont pas d'autres choix que d'embaucher des gardes du corps, car personne ne les protège dans ces rues numériques.

La modération est un sujet complexe, car les plateformes sur lesquelles on évolue sont trop grosses pour être contrôlées. Alors on propose généralement aux internautes de bloquer ou masquer la haine, parce que c'est plus facile que de régler les problèmes structurels et économiques à l'origine de ces violences. La conséquence de ce système, c'est que les internautes deviennent responsables de leur propre tranquillité.

Mais la haine en ligne est bien un problème collectif. Comme beaucoup d'experts et d'expertes, je regrette que les grandes plateformes soient si peu transparentes sur leurs efforts de modération en France. Qu'il soit encore difficile de porter plainte, de retrouver les auteurs des cyberviolences, que la plateforme PHAROS fonctionne avec seulement une cinquantaine d'agents et d'agentes. Surtout, on a besoin d'éduquer sur ces sujets, pas seulement de punir. Pourquoi est-ce qu'une personne s'autorise à en insulter et menacer une autre ?

L'Assemblée nationale a publié en février les conclusions d'une mission sur l'éducation critique aux médias, qui souffre de grandes disparités territoriales. Je travaille beaucoup avec des professeurs documentalistes et des médiathécaires, qui parlent très bien d'internet aux jeunes avec trop peu de moyens. Je crois qu'on doit investir davantage dans ces efforts. Parce que l'éducation au numérique ce n'est pas qu'apprendre à coder. C'est aussi réfléchir à sa place dans notre société.

ALLER PLUS LOIN

18 propositions faites par les participants

Au cours des réunions et échanges ayant eu lieu dans le cadre du CNR Numérique, de nombreuses propositions ou actions ont été partagées par les participants. Toutes ne peuvent figurer dans l'immédiat de la présente feuille de route, faute de dépendre de compétences d'autres acteurs, renvoient à des décisions budgétaires qui relèvent d'autres enceintes de débat, tandis que d'autres sont déjà engagées ou relèveront de l'exercice de la régulation. Ces propositions sont toutefois listées ci-après.

Éduquer et former le plus grand nombre

1. **Étendre le dispositif PIX aux utilisateurs de tout âge**

   Pix est un outil de certification des compétences utilisé par de très nombreux élèves et professionnels, qui vise également à sensibiliser aux grands enjeux du numérique. À l'initiative du ministère de l'Éducation nationale et de la Jeunesse, Pix a élaboré pour les élèves de 6e un parcours de sensibilisation aux grands enjeux du numérique, et notamment à la haine en ligne et au cyberharcèlement. Alors que la haine en ligne affecte l'ensemble de la population, il pourrait être opportun d'étendre le dispositif Pix de sensibilisation aux grands enjeux du numérique aux utilisateurs de tous âges et d'inscrire ce parcours dans un apprentissage tout au long de la vie.

2. **Renforcer l'éducation à la sexualité et aux enjeux associés**

   L'éducation à la sexualité est inscrite au programme de l'Éducation nationale et de nombreux modules sont également disponibles en ligne. Il prévoit la transmission, tout au long de la vie scolaire et dans les différentes matières dispensées, d'informations scientifiques concernant la sexualité ainsi que l'éducation à la vie affective (respect de l'autre, image de soi, acceptation de la différence, empathie, confiance en soi). De nombreuses ressources explicatives et pédagogiques sont disponibles notamment depuis le portail Educscol.

   Pour autant, des associations opposent que les enseignements à la vie affective sont peu dispensés en pratique. Les raisons pour cela peuvent s'entendre : difficulté d'aborder ces sujets dans le cadre strict de la classe, manque de temps, de formation. Les risques peuvent rapidement prendre le pas.

Dans un environnement social et médiatique en éveil sur ces questions, de nombreux acteurs de la société civile animent des comptes, plateformes et contenus en lien avec nos vies sexuelles et affectives et fournissent autant de ressources disponibles. Entre de nombreuses autres organisations, Internet Sans Crainte met à disposition des programmes d'apprentissage de la vie affective : cultiver l'empathie, respecter autrui et accepter la différence. Encourager massivement l'intervention d'acteurs tiers peut faciliter la transmission de ces connaissances.

3. **Poursuivre le programme pHARe**

Le programme pHARe vise à lutter contre le harcèlement à l'école qui, bien qu'encore récent, s'avère porteur. Mis en place à la rentrée 2021, il a été étendu à tous les écoles et collèges en 2022. Ce programme est construit sur 8 piliers, dont le premier est celui de la mesure du climat scolaire. Les autres piliers sont dédiés à la formation de la communauté, à l'intervention des enseignants, à la mobilisation des instances démocratiques des établissements et à l'association des parents au dispositif. Nécessairement, ce programme requiert les moyens, notamment humains, devant être associés à son effectivité.

Il prévoit trois temps forts de sensibilisation à mettre en place durant l'année scolaire : la journée « Non au harcèlement » (organisée chaque mois de novembre depuis 2013), le prix « Non au harcèlement » (depuis 2013) et le Safer Internet Day (tous les ans au mois de février). Ce programme sera étendu aux lycées à la rentrée 2023 et l'information sur les numéros d'urgence sera systématisée : 3018 (pour le cyberharcèlement) et 3020 (pour le harcèlement). Des ressources et protocoles sont disponibles pour l'ensemble des publics et professionnels sur le site du programme.

4. **Construire des règles de la communauté dans le secondaire**

Tout en respectant l'âge requis pour aller sur les réseaux sociaux, la période du collège ou du lycée peut être mise à profit pour sensibiliser sur le fonctionnement des réseaux sociaux et notamment sur la construction et l'application de ses règles d'utilisation. Les échanges entre élèves sur ce qui peut être accepté ou non de dire, sur la qualification des comportements peuvent être instructifs, amener le débat et une forme de compréhension sur ce qui est interdit ou devrait l'être. Mais surtout cela permettrait de construire des échanges sur la vie en collectivité, ce qui est acceptable ou non et laisser une place au ressenti de chacun.

La formulation collective de règles de vie en ligne et leur comparaison avec les règles de la communauté des principaux réseaux sociaux peut être instructive. De nombreux réseaux sociaux mettent pour cela du matériel pédagogique à disposition. Pour passer à l'action, il serait aussi possible de se saisir du réseau

social Mastodon qui, en tant que logiciel libre, permettrait d'appliquer les règles de la communauté à l'échelle d'un réseau social dédié par exemple à un établissement, au lycée par exemple.

Il est d'ailleurs à rappeler qu'une charte pour l'éducation à la culture et à la citoyenneté numérique a été récemment rédigée par le ministère de l'Éducation nationale et de la Jeunesse, en lien avec l'Arcom, la CNIL et le Clemi. Dans la poursuite d'autres chartes, elle a vocation à servir de support à réflexion et à l'action sur les bons usages du numérique dans le cadre scolaire.

Améliorer la réponse pénale

Extrait du compte-rendu de l'atelier du 22 mars 2023

Il semble exister le sentiment que de nombreux progrès ont été réalisés par les autorités pour améliorer la prise en charge des victimes, le dépôt et le traitement de leur plainte.

Si ces améliorations sont constantes, elles se heurtent au manque de moyens des forces de l'ordre et des institutions judiciaires. L'action des autorités n'est pas jugée dissuasive, ce qui peut générer un sentiment d'impunité et permettre la récidive des auteurs de ces violences. Il y a l'idée pour les femmes entendues qu'il est nécessaire de responsabiliser les auteurs de violences face à leurs comportements illicites.
Plusieurs femmes ont également témoigné du manque d'accessibilité financière de la Justice, notamment au regard de l'ampleur du cyberharcèlement subi et du coût financier induit pour les victimes.

Outre les dépenses judiciaires, les participantes à l'atelier témoignent des frais annexes qui leur ont été imposés : par exemple, des frais de déménagement, de changement de numéro de téléphone, de soutien psychologique.

Elles ont également fait part des difficultés rencontrées dans le dépôt et le traitement de leur plainte : un manque de sensibilisation des forces de l'ordre lors du dépôt de plainte, la lenteur du processus judiciaire, qui aboutit à un nombre limité de condamnations. Cette situation participe à générer un sentiment déceptif pour les victimes et d'impunité pour les agresseurs. Face à ces constats, certaines participantes réfléchissent à l'opportunité d'instaurer des mesures contraventionnelles, sur la base du fonctionnement d'Hadopi, afin de sanctionner plus systématiquement les agresseurs.

5. Réfléchir à l'instauration d'une réponse contraventionnelle automatique

Pour répondre au sentiment d'impunité qui habite les auteurs de violences en ligne, plusieurs participants ont partagé la nécessité de réfléchir à l'instauration de mesures contraventionnelles afin d'améliorer la réponse des autorités face aux phénomènes de haine en ligne. Inspiré du dispositif Hadopi, celui-ci viserait à imposer des amendes forfaitaires.

6. **Renforcer la formation des forces de l'ordre**

   Afin d'assurer une meilleure prise en compte des problématiques liées aux violences en ligne, il a été proposé d'améliorer et de renforcer la formation des forces de l'ordre aux évolutions des pratiques en ligne, aux spécificités des violences sexistes et sexuelles en ligne, au recueil de plainte pour des faits de violences en ligne et aux modes de collecte de preuve numérique.

7. **Accroitre les moyens des juridictions**

   Plusieurs échanges ont mis en lumière le manque de moyens des juridictions pénales pour instruire les enquêtes à un rythme qui soit satisfaisant, sans que cela soit dû uniquement aux affaires en matière numérique et peut aggraver leurs séquelles psychologiques. Aussi, le rôle du juge apparaît par ailleurs comme fondamental pour garantir l'équilibre des droits fondamentaux, là où les autorités administratives ne peuvent constitutionnellement se voir confier des modalités d'actions aussi étendues, notamment en matière de blocage.

8. **Améliorer l'accessibilité financière à la justice pénale**

   L'accessibilité financière à la justice a été évoquée comme entrave à l'action de tous malgré les dispositifs d'aide judiciaire existants. Pour y pallier, il a été proposé d'assurer le déclenchement de l'aide juridictionnelle dès le dépôt de plainte.

9. **Faciliter la collecte de preuves numériques**

   En matière de cyberharcèlement tout particulièrement, la collecte de preuves reste un problème particulièrement prégnant pour les utilisateurs qui ne peuvent raisonnablement pas collecter les preuves des agissements qu'elles peuvent subir, qu'un commissaire de justice soit requis ou non. De ce fait, de très nombreuses procédures pénales ne peuvent être engagées faute de preuves suffisantes. Le chantier permettant de parvenir à un dispositif de collecte rapide et à un coût nul d'une preuve exploitable pénalement doit être mené de manière prioritaire.

   De manière corollaire, un bouton de signalement entrainerait la conservation par les plateformes des contenus signalés afin de ne pas être effacés et d'être mis à disposition de procédures ultérieures. Ils pourraient être mis « hors de vue » mais être archivés pour être rendus accessibles au juge par exemple. Les utilisateurs pourraient alors bien supprimer ou faire supprimer les contenus qui leur portent atteinte et leur sont insupportables).

10. **Mettre les décisions des juridictions pénales à disposition du public**

    La mise à disposition du public de décisions de justice adoptées en matière pénale est importante pour assurer une bonne compréhension du public et des

acteurs des modalités d'application des lois applicables. Selon l'article 3 de l'arrêté du 28 avril 2021 pris en application de l'article 9 du décret n° 2020-797 du 29 juin 2020 relatif à la mise à la disposition du public des décisions des juridictions judiciaires et administratives, la mise à disposition du public des décisions juridictionnelles en matière pénale se fera à compter du 31 décembre 2024 pour les juridictions du fond. Cette évolution dans la politique d'open data des décisions de justice est attendue.

11. Travailler sur un parcours de suivi du signalement et des plaintes entre les autorités relevant du ministère de l'Intérieur et de la Justice

Les victimes peuvent avoir le sentiment que les plaintes déposées ne font pas l'objet du suivi dont elles devraient bénéficier, ce qui peut entraîner une perte de confiance envers les autorités. À travers un parcours de suivi dédié, les victimes pourraient être informées de l'avancement de leur dossier et les autorités seraient en mesure de mieux coordonner leurs actions pour garantir une réponse rapide et efficace aux signalements et plaintes déposées. En outre, cela permettrait également de mieux évaluer l'efficacité des politiques publiques mises en place pour lutter contre les violences et les discriminations.

Développer une atmosphère de confiance et de sécurité

12. Aller vers le *Dites-le-nous-une-fois* du signalement

L'idée de « Dites-le-nous-une-fois » en matière de signalement vise à simplifier les procédures en permettant de signaler une agression ou une infraction à une seule entité. Cela faciliterait aussi le travail des autorités en centralisant les informations et en permettant une meilleure coordination entre les différents services impliqués. Un tel dispositif devrait garantir la protection des données personnelles des victimes et s'assurer que leur consentement soit obtenu avant tout partage d'informations. Il exigerait aussi d'organiser l'interopérabilité entre les entités compétentes. Enfin, pour assurer un traitement efficace du signalement, l'idée d'un service mutualisé entre plateformes a été partagée.

13. Construire un protocole clair pour assurer la protection des personnes

Il semble nécessaire de penser à la mise sur pied d'un protocole clair face à la violence en ligne allant de la prévention jusqu'au traitement des conséquences des actes subis en passant par le traitement du signalement. Penser une telle liaison au long cours commence par initier une réflexion sur les modalités de retour à l'utilisateur à la suite de son signalement. Tous les acteurs ne peuvent pas effectuer de retour d'information, en raison des risques d'atteinte au secret des enquêtes judiciaires. Pour autant une liaison fiable entre toutes les plateformes et autorités compétentes et les personnes concernées est bien nécessaire. Au-delà, au regard des conséquences des violences en ligne sur les victimes, il importe de penser leur suivi au long cours.

14. Créer une norme technique internationale sur les processus de modération

Dans la lignée des mesures pouvant être prises par la Commission européenne en matière de standards techniques[40] au titre du règlement sur les services numériques, il serait intéressant de réfléchir à une norme technique du type ISO sur la modération pour harmoniser les processus de modération.

15. Permettre aux utilisateurs de protéger leurs informations confidentielles

Les professionnels ont souvent besoin de constituer de structures juridiques pour exercer leur activité. Plusieurs personnes ont témoigné du fait que leurs proches ou leur domicile avaient été trouvés par leurs harceleurs du fait de la publication des informations légales liées à la création de sociétés ou d'associations. Des aménagements devraient être possibles lorsque cette

[40] L'article 44 du règlement sur les services numériques prévoit que la Commission européenne peut encourager le développement de normes techniques pour la modération des contenus illicites en ligne.

publicité est à l'origine d'un risque particulier. Si ces moyens existent, ils devraient être partagés aux influenceurs et autres personnalités exposées.

16. Soutenir la production et la diffusion de contenus positifs

De nombreuses initiatives visent à soutenir la création sur les réseaux sociaux, participant à cultiver la richesse de la vie en ligne ainsi qu'à l'acquisition de compétences (montage, réalisation vidéo, construction narrative, sous-titrage, etc.). Dans leur poursuite, des collectivités territoriales, établissements scolaires ou professionnels pourraient s'associer avec des acteurs de la production audiovisuelle ainsi que des réseaux sociaux[41]. Des projections locales peuvent enfin participer à la valorisation des contenus produits et savoirs engrangés.

17. L'engagement du personnel politique en faveur de l'apaisement de l'espace numérique

Pour lutter contre le harcèlement en politique et promouvoir des pratiques éthiques dans le cadre du débat démocratique, les partis politiques et institutions les plus concernées pourraient s'engager lorsque ce n'est pas déjà le cas à diffuser et faire signer une charte de bonne conduite et à adopter des dispositifs de contrôle adéquats. Dans une recherche d'exemplarité, une charte commune ou plusieurs chartes du même type pourraient servir de guide pour les comportements attendus de la part du personnel politique en matière de respect, de tolérance et de dialogue constructif. Sur cette base, des programmes de sensibilisation et de formation sur le harcèlement pourraient être dispensés à l'intention du personnel politique.

18. Renforcer les mécanismes de circulation de l'information entre professionnels

De nombreuses pratiques à risque émergent quotidiennement, notamment dans l'environnement scolaire. Or, les enseignants qui s'y trouvent les premiers exposés n'ont pas nécessairement les moyens de partage de l'information avec leurs pairs ou avec les autorités compétentes.

À court terme, une solution pour assurer une circulation de l'information entre personnels publics de manière sécurisée et confidentielle peut être l'utilisation, parmi d'autres outils disponibles, de l'application de messagerie privée Tchap, accessible à l'ensemble du personnel étatique. Cette plateforme sécurisée facilite en effet le partage d'informations pertinentes entre les professionnels publics compétents, favorisant ainsi une meilleure coordination dans la gestion

[41] Pour le cas d'un concours de vidéos TikTok lancé par la mairie de Cannes ou un concours de photos sur les réseaux sociaux mettant en valeur le patrimoine local lancé par la mairie de Mamers, voir Laurent Vareille, *Un concours de vidéos sur TikTok récompensé lors du festival de Cannes*, France Bleu, 15 avril 2022 ou encore Carine Mordrelle, Fabienne Even. *Sarthe. Mamers lance un concours de photos sur les réseaux sociaux*, France 3, 12 février 2022.

des questions liées aux conduites à risque. De plus, elle offre l'opportunité de développer des dispositifs de veille collaborative, aussi bien à l'échelle locale que nationale. S'il revient à chaque communauté de mettre en place ses circuits d'information adaptés, les autorités centrales ou déconcentrées pourraient jouer un rôle dans l'impulsion et le partage des meilleures pratiques.

Listes des entités et personnes contributrices ou participantes

Institutions publiques

- Arcom
  - Jeremy Bonan
  - Manon Cassoulet-Fressineau
  - Lucile Petit
- Assemblée nationale
  - Erwan Balanant
  - Paul Midy
  - Véronique Riotton et Ariane Moret
  - Prisca Thevenot
- Comité interministériel de prévention de la délinquance et de la radicalisation (CIPDR) :
  - Hélène Debiel
- Conseil national du numérique
  - Marie Bernhard
  - Jean Cattan
  - Margot Godefroi
  - Joséphine Hurstel
  - Yaël Morinière
  - Joëlle Toledano
- Cybermalveillance.gouv.fr
  - Franck Gicquel
  - Alexandra Ketchayan
  - Jérôme Notin
- Défenseur des droits
  - Céline Girardot
- Délégation interministérielle à la lutte contre le racisme, l'antisémitisme et la haine anti-LGBT (DILCRAH)
  - Shani Benoualid
  - Hana Ouatik
- Direction interministérielle du numérique (DINUM)
  - Fadila Leturcq
  - Marion Loustric
- Direction interministérielle de la transformation publique (DITP)
  - Mariam Chammat
  - Stephan Giraud
- Gendarmerie nationale
  - Sébastien Possemé
  - Barnabé Watin-Augouard
- Haut Conseil à l'Egalité entre les femmes et les hommes
  - Xavier Alberti
- Ministère de la Culture
  - Michel Petit
- Ministère de l'Économie et des Finances
  - Damien Caillou
  - Chantal Rubin
- Ministère de l'Éducation nationale et de la Jeunesse
  - Sadate Hamadi
  - Mathilde Leucci
  - Vivien Turc
- Ministère de l'Europe et des Affaires étrangères
  - Paul Schmite
- Ministère de la Justice
  - Xavier Leonetti
- Parquet des Mineurs de Paris
  - Lisa-Lou Wipf
- PHAROS
  - Jean-Baptiste Baldo
- PIX
  - Marie Bancal

    - Déborah Dobaire
    - Sophie Puig de Fabregas
- Pôle d'expertise de la régulation numérique (PEReN)
    - Nicolas Deffieux
    - Camilla Penzo
- Pôle national de lutte contre la haine en ligne
    - Grégory Weill

Plateformes

- Dailymotion
    - Sébastien Leroux
- Google
    - Thibaut Guiroy
    - Benoît Tabaka
    - Arnaud Vergnes
- Jeuxvideos.com
    - Frédéric Fau
- Meta
    - Élisa Borry
    - Clotilde Briend
    - Jeanne Elone
    - Béatrice Oeuvrard
- Snapchat
    - Sarah Bouchahoua
- TikTok
    - Louis Ehrmann
    - Sarah Khemis
- Twitch
    - Olaf Cramme
    - Conner McDowell
- Twitter
    - Claire Dile
    - Alica Garza

Entreprises

- AXA
    - Véronique Jeandot
- Bodyguard
    - Manon Salletta
- C-Ways
    - Jean-Thomas Muyl
- EduPad
    - Daniel Jasmin
- Internet sans crainte
    - Axelle Desaint
- OVHcloud
    - Alexandre Dangreau
- Tralalère
    - Deborah Elalouf-Lewiner
- Tremau
    - Louis-Victor de Franssu
- Yoti
    - Florian Chevoppe-Verdier

Associations

- Crif
    - Robert Ejnes
    - Sophie Taieb
- Civic Fab
    - Samira Bourezama
- e-Enfance/3018
    - Justine Atlan
    - Samuel Comblez
- Féministes contre le cyberharcèlement
    - Johanna-Soraya Cayre-Benamrouche
    - Ketsia Sabwe Mutombo
    - Laure Salmona
- Génération Numérique :
    - Cyril di Palma
- #Jesuisla
    - Xavier Brando
- Ligue des droits de l'Homme
    - Maryse Artiguelong
- Licra
    - Maia Feijoo
- Osez le féminisme
    - Céline Piques
- Point de Contact
    - Quentin Aoustin

    - Jean-Christophe Le Toquin
    - Yann Lescop
    - Alejandra Mariscal Lopez
    - Flora Matéo
- Respect Zone
    - Laura-Blu Mauss
- SOS Racisme
    - Hermann Ebongue
    - Ester Mbikinkam
    - Alice Murgier
- Stop Homophobie
    - Terrence Katchadourian
- StopFisha
    - Shanley Clermot MacLaren
    - Rachel-Flore Pardo
- UFC-Que Choisir
    - Frithjof Michaelsen
- UNAF
    - Olivier Gérard
    - Stéphanie Puria
- CyberNeTic
    - Marlène Dulaurans
    - Jean-Christophe Fedherbe

Personnalités individuelles

- Agathe Auproux
- Léa Coffrant
- Elvire Duvelle-Charles
- Florence Hainaut
- Louise Leguen
- Lynadriel
- Nat_Ali
- Anissa Maille
- Marion Séclin