INSTITUT
MONTAIGNE

Internet :
le péril jeune ?

RAPPORT AVRIL 2020

Think tank indépendant créé en 2000, l'Institut Montaigne est une plateforme de réflexion, de propositions et d'expérimentations consacrée aux politiques publiques en France et en Europe. À travers ses publications et les événements qu'il organise, il souhaite jouer pleinement son rôle d'acteur du débat démocratique avec une approche transpartisane. Ses travaux sont le fruit d'une méthode d'analyse et de recherche rigoureuse et critique, ouverte sur les comparaisons internationales. Association à but non lucratif, l'Institut Montaigne réunit des chefs d'entreprise, des hauts fonctionnaires, des universitaires et des personnalités issues d'horizons divers. Ses financements sont exclusivement privés, aucune contribution n'excédant 1,5% d'un budget annuel de 6,5 millions d'euros.

INSTITUT
MONTAIGNE

Internet :
le péril jeune ?

RAPPORT – AVRIL 2020

Il n'est désir plus naturel
que le désir de connaissance

RÉSUMÉ

LES ENJEUX

En 20 ans, l'émergence du numérique, puis le développement des usages mobiles, ont considérablement transformé les pratiques de sociabilité, d'apprentissage et plus globalement le mode de vie des jeunes Français. Pourtant, ces pratiques et surtout leur impact sur cette catégorie de la population demeurent mal connus. De fait, les conduites propres à l'adolescence pour échapper au regard et au contrôle du monde adulte, renforcées par l'émergence incessante de nouveaux canaux et espaces virtuels de sociabilité, constituent des obstacles puissants à l'analyse.

La nécessité de mieux comprendre le rapport des jeunes à Internet, aux plateformes et aux réseaux sociaux apparaît d'autant plus forte dans la période actuelle où les mesures de confinement liées à la crise du Covid-19 impliquent une utilisation plus grande des outils numériques.

Dans le prolongement d'une étude conduite aux États-Unis par le *Pew Research Center*[1], l'Institut Montaigne a souhaité :

- **mieux connaître les pratiques numériques des jeunes de 11 à 20 ans et identifier les principaux risques auxquels ils sont confrontés ;**
- **proposer des réponses afin de sécuriser les pratiques numériques des jeunes en déterminant le rôle que peuvent jouer l'ensemble des parties prenantes.**

Pour disposer de données solides, l'Institut Montaigne, AXA Prévention et Dentsu Aegis Network ont réalisé une enquête d'opinion quantitative et qualitative auprès de 3000 jeunes âgés de 11 à 20 ans, de 1000 parents d'adolescents

1 Pew Research Center, *A Majority of Teens Have Experienced Some Form of Cyberbullying*, septembre 2018.

de 11 à 20 ans, ainsi que d'un échantillon de 1 000 personnes représentant la population générale. Cette enquête a permis de faire le point sur quatre enjeux majeurs : le cyberharcèlement, les contenus choquants, le rapport à la vérité et la protection de leur vie privée.

Dans le prolongement de l'enquête, un groupe de travail constitué d'experts pluridisciplinaires a formulé dix propositions pour répondre aux défis que soulèvent les pratiques numériques des jeunes Français.

Principaux messages

L'enquête révèle que les parents connaissent mal les pratiques numériques de leurs enfants et n'identifient généralement pas les principales zones de risque. Si les jeunes indiquent être conscients des risques potentiels et savoir y faire face, l'enquête souligne que **l'usage d'Internet et des réseaux sociaux constitue un apprentissage comme les autres** dont la spécificité est de concerner autant les jeunes que les adultes qui les entourent, autant les familles que les professeurs, autant les pouvoirs publics que les entreprises qui gèrent les plateformes et réseaux sociaux.

L'enquête met en évidence l'ampleur des phénomènes de violences auxquels les jeunes sont confrontés en ligne (35 % des jeunes interrogés ont déjà été confrontés à des formes de cyberviolences). Ces phénomènes touchent **en particulier les jeunes filles,** qui sont fréquemment exposées à des attaques sexistes. Ces pratiques sont souvent lancées et relayées par des jeunes qui connaissent la victime. Loin de se cantonner à la sphère numérique, elles connaissent des prolongements dans la « vie réelle ».

Face à ces phénomènes, quelles réponses apporter ?

- Face à l'ampleur que peut prendre le cyberharcèlement, notamment à cause de mécanismes de viralité, l'urgence est de **repenser la prise en charge des jeunes victimes.** Les dispositifs de signalement et d'écoute sont aujourd'hui segmentés. Nous proposons de créer une interface unique, facilement accessible à toute heure et connectée avec les acteurs éducatifs, les forces de sécurité, la justice et, le cas échéant, les acteurs sociaux.
- Plus globalement, **le numérique doit devenir une démarche d'apprentissage,** tout au long de laquelle les jeunes vont être accompagnés, guidés et protégés. Ce processus passe par une protection effective des jeunes en ligne et par un renforcement de l'enseignement de l'informatique comme de la formation à l'esprit critique tout au long de la scolarité.

Enfin, les grandes plateformes de réseaux sociaux sont devenues un espace public, fréquentées par tous, y compris les jeunes, et leur caractère fondamental et systématique implique une transparence accrue. Nous proposons **un système d'audit régulier des grandes plateformes fréquentées par les jeunes** afin de vérifier qu'elles appliquent effectivement les règlements en vigueur et évaluer, sous la forme de *stress tests*, les réponses des algorithmes à des situations de cyberharcèlement, de diffusion de contenus choquants voire illégaux ou de *fake news*, ainsi que de publication d'informations à caractère personnel.

SOMMAIRE

INTRODUCTION

Le numérique constitue une dimension majeure des sociétés contemporaines. Un basculement est en effet intervenu et la vie des jeunes générations s'inscrit désormais autant en ligne qu'hors ligne. 71 % des 15-34 ans utilisent les réseaux sociaux tous les jours ou presque. Les pratiques ont d'ailleurs évolué avec une diversification des supports et la montée en puissance considérable des usages mobiles depuis le début des années 2010[2]. Fin 2010, 91 % des 15-34 ans étaient « ordinautes » et 51 % « mobinautes ». Fin 2017, la proportion de mobinautes était passée à 90 % chez les 15-34 ans contre 86 % d'ordinautes. Si le mouvement est le même dans l'ensemble de la population, les jeunes gardent un temps d'avance (69 % de mobinautes dans la population générale).

Le contexte spécifique aux mesures de confinement liées à la crise du Covid-19 renforce encore la prépondérance du numérique dans la vie de la plupart des Français, et des jeunes en particulier. Déjà habitués à utiliser les outils numériques pour de nombreux cas d'usage et notamment pour échanger avec leurs amis en dehors de l'école, les jeunes sont amenés dans la période actuelle à ne pouvoir utiliser que ce canal, avec les risques qui y sont associés. De fait, s'il est encore trop tôt pour disposer d'une vision précise, la période de confinement semble s'accompagner d'un développement des cyberviolences. Ainsi, l'association e-Enfance note que le nombre d'appels liés à des cas de cyberharcèlement (revenge porn, chantage à la webcam, comptes fishas) reçus par le numéro NET ECOUTE a augmenté de 20 %, tandis que les signalements vers les plateformes numériques ont doublé, entraînant des suppressions de comptes sur SnapChat et Facebook[3].

L'évolution des usages et des pratiques a entraîné l'émergence de nouveaux risques, dont la prise de conscience est progressive : addiction aux écrans, cyberharcèlement, consultation sans filtre d'images choquantes et, plus

2 Ministère de la Culture, *Les jeunes et l'information*, Baromètre Médiamétrie, juillet 2018.
3 e-Enfance, *Enfants et adolescents : le confinement accroît les dangers d'Internet*, Communiqué de presse, 9 avril 2020.

largement, cyberviolences, diffusion généralisée de fausses nouvelles grâce aux réseaux sociaux, exposition de la vie privée, ciblage publicitaire.

C'est précisément à cette problématique que l'Institut Montaigne a souhaité apporter des éléments de réponse. Les jeunes Français de 11 à 20 ans sont-ils conscients des risques du numérique ? Disposent-ils d'une maîtrise des outils suffisante et d'un recul adapté pour déjouer les pièges et adopter en toutes circonstances une conduite numérique responsable ?

En partant d'une enquête menée par le Pew Research Center auprès des adolescents américains, l'Institut Montaigne a cherché à collecter des données précises sur les adolescents français, en examinant tout particulièrement quatre grandes dimensions :

- le cyberharcèlement et les cyberviolences ;
- la consultation de contenus choquants ;
- le rapport à la vérité en ligne ;
- la protection de la vie privée sur Internet.

Les résultats de l'enquête d'opinion conduite apparaissent proches de ceux obtenus aux États-Unis.

Synthèse de l'enquête du Pew Research Center

***A Majority of Teens Have Experienced Some Form of Cyberbullying* - Septembre 2018**

Méthodologie : l'enquête est composée d'entretiens auprès de 1 058 parents de jeunes âgés de 13 à 17 ans et auprès de 743 jeunes âgés de 13 à 17 ans, en ligne ainsi que par téléphone.

59 % des jeunes américains déclarent avoir déjà été harcelés ou intimidés en ligne et 63 % considèrent qu'il s'agit d'un problème grave pour des personnes de leur âge.

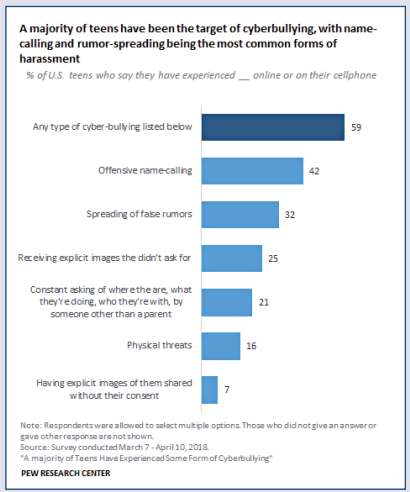
.../...

Une proportion équivalente de garçons et de filles ont subi ce phénomène mais les filles ont tendance à être victimes de rumeurs répandues à leur encontre en ligne (39 % contre 26 % pour les garçons) ou à recevoir des messages non désirés au contenu sexuellement explicite (29 % contre 20 % pour les garçons).

40 % des jeunes déclarent avoir été confrontés à au moins deux situations différentes caractérisant un harcèlement ou une intimidation en ligne. À cet égard aussi, les filles sont davantage ciblées puisque 15 % d'entre-elles disent avoir vécu au moins 4 des situations identifiées contre 6 % des garçons.

Dans le même temps, les jeunes pensent majoritairement que leurs parents appréhendent bien le cyberharcèlement (59 %) mais que leurs professeurs (58 %), les entreprises de réseaux sociaux (66 %) et les responsables politiques (79 %) ne parviennent pas à résoudre ce problème.

Environ 6 parents sur 10 craignent que leur enfant soit intimidé en ligne (59 %) ou échange des images à caractère sexuel (57 %) mais la plupart sont confiants dans leur capacité à apprendre à leur enfant comment bien se comporter en ligne (45 %).



Ces résultats, de même que les entretiens menés, font clairement apparaître que les risques existent mais que les adolescents apprennent progressivement à les appréhender et à adapter leur comportement en conséquence. En d'autres termes, le numérique est un apprentissage, comme les autres. C'est un processus qui suppose que chaque jeune soit protégé, guidé et accompagné.

La singularité de cet apprentissage réside dans le fait que la transmission intergénérationnelle n'est pas aisée. En effet, l'apparition du numérique demeure récente et des technologies comme des usages nouveaux apparaissent en permanence. Par conséquent, les adultes ne disposent pas nécessairement d'une antériorité et d'une expérience supérieure à celles des jeunes générations. Ils sont parfois démunis face au numérique et aux expériences numériques des jeunes, de leurs enfants. À ce titre, les adultes, les parents mais aussi les professeurs et les institutions se trouvent eux aussi en situation d'apprentissage face au numérique.

L'objectif de cette étude est précisément de déterminer comment protéger les plus jeunes et permettre un apprentissage progressif des codes et des règles d'une vie numérique sereine et sans risque. Pour cela, le groupe de travail réuni par l'Institut Montaigne a identifié les principaux enjeux et déterminé les politiques publiques à amender, renforcer, voire construire pour apporter des réponses aux défis que rencontrent les jeunes générations.

La réponse à apporter n'est cependant pas univoque. Elle est nécessairement multidimensionnelle puisque ces défis exigent une implication et une responsabilisation de chacun des acteurs, afin de tirer le meilleur du numérique :

- responsabilisation de ceux qui produisent des contenus en lignes (les éditeurs) ;
- responsabilisation des hébergeurs, et tout particulièrement des gestionnaires de plateformes, réseaux et sites fréquentés par les jeunes ;
- responsabilisation des « médiateurs », chargés de guider les jeunes vers l'âge adulte, qu'il s'agisse des professeurs, des éducateurs ou des parents ;
- responsabilisation des jeunes eux-mêmes, pour qu'ils acquièrent l'esprit critique et la « citoyenneté numérique » nécessaire à un usage serein et enrichissant de ce nouvel outil.

Dans cette démarche de responsabilisation, les pouvoirs publics peuvent s'appuyer sur des atouts solides, notamment sur la formation de l'esprit critique qui est au cœur de la tradition scolaire française. De plus, dans bien des domaines, des initiatives existent déjà. Il s'agit souvent de les approfondir et de les mettre en cohérence. D'autres dimensions dépassent le cadre national et appellent une action coordonnée au niveau européen.

Trois axes principaux structurent la démarche d'apprentissage et de responsabilisation nécessaire de la part de chacune des parties prenantes :

- **prévenir** les risques liés au numérique pour permettre aux jeunes d'être à même d'utiliser Internet et les réseaux sociaux de la manière la plus épanouissante tout en sachant identifier et faire face à ces risques, pour soi-même et pour les autres ;
- **accompagner** les jeunes pour traiter avec simplicité, rapidité et de la façon la plus adaptée les situations de cyberviolence et de cyberharcèlement que peuvent vivre les jeunes, avec le soutien de leurs proches et de leurs parents ;
- **responsabiliser** l'ensemble des acteurs pour que ceux-ci agissent avec vigilance et civisme, permettant ainsi à Internet et aux réseaux sociaux d'offrir plus d'opportunités que de menaces pour les jeunes.

Prévenir les risques liés au numérique, aux plateformes et aux réseaux sociaux

- Permettre aux jeunes de protéger leur **vie privée en ligne,** afin de limiter leur exposition à des risques en ligne, notamment les cyberviolences
- Former les jeunes à **développer leur esprit critique en ligne,** pour leur éviter d'être manipulés et de devenir relayeurs et complices

Accompagner rapidement et efficacement en cas de difficultés (en ligne)

- Permettre aux jeunes victimes de cyberviolences de bénéficier d'un **point de contact unique et identifié** pour être accompagnés
- Protéger effectivement les jeunes des contenus réservés aux majeurs et leur permettre de facilement **signaler des contenus choquants**

Responsabiliser les jeunes ainsi que les entreprises qui gèrent les réseaux sociaux

- S'assurer que chaque jeune sache qu'il a une responsabilité en ligne et qu'il doit **réparer les torts** qu'il peut causer à d'autres personnes en ligne
- Construire un cadre concret de responsabilité des plateformes pour qu'elles aident les jeunes à grandir en ligne

MÉTHODOLOGIE ET PRINCIPAUX ENSEIGNEMENTS DE L'ENQUÊTE D'OPINION

Une enquête a été réalisée en octobre 2019 par le cabinet Odoxa auprès de trois échantillons interrogés par Internet :

- 3005 jeunes âgés de 11 à 20 ans (quotas appliqués au sexe et à l'âge) ;
- 1002 parents de jeunes de 11 à 20 ans (quotas appliqués au sexe et à l'âge de l'enfant) ;
- 1001 Français, dans un échantillon représentatif de la population française âgée de 18 ans et plus. La représentativité est assurée par la méthode des quotas appliqués aux variables suivantes : sexe, âge, niveau de diplôme et profession de l'interviewé après stratification par région et catégorie d'agglomération.

Les résultats obtenus le sont avec un intervalle de confiance de 95%.

Celle-ci a été complétée par trois focus groupes de 2h réunissant 8 à 10 personnes réalisés à Paris :

- Un groupe de parents ayant des enfants de 7 à 20 ans ;
- Un groupe de jeunes filles de 15 à 18 ans ;
- Un groupe de jeunes garçons de 15 à 18 ans.

Plusieurs enseignements majeurs ont découlé de cette étude.

I. L'activité en ligne n'est pas distincte de la vie réelle pour une grande majorité des jeunes

- Seuls 20% des 11-20 ans affirment en effet que ce qu'ils font en ligne ne reste que virtuel ;

- 58% des 11-20 ans préfèrent en effet voir leurs amis plutôt que de discuter avec eux sur Internet (9%) ;
- 77% des 11-20 ans préfèrent exprimer un désaccord en face-à-face.

II. Les réseaux sociaux les plus utilisés par les jeunes sont Snapchat (68%) et Instagram (59%) qui devancent Facebook (43%)

- Avec 43% d'utilisateurs chez les jeunes interrogés, Facebook, réseau n° 1 des Français, est aujourd'hui devancé par Snapchat (68%) et Instagram (59%) chez les jeunes. Viennent ensuite Whatsapp (27%), Twitter (15%) et TikTok (11%).
- Les 11-14 ans citent en effet bien davantage TikTok (21%), que leurs aînés (3% chez les 18-20 ans). En revanche, ils se détournent bien plus de Facebook que leurs aînés (28% seulement sont sur Facebook contre 61% des 18-20 ans).
- En moyenne, les jeunes considèrent 47% de leurs contacts sur les réseaux sociaux comme des amis.

III. Le regard porté par les parents sur Internet varie en fonction de l'âge de leur enfant. Les jeunes sont quant à eux parfaitement conscients des risques du web

- Pour les parents, Internet est synonyme de danger quand leur enfant a moins de 15 ans (59%) et d'opportunité ensuite (60% pour les parents d'enfants de 15 à 17 ans, 72% de 18 à 20 ans).
- 79% des 11-20 ans se rendent plusieurs fois par semaine sur Internet pour un usage scolaire (cet usage s'accroît avec l'âge).
- Les jeunes utilisent essentiellement les moteurs de recherche (75%) pour leurs recherches scolaires.
- Harcèlement (97%), contenus choquants (89%) ou divulgations d'informations personnelles (93%) sont qualifiés de « graves » par les jeunes.

Le Focus groupe « Parents » a permis de relever que, pour les parents, Internet constituait une opportunité incontournable pour les enfants de s'informer, de trouver de l'aide pour leurs devoirs, de se sociabiliser, de s'amuser et de partager des scènes de vie. En revanche, les parents ont rappelé qu'Internet pouvait être source de beaucoup de dangers, d'où une vigilance nécessaire, en particulier s'agissant de risques d'addiction. Le Focus groupe « Parents » a également montré que les parents associaient spontanément le danger à l'inconnu plutôt qu'aux proches et qu'ils n'évoquaient pas du tout le cyberharcèlement.

Les Focus groupes « Jeunes » ont permis de souligner que les jeunes filles étaient très conscientes des risques d'Internet et des réseaux sociaux, exprimant spontanément des craintes assez fortes. Par contraste, les jeunes garçons paraissaient moins craintifs bien que très conscients des risques d'Internet et des réseaux sociaux.

IV. Pour les parents, l'usage d'Internet est devenu un processus d'apprentissage comme un autre, fait de libertés et de contraintes

- 31 % d'entre eux limitent les plages horaires d'accès à Internet (48 % chez les parents de 11-14 ans), 28 % contrôlent l'historique de navigation (45 % chez les parents de 11-14 ans) et 24 % ont mis en place un contrôle parental (40 % chez les parents de 11-14 ans) ;
- 72 % d'entre eux nous disent que leur enfant navigue principalement sur son propre smartphone (57 % chez les 11-14 ans).

V. Plus d'un jeune sur deux (56 %) dit avoir été victime de cyberviolences[4] au moins une fois et plus d'un sur trois (35 %) y a déjà été confronté à plusieurs reprises

- Dans le détail, un jeune sur cinq déclare par exemple qu'il lui est déjà arrivé plus d'une fois d'être « victime d'insultes » (18 %), ou de « recevoir des images intimes non demandées » (17 %).
- Plus d'un jeune sur dix a été à plusieurs reprises victime « de rumeurs » (13 %) et même de « menaces » (9 %) ; plus d'un jeune sur cinq a plusieurs fois vu « un groupe se créer contre lui » (6 %) ou que « des images intimes de lui soient mises en ligne sans son accord » (5 %).
- Près d'un jeune sur quatre (24 %) reconnaît avoir commis des cyberviolences.

Les Focus groupes « Jeunes » ont souligné que, parmi les cyberviolences, le cyberharcèlement pouvait rapidement évoquer un sentiment de peur morbide chez les jeunes filles (« détruire une vie », « dépression », « haine », « mort », « suicide ») et que les jeunes garçons se montraient aussi très craintifs (« intimidations », « chantage », « réputation », « suicide »).

4 niveaux de gravité des cyberviolences ont été identifiés :

- très grave : la mise en ligne de photos/vidéos intimes sans consentement qui peut avoir des conséquences dramatiques ;
- grave : être victime de menaces sur les réseaux sociaux, ce qui peut mettre une pression insupportable sur un jeune ;
- moyennement grave : être victime d'insultes ou de rumeurs répétées sur les réseaux sociaux car cela peut « pourrir la vie » d'un jeune ;
- peu grave : un groupe qui se crée contre un jeune ou recevoir des photos/vidéos pornographiques.

4 La notion de cyberviolence a été utilisée ici pour rendre de compte la diversité des situations de violence auxquelles les jeunes peuvent être confrontés en ligne. Au sein des cyberviolences l'étude examine tout particulièrement les formes de cyberharcèlement. Le cyberharcèlement, qui fait partie des cyberviolences, suppose à la fois une intention de nuire et la répétition des faits.

Un jeune choisit en outre un confident en fonction de la nature du harcèlement :

- dans le cas d'images intimes ou de rumeurs intimes, surtout pour les filles, les amis ou des proches seront privilégiés, en dehors des parents et des professeurs ;
- dans le cas de menaces, les parents sont privilégiés, tant qu'elles ne sont pas liées à l'intimité ;
- dans tous les autres cas, les amis proches sont privilégiés.

Ces résultats concordent avec ceux observés par le *Pew Research Center* aux États-Unis.

Comparaison des résultats aux États-Unis et en France

	Pew Research Center (avril 2018)	Institut Montaigne (octobre 2019)	
˝% of U.S. teens who say they have experienced_ online or on their cellphone˝			« Sur Internet, t'est-il déjà arrivé… »
Offensive name-calling	42 %	41 %	D'être victime d'insultes
Spreading or false rumors	32 %	29 %	D'être victime de rumeurs
Receiving explicit images you didn't ask for	25 %	31 %	De recevoir des images intimes (« nudes ») / pornographiques non demandées
Physical threats	16 %	21 %	D'être victime de menaces
Having explicit images of you shared whithout youy consent	7 %	11 %	Que soient mises en ligne des images intimes de toi sans ton accord

VI. Les parents ne savent pas vers quelle administration se tourner si leur enfant est victime de cyberharcèlement

- Les parents sont parfois démunis face aux actes de cyberharcèlement. La majorité d'entre eux (61 %) ne saurait d'ailleurs pas vers quelle administration se tourner si leur enfant était victime.

Le Focus groupe «Parents» a permis de réaliser que le cyberharcèlement constituait une vraie peur pour les parents, exprimée spontanément par des mots forts («peur», «meute», «honte», «racket»).

VII. Les jeunes sont presque aussi exposés aux contenus choquants que les Français dans leur ensemble

- Plus d'un jeune sur deux a déjà accédé à un contenu choquant (56%). Si l'on met de côté les réponses «non, rarement», cela représente un niveau toujours élevé de 39% de jeunes ayant été exposés à plusieurs reprises à ce type de contenus.
- 30% des 11-20 ans déclarent avoir déjà accédé à des contenus violents, c'est-à-dire autant que les Français pris dans leur ensemble. 17% des jeunes ont déjà été exposés à des contenus racistes, antisémites ou homophobes (contre 19% observés sur la moyenne nationale).
- Ils sont en revanche davantage confrontés aux contenus incitant à se livrer à des jeux dangereux (14% contre 9% des Français).
- Les jeunes de 11-20 ans sont 11% à avoir au moins une fois été confrontés à des contenus incitant à commettre des actes terroristes ou les justifiant; ils sont 3% à y avoir été confrontés plusieurs fois, contre 6% des Français.
- Les jeunes âgés de 11 à 20 ans sont en revanche nettement moins nombreux à dire qu'il ont consulté des contenus pornographiques (21%) que l'ensemble des Français (45%).

VIII. Les parents sous-estiment légèrement l'accès de leurs enfants aux contenus choquants

- 40% des parents pensent que leur enfant a déjà été exposé à des contenus violents alors que 47% des jeunes déclarent l'avoir été au moins une fois.
- Ils sont 28% à le penser à propos des contenus pornographiques (contre 36% des jeunes qui déclarent l'avoir été au moins une fois), 21% pour les contenus racistes, antisémites ou homophobes (contre 31% des jeunes qui déclarent l'avoir été au moins une fois), 19% s'agissant des contenus incitant à se livrer à des jeux dangereux (contre 30% des jeunes qui déclarent l'avoir été au moins une fois) et enfin 4% des parents pensent que leur enfant a déjà été confronté à des contenus incitant ou justifiant des actes terroristes (contre 11% des jeunes qui déclarent l'avoir été au moins une fois).

IX. Les jeunes n'échappent pas aux *fake news* mais considèrent être globalement sensibilisés et vigilants

- 74% d'entre eux affirment qu'ils se sont souvent ou parfois rendu compte qu'ils avaient consulté des informations s'étant révélées fausses.
- Lorsqu'ils souhaitent apprendre de nouvelles choses sur un sujet, ils se tournent en premier lieu vers leurs parents (51%), notamment lorsqu'ils ont moins de 15 ans (70%). Les sites web constituent leur deuxième source d'information (39%), c'est même la première chez les 18-20 ans (55%).
- YouTube et les réseaux sociaux arrivent aux deux dernières positions des sources consultées pour apprendre de nouvelles choses. 20% des jeunes citent en effet YouTube et seulement 15% les réseaux sociaux.
- 83% des 11-20 ans et 82% des Français jugent en effet que le phénomène des *fake news* devrait être encadré par la loi. Ils sont respectivement 73% et 79% à considérer que les *fake news* représentent un grave problème pour la démocratie et 57% et 65% à juger que c'est un problème qui ne peut pas être résolu facilement.

X. Les jeunes sont encore plus soucieux de la protection de leur vie privée en ligne que leurs aînés même s'ils rejettent moins le marketing personnalisé

- 94% des jeunes âgés de 11 à 20 ans affirment que protéger leur vie privée en ligne est pour eux un sujet important (88% chez les adultes).
- Question technique, les jeunes estiment être plutôt bien informés, surtout lorsqu'ils avancent dans l'âge. 63% des 11-20 ans déclarent connaître les moyens de protéger leur vie privée sur Internet (74% des 18-20 ans) et 54% d'entre eux ont déjà utilisé des outils pour limiter leurs traces sur le web (70% des 18-20 ans).
- 52% des 11-20 ans pensent qu'il est bien d'utiliser les informations sur leur âge, leurs goûts ou l'endroit où ils habitent pour leur proposer des produits qui leur plairont.

Les Focus groupes «jeunes» ont permis de souligner que les jeunes, en grande majorité, estimaient très bien connaître les fonctionnalités des réseaux sociaux qu'ils utilisent, et que leurs attitudes et la prudence variaient selon le réseau social utilisé : ils n'hésitent pas à ajouter des amis sur Snapchat, estimant que les contenus disparaissent rapidement ; ils sont davantage prudents sur Instagram où ils privilégient les «vrais amis» ; enfin, ils considèrent que Facebook est un réseau social «pour les vieux» et ne le voient pas comme une vraie communauté d'amis.

XI. S'agissant de l'apprentissage d'Internet, les parents expriment une forte défiance (66 %) à l'égard de l'Éducation nationale alors que les jeunes apprécient massivement la formation de leurs professeurs (67 %)

- 77 % des parents estiment qu'ils aident leur enfant à naviguer sur Internet sans prendre de risques ;
- 66 % d'entre eux considèrent que l'Éducation nationale ne forme pas leur enfant à naviguer sur Internet sans prendre de risques ;
- Les jeunes battent cette idée en brèche : ils apprécient les explications données par leurs professeurs. 67 % les ont jugées bonnes ;
- 64 % des jeunes de 11-20 ans et 77 % de leurs parents déclarent ne pas faire confiance à l'État pour protéger la vie privée. Ils font encore moins confiance aux entreprises qui gèrent les réseaux sociaux (79 % et 85 %).

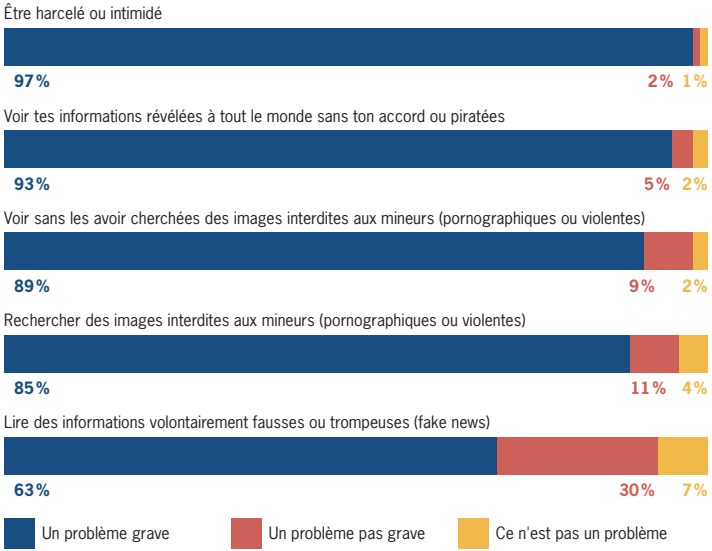
Les Focus groupes ont permis d'identifier plusieurs attitudes des parents pour garantir la sécurité de leurs enfants sur Internet, de la surveillance voire l'interdiction à des pratiques plus permissives. Toutefois, le constat est que les jeunes arrivent toujours plus ou moins à déjouer le contrôle parental.

I. PRÉVENIR LES RISQUES LIÉS AU NUMÉRIQUE, AUX PLATEFORMES ET AUX RÉSEAUX SOCIAUX

I.A. PRÉVENIR : PERMETTRE AUX JEUNES DE PROTÉGER LEUR VIE PRIVÉE EN LIGNE

Savoir comment protéger sa vie privée en ligne constitue le moyen préventif le plus sûr pour limiter au maximum les risques auxquels on peut être confronté sur Internet et sur les réseaux sociaux, en particulier ce qu'on identifie sous le terme de «cyberviolences» (partie II). L'enquête d'opinion réalisée pour le compte de l'Institut Montaigne, Axa Prévention et Dentsu Aegis Network a en effet permis de souligner que les situations considérées par la quasi-totalité des jeunes comme présentant un caractère grave sont souvent liées à la circulation de données à caractère personnel, notamment les images intimes. Les cas de harcèlement et d'intimidation mais aussi, de façon plus générale, la diffusion d'informations personnelles et même intimes peuvent donc être accentués, et même parfois permis, quand la victime n'est pas suffisamment formée à protéger ses données personnelles.

Appréciation par les jeunes de la gravité de certaines situations en ligne



Former et être formé à une navigation prudente constitue donc la première des protections face aux risques et menaces qui peuvent survenir sur Internet et les réseaux sociaux.

1. Protéger sa vie privée en ligne est devenu une priorité pour chacun d'entre nous, et encore davantage pour les jeunes

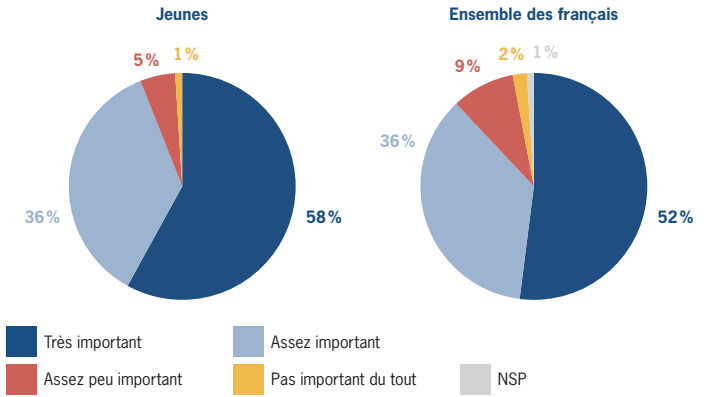
Plusieurs études d'opinion récentes réalisées par l'IFOP pour le compte de la CNIL révèlent que la protection des données personnelles est devenue une véritable préoccupation en France. Ainsi, fin octobre 2018[5], deux tiers des

5 CNIL, Les Français et la protection des données personnelles, Sondage Ifop, Novembre 2018.

Français se déclaraient plus sensibles qu'auparavant à la protection des données, leur prise de conscience s'expliquant en raison des cas nombreux de piratage, de vol de données, notamment en cas de failles de sécurité, ainsi que de la multiplication des sollicitations commerciales sous la forme de spam.

Les jeunes interrogés dans le cadre de l'enquête réalisée pour l'Institut Montaigne, Dentsu Aegis Network et Axa prévention apparaissent encore plus sensibles à cet enjeu que le reste de la population française puisque 94 % d'entre eux considèrent qu'il est assez important voire très important de protéger sa vie privée en ligne (contre 88 % pour l'ensemble de la population)[6]. Plusieurs des interlocuteurs rencontrés ont par ailleurs confirmé l'enjeu essentiel que constitue désormais l'apprentissage par les jeunes, mais aussi par les moins jeunes, des moyens effectifs de protéger leur vie privée en ligne : une telle vigilance de chacun d'entre nous est la seule manière de réduire le plus possible les risques et de rendre les actions curatives plus efficaces lorsqu'il est nécessaire d'y recourir.

Évaluation de l'importance de protéger sa vie privée en ligne



6 Les jeunes n'appréhendent toutefois pas leur vie privée de la même manière que le reste de la population : ils sont en effet 52 % à penser qu'il est bien d'utiliser des informations sur leur âge, leurs goûts ou l'endroit où ils habitent pour leur proposer des produits qui leur plairont.

2. Le règlement général sur la protection des données (RGPD) prévoit plusieurs droits à cet effet mais ne décline pas les moyens concrets pour les mettre en œuvre

Le règlement général sur la protection des données, ou RGPD, encadre le traitement des données personnelles sur le territoire de l'Union européenne. Il s'inscrit dans la continuité de la loi française « Informatique et Libertés » de 1978 et renforce le contrôle par les citoyens de l'utilisation qui peut être faite des données les concernant. L'approche retenue est large s'agissant :

- des données concernées par cette protection, une donnée personnelle se définissant comme « toute information se rapportant à une personne physique identifiée ou identifiable » (article 4.1). Il peut donc s'agir de ses données d'état civil (nom, prénoms, date de naissance, etc.) mais aussi d'informations inhérentes à chaque personne (caractéristiques physiques, génétiques, culturelles, etc.);
- du traitement de données réalisé, celui-ci comprenant un large ensemble d'opérations, c'est-à-dire notamment de collecte, d'enregistrement, de conservation et de diffusion de données à caractère personnel (article 4.2);
- des organismes soumis aux obligations du RGPD puisque celles-ci concernent tous les organismes indépendamment de leur taille, de leur pays d'implantation et de leur activité, publics comme privés, agissant ou non pour le propre compte ou le compte d'un tiers, dès lors que sont concernés directement les données personnelles des résidents européens ou dès lors que les activités de traitement de ces organismes sont sur le territoire européen (article 3)[8].

Le RGPD confère plusieurs droits aux personnes dont les données personnelles font l'objet d'un traitement, ce qui permet, en théorie, de leur permettre de protéger leur vie privée. Il s'agit notamment du droit d'accéder aux données traitées et de comprendre à qui et à quoi elles sont destinées (article 15), du droit de demander que les données qui nous concernent soient corrigées si elles sont fausses (article 16) ou qu'elles soient effacées (article 17). Il peut aussi s'agir du droit de s'opposer à ce que les données personnelles soient utilisées par le traitement (article 21). Toutefois, le RGPD demeure un texte de niveau général : même les personnes qui connaissent son existence voire les droits qu'il garantit ne connaissent pas pour autant les dispositifs concrets permettant d'exercer effectivement ces droits. C'est ce que l'Institut Montaigne soulignait dans son rapport *Données personnelles : comment gagner la bataille*.

8 Les règles du RGPD sont particulièrement strictes dans certains champs. Dans le domaine de la santé, un principe d'interdiction de collecte et de traitement des données est prévu et il est assorti d'exceptions (consentement de la personne concernée, finalité de diagnostic ou de prise en charge, recherche médicale). Dans le champ de la sécurité publique et pénal, une directive spécifique (n° 2016/680) complète les dispositions du RGPD s'agissant des traitements de données à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces.

Le droit au déréférencement et le droit à l'oubli en droit européen

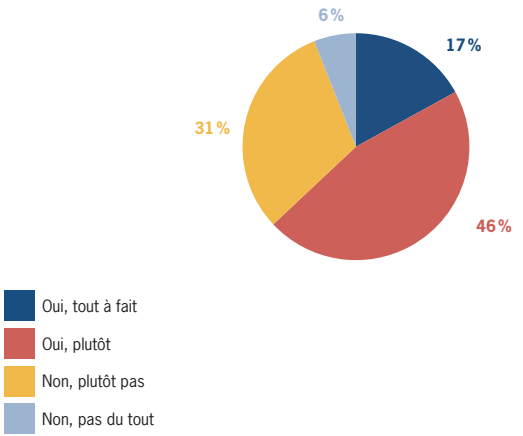
Sous l'empire de la directive 95/46 qui a précédé l'entrée en vigueur du règlement général à la protection des données (RGPD) la Cour de Justice de l'Union européenne a consacré un droit au déréférencement dans un arrêt Google Spain c/ Costeja du 13 mai 2014. Par conséquent, obligation est faite à un moteur de recherche de supprimer de la liste des résultats affichée à la suite d'une recherche nominative les liens vers les pages web contenant des informations relatives à la personne dont le nom est recherché, même si la publication de ces informations est licite. Cette obligation est néanmoins limitée aux versions européennes des moteurs de recherche.

Par ailleurs, l'article 17 du RGPD consacre un droit à l'effacement des données personnelles, poursuivant la logique suivie par la CJUE. Toute personne concernée par un traitement de données peut obtenir auprès du responsable de ce traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant lorsque ces données ne sont plus nécessaires au regard des finalités du traitement, lorsqu'elle décide de retirer son consentement ou de s'opposer au traitement, en cas de traitement illicite, si une obligation légale l'impose ou enfin lorsque les données ont été collectées dans le cadre de l'offre de services de la société de l'information.

Le bilan dressé par la CNIL en mai 2019, soit un an après l'entrée en vigueur du RGPD, montre qu'une appropriation du RGPD est en cours. Ainsi, sur la période de mai 2018 à mai 2019, la CNIL a constaté une augmentation de 30 % des plaintes pour violation des dispositions du règlement, soit un total de 11 900 plaintes en France. Cette prise de conscience est générale au niveau de l'Union européenne où près de 145 000 plaintes ont été recensées sur la même période.

Le sondage réalisé auprès des jeunes de 11 à 20 ans dans le cadre du présent rapport indique que ceux-ci sont plus de 60 % à estimer connaître les moyens de se protéger en ligne. Toutefois, de l'avis de plusieurs des interlocuteurs rencontrés, cette appréciation doit être nuancée car les jeunes ont souvent tendance à surestimer leur degré de maîtrise des risques en général et sur Internet en particulier.

Connaissance par les jeunes des moyens de protéger leur vie privée en ligne



3. Plusieurs initiatives ont été prises par les plateformes pour renforcer la vie privée en ligne, sans que cela soit totalement suffisant ni surtout adapté aux plus jeunes utilisateurs

Il est certain que, depuis une période relativement récente, les plus grandes plateformes en ligne s'engagent de plus en plus pour permettre à leurs utilisateurs d'avoir davantage de maîtrise sur leurs données personnelles. Ce mouvement peut s'expliquer comme une réponse aux actions plus coercitives des régulateurs, en Europe comme aux États-Unis - la dernière partie du rapport aborde ainsi la responsabilité des plateformes.

Facebook a renforcé depuis l'été 2019 les outils de contrôle de ses utilisateurs, notamment s'agissant des données obtenues auprès de tiers et en matière de reconnaissance faciale. Google, pour sa part, a prévu des dispositifs de suppression automatique de certains types de données après une période définie.

Outils de contrôle des données personnelles de Facebook et de Google

Facebook a agi sur deux terrains pour renforcer les pouvoirs de ses utilisateurs :

- **Une nouvelle fonctionnalité permet de contrôler les données obtenues en dehors du réseau social depuis août 2019.** En pratique, les utilisateurs peuvent décider si les données que récupère Facebook auprès des applications ou des sites Internet tiers qu'ils consultent peuvent être ou non liées à leur compte Facebook. Si l'utilisateur refuse l'association, Facebook continue de recevoir les informations, mais sous un format anonymisé afin de pouvoir établir des statistiques sur les interactions publicitaires ;
- **La fonction de reconnaissance faciale de Facebook a été mise à jour en septembre 2019 afin d'être désactivée par défaut.**

.../...

Par conséquent, les utilisateurs qui souhaitent utiliser cette fonctionnalité doivent l'activer pour être identifiés dans les photos postées sur le réseau social, ce qui constitue une inversion du principe et de l'exception.

Google permet depuis mai 2019 la suppression automatique après une période définie de certains types de données d'un compte Google, c'est-à-dire celles concernant les activités de l'utilisateur sur Internet et les applications qu'il utilise. En outre, Google a publié en open source un outil permettant aux développeurs de traiter de vastes quantités de données tout en anonymisant les données se rattachant à l'identité de l'utilisateur (principe de « confidentialité différentielle »).

Il est toutefois évident que ces initiatives, qui doivent être saluées, surtout si elles aboutissent à des améliorations réelles pour les utilisateurs, n'apparaissent pas suffisantes. En effet, alors qu'en théorie un utilisateur devrait pouvoir choisir les données personnelles qu'il autorise les plateformes à utiliser, c'est en réalité l'inverse qui s'observe, les plateformes disposant de nombreuses données personnelles pour lequel un consentement clair n'a en réalité pas été donné au départ.

S'agissant plus spécifiquement des enfants, ceux-ci sont considérés par le RGPD comme des « personnes vulnérables ».

Des exigences renforcées existent :

- **Le consentement du mineur au traitement de ses données personnelles doit être éclairé.** L'article 8 du règlement détermine de ce fait des conditions particulières en ce qui concerne le consentement des mineurs sur Internet, distinguant selon qu'ils ont plus ou moins de 16 ans, cet âge pouvant être modifié par les dispositions nationales – 15 ans en France[9] : ainsi, le

9 Article 7-1, *Loi Informatique et Libertés* telle que modifiée par l'ordonnance n° 2018-1125, 12 décembre 2018.

mineur de moins de 15 ans a besoin d'une autorisation parentale pour que son consentement soit valable. Toutefois, les dispositifs en place présentent un caractère exclusivement déclaratif qui limite la portée de cet article et permet aux jeunes de contourner les éventuelles interdictions ;

- **Le principe de transparence sur le traitement est renforcé lorsque celui-ci concerne un mineur.** Le considérant 58 indique que « les enfants méritant une protection spécifique, toute information et communication, lorsque le traitement les concerne, devraient être rédigées en des termes clairs et simples que l'enfant peut aisément comprendre », il est repris à l'article 12 ;
- **Une présomption de justification permet d'invoquer le droit à l'oubli.** Ce droit est le même pour les mineurs que pour les majeurs (article 17 du RGPD) mais il est renforcé en France : aux termes de l'article 51 de la Loi Informatique et Libertés, « *sur demande de la personne concernée, le responsable du traitement est tenu d'effacer dans les meilleurs délais les données à caractère personnel qui ont été collectées dans le cadre de l'offre de services de la société de l'information lorsque la personne concernée était mineure au moment de la collecte* ».

Dispositions du RGPD spécifiques aux jeunes

Considérant 38

Les enfants méritent une protection spécifique en ce qui concerne leurs données à caractère personnel parce qu'ils peuvent être moins conscients des risques, des conséquences et des garanties concernées et de leurs droits liés au traitement des données à caractère personnel. Cette protection spécifique devrait, notamment, s'appliquer à l'utilisation de données à caractère personnel relatives aux enfants à des fins de marketing ou de création de profils de personnalité ou d'utilisateur et à la collecte de données à caractère personnel relatives aux enfants lors de l'utilisation de services proposés directement à un enfant. Le consentement du titulaire de la responsabilité parentale ne devrait pas être nécessaire dans le cadre de services de prévention ou de conseil proposés directement à un enfant.

.../...

Considérant 58

Le principe de transparence exige que toute information adressée au public ou à la personne concernée soit concise, aisément accessible et facile à comprendre, et formulée en des termes clairs et simples et, en outre, lorsqu'il y a lieu, illustrée à l'aide d'éléments visuels. Ces informations pourraient être fournies sous forme électronique, par exemple via un site Internet lorsqu'elles s'adressent au public. Ceci vaut tout particulièrement dans des situations où la multiplication des acteurs et la complexité des technologies utilisées font en sorte qu'il est difficile pour la personne concernée de savoir et de comprendre si des données à caractère personnel la concernant sont collectées, par qui et à quelle fin, comme dans le cas de la publicité en ligne. **Les enfants méritant une protection spécifique, toute information et communication, lorsque le traitement les concerne, devraient être rédigées en des termes clairs et simples que l'enfant peut aisément comprendre.**

Considérant 75

Des risques pour les droits et libertés des personnes physiques, dont le degré de probabilité et de gravité varie, peuvent résulter du traitement de données à caractère personnel qui est susceptible d'entraîner des dommages physiques, matériels ou un préjudice moral, en particulier : lorsque le traitement peut donner lieu à une discrimination, à un vol ou une usurpation d'identité, à une perte financière, à une atteinte à la réputation, à une perte de confidentialité de données protégées par le secret professionnel, à un renversement non autorisé du processus de pseudonymisation ou à tout autre dommage économique ou social important ; lorsque les personnes concernées pourraient être privées de leurs droits et libertés ou empêchées d'exercer le contrôle sur leurs données à caractère personnel ; lorsque le traitement concerne des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, la religion ou les convictions philosophiques, l'appartenance syndicale, ainsi que des données génétiques, des données concernant la santé ou des données

.../...

concernant la vie sexuelle ou des données relatives à des condamnations pénales et à des infractions, ou encore à des mesures de sûreté connexes ; lorsque des aspects personnels sont évalués, notamment dans le cadre de l'analyse ou de la prédiction d'éléments concernant le rendement au travail, la situation économique, la santé, les préférences ou centres d'intérêt personnels, la fiabilité ou le comportement, la localisation ou les déplacements, en vue de créer ou d'utiliser des profils individuels ; **lorsque le traitement porte sur des données à caractère personnel relatives à des personnes physiques vulnérables, en particulier les enfants ;** ou lorsque le traitement porte sur un volume important de données à caractère personnel et touche un nombre important de personnes concernées.

Article 8 - Conditions applicables au consentement des enfants en ce qui concerne les services de la société de l'information

1. Lorsque l'article 6, paragraphe 1, point a), s'applique, en ce qui concerne l'offre directe de services de la société de l'information aux enfants, le traitement des données à caractère personnel relatives à un enfant est licite lorsque l'enfant est âgé d'au moins 16 ans. Lorsque l'enfant est âgé de moins de 16 ans, ce traitement n'est licite que si, et dans la mesure où, le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant.
2. Les États membres peuvent prévoir par la loi un âge inférieur pour ces finalités pour autant que cet âge inférieur ne soit pas en-dessous de 13 ans.
3. Le responsable du traitement s'efforce raisonnablement de vérifier, en pareil cas, que le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant, compte tenu des moyens technologiques disponibles.
4. Le paragraphe 1 ne porte pas atteinte au droit général des contrats des États membres, notamment aux règles concernant la validité, la formation ou les effets d'un contrat à l'égard d'un enfant.

L'analyse des politiques de recueil, d'utilisation et de confidentialité des données personnelles des grandes plateformes révèle toutefois **qu'il n'y a pas de réelle prise en compte de ces droits renforcés pour les utilisateurs mineurs.**

Extraits des consignes en matière de confidentialité et politique de protection de l'identité sur YouTube

Les consignes concernent *« tous les utilisateurs, quel que soit leur pays. Par conséquent, même si la vidéo respecte les lois relatives à la vie privée en vigueur dans [le pays de l'utilisateur], elle peut porter atteinte aux consignes YouTube en la matière »*. Il n'existe pas de consigne spécifique pour les plus jeunes.

Une procédure de réclamation pour atteinte à la vie privée est prévue. Pour qu'un contenu soit retiré du site, il faut qu'une personne soit identifiable personnellement par son image, sa voix, son nom, son numéro de carte d'identité, son numéro de compte bancaire, ses coordonnées ou d'autres informations personnelles. YouTube précise prendre également en compte l'intérêt pour le public, l'intérêt médiatique et l'autorisation des personnes impliquées et rappelle que la décision finale de savoir si le contenu porte atteinte ou non aux consignes en matière de confidentialité du site lui appartient.

Les réclamations doivent émaner des personnes concernées sauf exceptions (si elle ne dispose d'aucun ordinateur, si elle est vulnérable, si la réclamation est déposée par le parent ou le tuteur légal ou par le représentant légal).

- Contrairement à ce que prévoit le RGPD, le consentement éclairé du mineur ne fait pas l'objet d'une mention explicite dans les règles d'utilisation et il n'est pas non plus prévu une rédaction simplifiée des règles d'utilisation pour les rendre accessibles à un public mineur . Par conséquent, les règles internes de YouTube semblent prévaloir sur les dispositions légales auxquelles il n'est fait ni référence ni application.

Proposition 1 : garantir la pleine protection des données à caractère personnel des jeunes, tenant compte de leur vulnérabilité spécifique

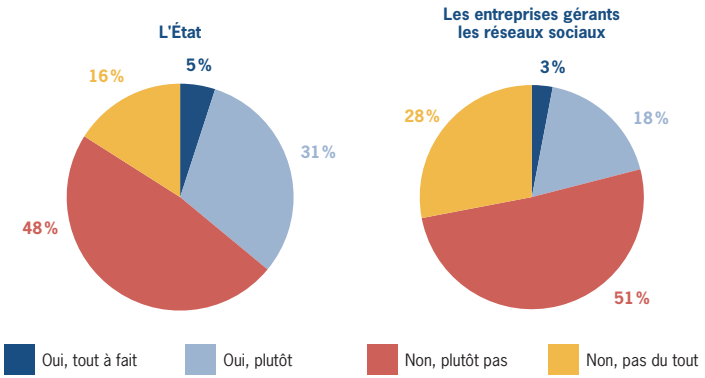
Cette garantie trouverait à se décliner à trois égards, en :

- **intégrant les dispositions du RGPD ouvrant des droits aux utilisateurs** au sein des règles posées par les plateformes quant aux conditions de recueil et d'utilisation des données à caractère personnel de leurs utilisateurs. L'objectif serait d'assurer la pleine prééminence des règles posées par le RGPD sur les règles internes des différents sites Internet et plateformes, les secondes devant se conformer aux premières et non l'inverse. Il serait également nécessaire que les termes recevant une qualification législative précise reçoivent une définition identique dans les règles internes d'utilisation des sites Internet et plateformes ;
- **adaptant les règles de consentement ainsi que de recueil et d'utilisation des données** à caractère personnel aux personnes se trouvant en situation de minorité légale et bénéficiant d'une protection renforcée au titre des personnes vulnérables, via l'édiction de guides ou de lignes directrices de la CNIL, voire du Comité européen de la protection des données (CEPD), qui viennent traduire opérationnellement les mesures spécifiques du RGPD consacrées aux mineurs. De la sorte, la minorité des utilisateurs dès la création de leur compte sera pleinement prise en compte afin de permettre aux jeunes de disposer d'une véritable maîtrise sur leurs données à caractère personnel ;
- **renforçant la responsabilité pécuniaire des sites Internet ou plateformes** en cas d'absence de protection ou de protection insuffisante des données personnelles de mineurs (cf. partie III).

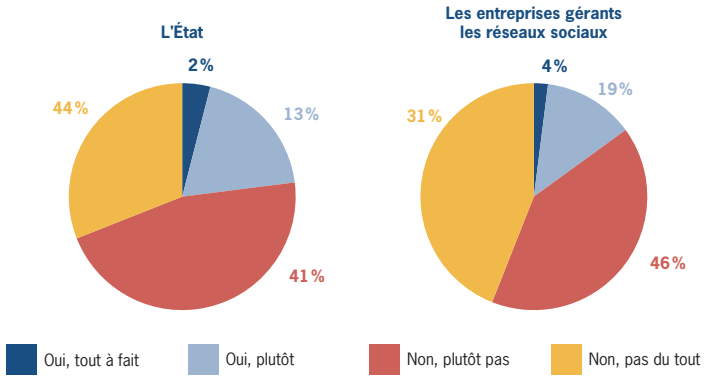
4. L'éducation constitue la principale réponse pour offrir à tous les jeunes les moyens de protéger leur vie privée en ligne

Si les mesures prises par les régulateurs et les plateformes constituent une amorce et plutôt un préalable, elles ne sont pas perçues comme les plus nécessaires ni les plus crédibles pour protéger la vie privée des jeunes en ligne. Dans le cadre de l'étude d'opinion conduite pour établir le présent rapport, les jeunes comme les parents ont fait part d'avis concordants quoique plus prononcés chez les parents : 64 % des jeunes et 85 % des parents ne font pas confiance à l'État ; ils sont respectivement 79 % et 77 % à ne pas faire confiance aux entreprises qui gèrent les réseaux sociaux.

Confiance accordée par les jeunes à…
pour protéger leur vie privée en ligne



Confiance accordée par les parents à…
pour protéger la vie privée de ceux-ci en ligne

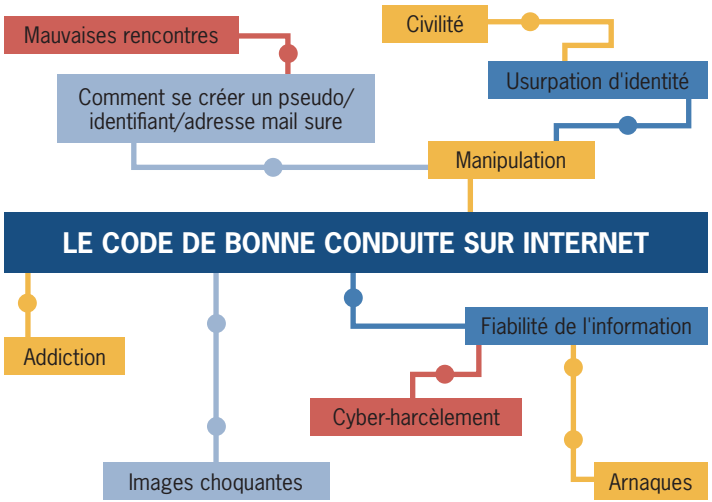


Cette appréciation est corroborée par la réponse formulée par l'ensemble des Français : 79 % d'entre eux ont estimé se faire confiance à eux-mêmes en premier lieu pour protéger leur vie privée en ligne, contre 11 % aux réseaux, sites et plateformes numériques et 9 % à l'État. Ce constat souligne la nécessité de former chaque jeune, afin de lui donner les outils pour protéger sa vie privée, prendre les précautions pour limiter ses traces en ligne et ainsi réduire les risques auxquels il s'expose. L'Éducation nationale mène dès à présent des actions pour permettre aux élèves de ne pas seulement être des consommateurs d'outils et de services numériques, mais encore des acteurs conscients, éclairés et prudents. La protection des données personnelles des jeunes fréquentant les établissements scolaires est ainsi garantie par l'utilisation du référentiel CNIL « Protection des données personnelles » dans les programmes d'enseignement.

Plus largement, l'Éducation nationale a cherché depuis plusieurs années à **renforcer l'usage des technologies de l'information et de la communication pour l'éducation (TICE) et l'éducation au numérique.** Il est clair que ces évolutions apparaissent tout à fait nécessaires pour contribuer à former les

jeunes à un usage raisonné et informé du numérique, ainsi que leurs professeurs. Désormais, une certification du niveau de maîtrise des compétences numériques est délivrée à tous les élèves à la fin du collège et à la fin du lycée. Elle repose sur l'évaluation des compétences attendues dans les cinq domaines d'activité qui forment le cadre de référence des compétences numériques : information et données, communication et collaboration, création de contenus, protection et sécurité, environnement numérique.

Certains dispositifs complémentaires associent pouvoirs publics et acteurs de la société civile. C'est le cas du « Permis Internet pour les enfants » qui est un programme national de prévention pour un usage d'Internet vigilant, sûr et responsable à destination des enfants en classe de CM2 et de leurs parents. L'initiative part du principe qu'avant de laisser un jeune utiliser Internet seul, il est indispensable de s'assurer qu'il a assimilé les règles élémentaires de vigilance, de civilité, et de responsabilité sur Internet ; à l'image de ce qu'il est nécessaire de lui apprendre avant d'apprendre à conduire.



Détail du « Permis Internet pour les enfants »

Plusieurs règles de prudence sont rappelées dans ce Permis : choix du mot de passe ou de l'adresse mail, rencontres virtuelles, achats en ligne, cyberharcèlement, respect de la vie privée, etc. Les risques sur Internet sont facilement évitables si les jeunes sont suffisamment informés et avertis.

La Gendarmerie nationale, la Police nationale, la Préfecture de Police et l'association AXA Prévention unissent leurs forces et leurs expertises en matière de protection et de prévention contre les risques sur Internet pour mener ensemble ce programme pédagogique. Le Permis Internet est Lauréat du Prix Prévention de la Délinquance 2015, remis par le Comité Interministériel de Prévention de la Délinquance et le Forum Français pour la Sécurité Urbaine. Le Permis Internet est proposé aux enseignants par les forces de gendarmerie et de police dans le cadre de leurs actions habituelles de prévention en milieu scolaire. Il peut être aussi mis en place à l'initiative des maires dans le cadre du temps périscolaire par les forces de police municipale. Deux millions d'enfants ont été sensibilisés dans ce cadre.

D'autres actions sont menées par des médias, organismes publics ou associations, à l'image de la série « la famille Tout écran », créée par la caisse nationale d'allocations familiales en partenariat avec le Clemi et diffusée par France Télévisions. Au fil des épisodes, la série entend proposer des réponses simples à des situations que rencontrent les familles dans la vie quotidienne (fausses nouvelles, images pornographiques, règles d'usage des écrans…).

Le sondage mené à l'occasion de cette étude fait apparaître un regard contrasté sur l'action de l'Éducation nationale pour former les jeunes à se protéger et à protéger leur vie privée en ligne : 67 % des jeunes estiment que leurs professeurs leurs ont donné de bonnes explications pour naviguer sans danger sur

Internet (les explications des parents sont jugées bonnes à 89 %). A l'inverse, 66 % des parents estiment que l'Éducation nationale ne forme pas leurs enfant à naviguer sur Internet sans prendre de risques.

Parallèlement aux actions déjà entreprises en matière d'utilisation du numérique comme un outil au service des apprentissages (tableau numérique interactif – TNI, serious game, aide aux devoirs, etc.) ou de formation centrée sur les usages (savoir se servir d'un ordinateur, d'un logiciel, naviguer en toute sécurité), le volet « informatique » pourrait être encore consolidé. En effet, un biais important consiste généralement à croire que les plus jeunes, ceux qui ont connu Internet et les réseaux sociaux dès leur plus jeune âge, en connaissent le fonctionnement et sont donc les mieux à même de se protéger en ligne. Cette approche est désormais démentie, les *« digital natives »* pouvant être, en même temps, des *« digital naives »*[10].

Un interlocuteur du monde de la recherche en informatique a ainsi insisté sur le besoin d'acculturer les jeunes aux fondamentaux de l'informatique pour quitter une forme de « naïveté », souvent occultée derrière leur relative aisance à utiliser les outils numériques[11]. Comment comprendre ce que signifie protection des données personnelles, si on ne fait pas la différence entre un contenu sur une ordinateur ou un téléphone et un contenu sur le cloud ou un réseau social ? Savoir qu'il est très difficile, voire impossible, de garantir la suppression complète d'un fichier mis en ligne suppose une maîtrise des fondamentaux de l'informatique qui demeure encore largement perfectible chez les jeunes. De manière générale, comprendre le fonctionnement concret des systèmes et la manière dont les données sont captées, circulent et sont utilisées constituent en effet des bases importantes pour assurer un usage responsable du numérique.

Derrière les usages, il est nécessaire que les jeunes aient conscience qu'Internet et les réseaux sociaux ne sont pas des espaces neutres mais que s'y déploient

10 Plantard, Pascal et Le Boucher, Caroline, « Les Digital Natives… Ils sont encore là ?! », *Bulletin de veille n° 1* dans GTnum 4 - Les usages numériques des jeunes, mars 2020.

11 La difficulté à comprendre les principes fondamentaux de l'informatique concerne parfois les parents ou même les professeurs, qui peuvent alors ne pas se sentir légitimes pour éclairer les élèves.

des logiques commerciales que leurs données personnelles peuvent contribuer à alimenter. Ainsi, connaître le fonctionnement d'un algorithme de classement est nécessaire pour comprendre que ce que l'on voit à l'écran dépend en réalité de ce que le système sait de nous. Des étapes importantes ont été franchies ces dernières années. Ainsi, la connaissance des langages informatiques est inscrite dans la nouvelle version du socle commun de connaissances, de compétences et de cultures et les programmes de l'école et du collège, publiés en 2015 ont constitué un pas en avant, avec une place nouvelle accordée au code et à la pensée algorithmique.

Plusieurs initiatives récentes vont dans le sens d'un renforcement de l'enseignement de l'informatique :

- **le développement d'enseignements dédiés dans le cadre de la réforme du lycée** mise en œuvre à compter de la rentrée 2019 ;
- **l'ouverture de concours spécifiques à l'informatique pour les enseignants,** afin d'assurer les nouveaux cours dédiés à cette discipline.

Les nouveaux enseignements et concours de recrutement dédiés au numérique au sein de l'Éducation nationale

La réforme du lycée en voie générale de 2019 a fait une place nouvelle au numérique dans les programmes d'enseignement :

- **l'enseignement « Sciences numériques et technologie » de 1 h 30 hebdomadaire pour tous les élèves en classe de seconde a pour but l'acquisition des principaux concepts des sciences numériques,** des savoir-faire et des connaissances leur permettant d'adopter un usage réfléchi et raisonné des technologies numériques dans leur vie quotidienne puis professionnelle. Les thèmes abordés concernent notamment Internet, le web, les réseaux sociaux et la photographie numérique ;

…/…

- **l'enseignement de spécialité « Numérique et sciences informatiques » de 4 h hebdomadaire en classe de première et de 6h hebdomadaire en classe de terminale permet aux élèves d'acquérir les concepts et les méthodes qui fondent l'informatique,** dans ses dimensions scientifiques et techniques. Plusieurs compétences sont développées : analyse et modélisation d'un problème en termes de flux et de traitement d'informations ; conception de solutions algorithmiques ; traduction d'un algorithme dans un langage de programmation. Pour sa première année, cet enseignement a été choisi par environ 8 % des élèves de première mais majoritairement par des garçons (15 % contre 2 % pour les filles).

Pour accompagner la montée en puissance de ces enseignements, des mesures spécifiques ont été prises à destination des enseignants :

- **une formation spécifique a été mise en place dans le cadre d'un diplôme universitaire ;**
- **un CAPES « Numérique et sciences informatiques »** a été créé pour la session de recrutement 2020.

Désormais, l'enjeu est d'assurer l'attractivité des enseignements de spécialité dédiés au numérique et à l'informatique, avec une attention particulière aux jeunes filles, et de veiller au développement des concours d'enseignement dédiés au numérique.

Proposition 2 : renforcer l'enseignement de l'informatique, de la donnée et du numérique pour former les jeunes à se protéger en ligne et à protéger leur vie privée

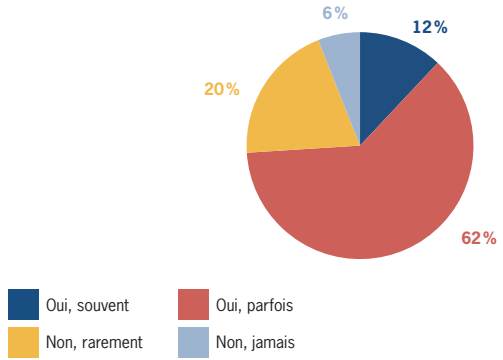
Trois dimensions permettraient ce renforcement :

- **le renforcement d'enseignements fondamentaux en amont du lycée,** pour assurer l'acquisition des concepts de base de l'informatique. Une redéfinition du contenu et des objectifs de l'enseignement de technologie au collège serait un vecteur possible pour développer cet enseignement, en complémentarité avec les mathématiques ;
- **le développement de l'enseignement de spécialité « Numérique et sciences informatiques »** en classe de première et de terminale. Cela passe par sa promotion via une communication sur les débouchés offerts, afin qu'un nombre croissant d'élèves, et notamment de jeunes filles, choisisse cet enseignement ;
- **l'élargissement progressif du vivier de professeurs spécialisés,** notamment par la création d'une agrégation d'informatique en complément du CAPES dédié et, parallèlement, le renforcement de la formation continue des professeurs consacrée à ces enjeux.

I. B. PRÉVENIR : FORMER LES JEUNES À DÉVELOPPER LEUR ESPRIT CRITIQUE FACE AUX CONTENUS EN LIGNE

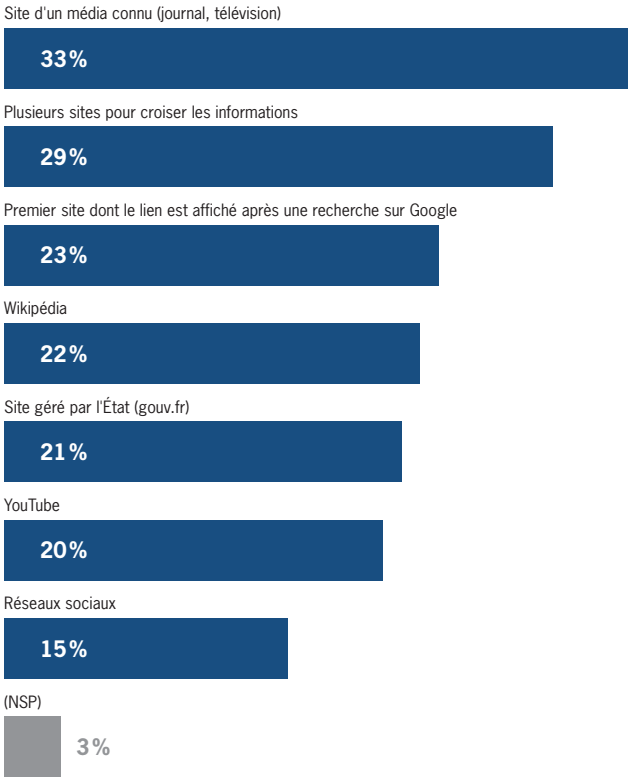
Comprendre les mécanismes fondamentaux de l'informatique et être formé à protéger ses données personnelles constituent la meilleure solution pour éviter de courir des risques importants en ligne et de devenir victime, notamment de cyberviolences. Cela n'est toutefois pas suffisant car, en l'absence d'un recul suffisant et d'une approche critique, les jeunes peuvent aussi être manipulés par les contenus qui leur sont proposés en ligne. Surtout, sans y être sensibilisés, ils sont aussi susceptibles de relayer de fausses informations ou de contenus qui ont pour but de nuire à certaines personnes. Donner aux jeunes les moyens de cette distance critique est donc nécessaire pour éviter qu'ils ne deviennent des relais, et donc des complices, d'autres utilisateurs souvent mal intentionnés. Les jeunes sondés dans le cadre du présent rapport ont été nombreux à déclarer être confrontés à de fausses informations en ligne : 12 % le sont souvent et 62 % le sont parfois. Le phénomène apparaît donc bien prépondérant dans la vie des jeunes sur Internet et les réseaux sociaux.

Degré de confrontation aux fausses informations en ligne déclaré par les jeunes



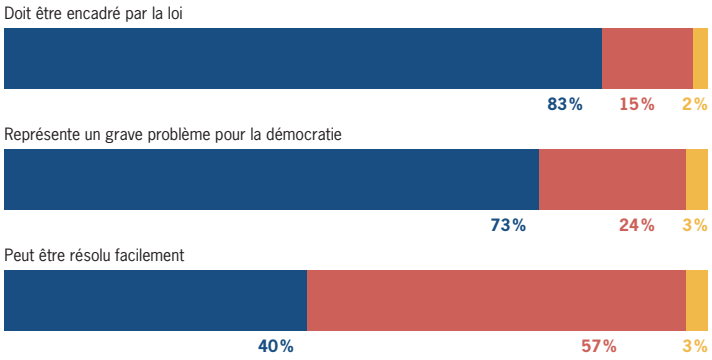
Les données collectées dans le cadre du sondage ne permettent évidemment pas d'identifier les situations où des jeunes ont été, à leur insu, victimes de fausses nouvelles. Pour autant, les données collectées montrent que les jeunes sont parfaitement conscients de la problématique des *fake news*, y ont déjà largement été confrontés et ne se tournent guère vers les réseaux sociaux lorsqu'ils cherchent de l'information.

Sources privilégiées par les jeunes lorsqu'ils cherchent une information fiable



Par ailleurs, alors que les jeunes sondés sont nombreux à identifier ce sujet comme un grave problème pour la démocratie, et qui ne peut être résolu facilement, ils sont encore plus nombreux à souhaiter un encadrement plus fort par la loi.

Appréciation portée par les jeunes sur le phénomène des fausses informations en ligne



1. De nombreux acteurs cherchent à proposer des solutions et des outils pour lutter contre les fausses informations, sans toutefois chercher à cibler les jeunes

Les médias traditionnels se sont engagés dans une démarche de *fact-checking*, laquelle se renforce et permet aux utilisateurs de disposer de nouveaux outils pour ne pas être « trompés » en ligne. Dans ce cadre la vérification des informations est effectuée par des professionnels qui remontent à une source primaire, comparent à des bases de données et demandent confirmation le cas échéant. Il peut aussi être fait appel à la collaboration des internautes par *crowdsourcing*. C'est le cas du magazine *Slate* aux États-Unis depuis 2016 ou du journal Le Monde en France avec une rubrique « Les Décodeurs » créée en 2014.

Les plateformes ont été contraintes de mettre en place des mesures en matière de fausses informations. Les GAFAM[12] se sont vu imposer la mise

12 Google, Amazon, Facebook, Apple, Microsoft.

en œuvre de dispositifs destinés à rendre effectif l'objectif de pluralisme des contenus, afin de réduire les bulles informationnelles, ces mécanismes de recommandation qui tendent à ne proposer à l'internaute que des contenus correspondant à ses centres d'intérêt et ses opinions. Facebook collabore ainsi avec des sites comme *Snopes* ou *Politifact* ou avec *ABC News* et *Associated Press* pour signaler des contenus suspects : le dispositif propose aux utilisateurs de consulter des articles réputés sérieux contestant ces contenus ; les utilisateurs sont aussi incités à appliquer des conseils de vérification et à signaler les contenus qui leur paraissent douteux. Cette démarche se décline notamment sur le terrain :

- **Politique.** En France, dans le contexte de l'élection présidentielle de 2017, la firme a passé un accord avec huit médias dont le Monde, l'AFP, BFM, Libération. Facebook fait monter sur son « mur » comme « articles en rapport », un discours réputé rationnel et vérifié, celui des médias classiques. Un article suspect est classé comme « contesté » dès lors que deux sources réputées fiables le signalent. Facebook, mais aussi Twitter et Youtube ont participé à la lutte contre la désinformation relative aux manifestations à Hong Kong suite à la propagation de *fake news* attribuée au gouvernement chinois[13] ;
- **Médical.** Pour lutter contre la désinformation sur la vaccination, Facebook s'est engagé à publier des informations factuelles élaborées par l'OMS sur les vaccins[14]. Plus récemment, dans le cadre de la crise liée à l'épidémie de Covid-19, Facebook, comme d'autres plateformes, suggèrent des liens vers les sites gouvernementaux afin de lutter contre la prolifération de fausses informations médicales.

13 Chardenon, Aude, *Facebook, Twitter et YouTube tentent d'endiguer la désinformation autour des manifestations à Hong Kong*, L'Usine Digitale, 23 août 2019.
14 Destination *Santé, Vaccination : l'OMS et les réseaux sociaux contre les idées reçues*, La Dépêche, 12 septembre 2019.

Mesures prises récemment par les GAFAM pour lutter contre les fausses informations

Google a annoncé mi-septembre 2019 avoir effectué un changement au sein de son algorithme de recherche pour mettre en avant des articles de qualité, issu d'un travail d'investigation.

YouTube propose actuellement une évolution de son système de recommandations pour lutter contre l'apparition des vidéos de désinformation et expérimente en Inde un dispositif « *Fact check* » s'affichant avant les résultats vidéo sur des sujets controversés et sur lesquels les informations qui circulent ne sont pas forcément fiables.

Instagram a annoncé que ses utilisateurs pourront signaler des publications qu'ils estiment être de la désinformation ; les posts signalés seront vérifiés par des *fact-checkers* indépendants et pourront disparaître des moteurs de recherche.

Les GAFAM dans leur ensemble, ainsi que d'autres acteurs comme IBM, participent financièrement à une initiative lancée début septembre 2019 visant à élaborer des outils technologiques permettant de lutter contre le « *deep fake* » qui est une technique de synthèse d'images fondée sur l'intelligence artificielle servant à superposer des fichiers audio et vidéo existants sur d'autres vidéos pour créer des infox et des canulars malveillants ainsi que pour créer des images pornographiques de personnes à leur insu.

Ces initiatives peuvent contribuer à aider les utilisateurs à mieux identifier les sources de confiance et les contenus controversés. Toutefois, les outils déployés reposent sur la capacité de l'internaute à identifier qu'une information est fausse ou biaisée. Ils sont donc généralement peu adaptés à un public jeune dont l'esprit critique demeure en construction. C'est donc davantage du côté de l'apprentissage de bons réflexes et le renforcement des capacité de raisonnement que se situe l'enjeu principal de la lutte contre les fausses informations auprès des jeunes.

À cet égard, il apparaît important que les jeunes puissent construire une distance critique vis-à-vis du rôle « éditorial » qui est celui des plateformes et qui repose à la fois sur une captation de l'attention et sur la recherche d'une audience maximale (viralité) contribuant à promouvoir les contenus les plus sensationnels (qui sont dans certains cas extrêmes)[15].

2. En matière d'éducation aux médias et à l'esprit critique, l'Éducation nationale dispose d'une forte expertise, désormais mobilisée à destination d'Internet et des plateformes

La prise en compte de la nécessité de former les jeunes à prendre de la distance par rapport aux informations est ancienne au sein de l'Éducation nationale.

L'enjeu d'aiguiser l'esprit critique des jeunes pour qu'ils sachent identifier les fausses nouvelles qui circulent sur Internet et évitent de les relayer questionne d'emblée le rôle de l'Éducation nationale. Ainsi, une enquête sur la confiance des Français dans les médias, publiée par La Croix en janvier 2018, montre que 88 % des Français estiment qu'il serait important d'enseigner aux élèves à rechercher sur Internet des informations vérifiées et à repérer de fausses informations.

En réalité, la France dispose d'atouts importants puisque le système éducatif français est fondé sur la tradition critique issue de Descartes et des Lumières. Apprendre à penser, former des êtres libres figurent parmi les objectifs du système éducatif français. Ils s'incarnent dans l'enseignement de la philosophie en classe terminale, mais irriguent en amont l'ensemble des disciplines et des différents niveaux de scolarité. Les enseignements d'éducation morale et civique ou encore de français sont particulièrement concernés par cette formation de l'esprit critique.

15 Le projet AlgoTransparency vise à ce titre à identifier les contenus mis en avant par l'algorithme de recommandation de YouTube.

Par ailleurs, le Centre de liaison de l'enseignement et des médias d'information (CLEMI) existe depuis 1982 et a progressivement intégré les médias numériques dans son champ d'intérêt. Cette structure, créée à l'instigation du professeur Jacques Gonnet, est un opérateur du ministère spécifiquement chargé de l'éducation aux médias et à l'information (ÉMI) dans l'ensemble du système éducatif français. Son originalité est d'associer des journalistes, des enseignants, des universitaires et des documentalistes.

Les missions et les axes de travail du CLEMI

Le CLEMI a pour mission de promouvoir, au niveau national et dans les différentes académies, notamment par des actions de formation, l'utilisation pluraliste des moyens d'information afin de favoriser une meilleure compréhension par les élèves du monde qui les entoure tout en développant leur sens critique.

Ses axes de travail concernent :

- la formation des enseignants du premier et du second degrés quelle que soit leur discipline ainsi que des formateurs (25 000 par an) et des éducateurs ;
- la production et la diffusion de ressources pour accompagner des actions à destination des élèves de la maternelle au lycée, en propre ou en coproduction (ressources vidéo, jeu sérieux « Classe investigation ») ;
- le conseil et l'expertise en France et à l'international ;
- l'organisation d'événements, dispositifs et concours d'éducation aux médias et à l'information (Semaine de la presse et des médias dans l'École qui regroupe 4 millions d'élèves et 300 000 enseignants, productions de médias scolaires – Médiatiks, #ZéroCliché, Wikiconcour Lycéen, classes Arté CLEMI reportages) ;
- l'animation du réseau des coordonnateurs académiques.

Dans la période récente, la nécessité de renforcer ce type d'apprentissage s'est faite jour. Après les attentats de 2015 sont ainsi apparues des formations ÉMI destinées à déconstruire les thèses conspirationnistes et complotistes. L'objectif poursuivi est de permettre aux jeunes de disposer des outils pour se repérer entre plusieurs sources d'information. Il ne s'agit donc pas dans ce cadre d'éviter toute forme de conformité dans la pensée, mais bien d'aider les jeunes à repérer les formes des discours complotistes, particulièrement susceptibles de bénéficier des mécanismes de viralité des plateformes en ligne.

Pour aider les jeunes à résister contre la manipulation de l'information, l'enjeu est donc double :

- Combattre la propagation de fausses nouvelles sur Internet et les réseaux sociaux, c'est le sens des outils et des solutions qui se développent actuellement ;
- Apprendre aux jeunes à identifier les fausses nouvelles et à les stopper, c'est là que le rôle de notre système éducatif et de ses forces prend toute sa place.

C'est en travaillant sur les deux aspects qu'il apparaît possible de former les jeunes à prendre toute la distance critique nécessaire par rapport à ce qu'ils consultent en ligne. Cela permet de limiter leur exposition à des risques de manipulation voire d'embrigadement. C'est aussi par cet esprit critique que les jeunes peuvent éviter de devenir les complices d'actes malveillants en en étant les relais.

Renforcer la formation à l'esprit critique pour prévenir la diffusion de fausses nouvelles et promouvoir des comportements numériques responsables se heurte toutefois à plusieurs difficultés. Tout d'abord, les professeurs, et plus largement le monde adulte, n'ont pas une connaissance précise des pratiques numériques des adolescents (quels réseaux fréquent-ils ? Pour quels usages ? Quels contenus échangent-ils en ligne ?). De fait, il n'est pas toujours facile d'accéder à une information synthétique sur le sujet, d'autant plus que les usages évoluent très rapidement[16]. De plus, comme cela a été indiqué précédemment, la formation à l'esprit critique est portée par les différentes disciplines d'enseignement, ce qui rend nécessaire une coordination entre les différents acteurs.

16 Outre l'étude Médiamétrie-DGMIC mentionnée sur les jeunes et l'information (2018), le Credoc (Baromètre du numérique) et l'INSEE publient également des données sur les usages du numérique. Il est également possible de se référer à l'étude barométrique Junior Connect sur les jeunes et les médias, réalisée par IPSOS et dont la dernière édition remonte à 2017 ou encore à l'étude "#bornsocial" sur les 10-13 ans réalisée depuis 2016 par l'agence Heaven en partenariat avec l'association Génération numérique. L'association Génération numérique réalise en outre des études avec la CNIL sur les 11-18 ans et la protection de leurs données personnelles. Par ailleurs, les enquêtes de climat scolaire et de victimation réalisés par la direction de l'évaluation, de la prospective et de la performance du ministère de l'Éducation nationale auprès des lycéens et des collégiens comportent un volet consacré aux cyberviolences. Dans le cadre de son Agence des usages, Canopé, opérateur du ministère de l'Éducation nationale, a mis en place un groupe de travail intitulé « Pratiques et usages numérique des jeunes », qui assure notamment une veille sur les publications scientifiques consacrées à ce sujet.

Proposition 3 : travailler au renforcement de l'esprit critique des jeunes pour lutter contre les fausses informations en ligne

À cet égard, plusieurs axes méritent d'être explorés :

- **la mise en place, au sein de l'Éducation nationale et en partenariat avec les administrations concernées (Direction générale des médias et des industries culturelles du ministère de la Culture notamment, CSA) d'un observatoire de la culture numérique des adolescents.** Cette structure légère, qui pourrait s'appuyer sur l'Agence des usages mise en place au sein de Canopé, suivrait en temps réel l'évolution des usages (en s'appuyant sur les études existantes et, au besoin, en faisant réaliser d'autres) et adresserait à l'ensemble du système éducatif des points de situation concrets sur les comportements des élèves. L'information pourrait également être adressée aux parents ;
- **le renforcement de la place de l'éducation aux médias et à l'esprit critique** dans les programmes, dès le cycle 3 (CM1), selon une progression claire jusqu'à la classe de terminale ;
- **la désignation, dans chaque académie et dans chaque établissement, d'un pilote transversal** pour la mise en œuvre d'une stratégie locale répondant à cette priorité donnée à l'éducation aux médias et à l'esprit critique. En collège et au lycée, le professeur documentaliste pourrait jouer ce rôle.
- **l'inclusion de nouveaux acteurs dans cette dynamique renforcement de l'esprit critique des jeunes** qui repose aujourd'hui sur les professeurs, le CLEMI, les délégués académiques au numérique ou encore les inspecteurs, en partenariat avec des médias, notamment à l'occasion de la Semaine de la presse et des médias dans l'école. Dans le respect du principe de neutralité attaché au service public de l'éducation, des acteurs du monde associatif et mutualiste ainsi que les acteurs du numérique et plateformes développant des outils de vérification et de croisement des informations et contenus pourraient être associés, sous forme de partenariats nationaux et locaux.

II. ACCOMPAGNER RAPIDEMENT ET EFFICACEMENT EN CAS DE DIFFICULTÉS (EN LIGNE)

II. A. ACCOMPAGNER : PRENDRE EN CHARGE LES JEUNES VICTIMES DE CYBERVIOLENCES AVEC SIMPLICITÉ, RÉACTIVITÉ ET EFFICACITÉ

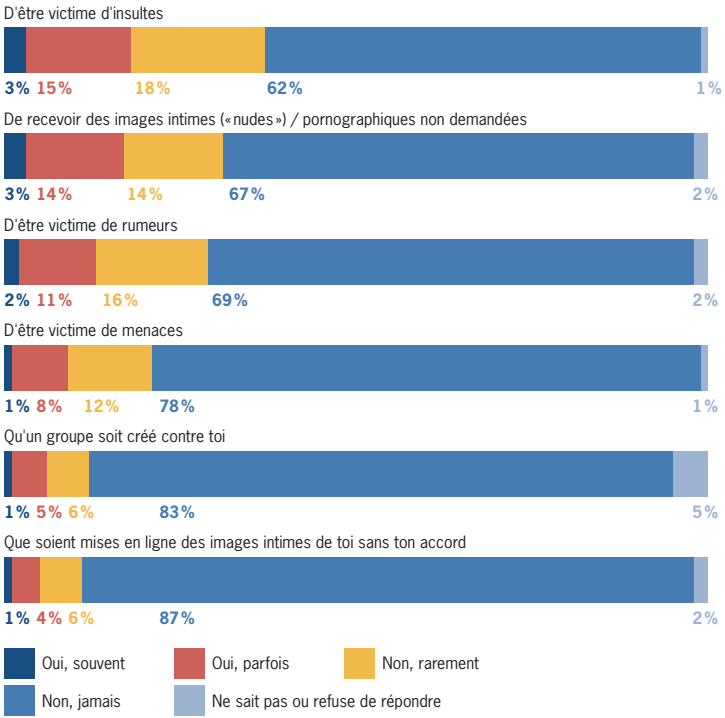
L'étude d'opinion réalisée auprès des jeunes et des parents de jeunes avait pour premier objectif de vérifier si les jeunes Français sont aussi confrontés que les jeunes Américains aux différentes formes de cyberviolence. En effet, le Pew Research Center a conduit une étude[17] dont les résultats, paru en septembre 2018, révélaient que 59 % des jeunes interrogés aux États-Unis déclaraient avoir été harcelés ou intimidés en ligne, considérant ce phénomène comme majeur et estimant que leurs professeurs, les entreprises gérant les réseaux sociaux et les politiques ne parvenaient pas à faire face à ce problème.

Les résultats obtenus sont concordants pour la France puisqu'au moins 56 % des jeunes interrogés ont déclaré avoir été confrontés au moins une fois à l'une des situations caractéristiques d'une cyberviolence,

17 Pew Research Center, *A Majority of Teens Have Experienced Some Form of Cyberbullying*, septembre 2018.

c'est-à-dire toute forme de violence réalisée au moyen d'outils numériques[18]. Ils sont encore 35 % à vivre ces situations « souvent » ou « parfois ».

Part de jeunes déclarant avoir été confrontés à une forme de cyberviolence



18 La notion de cyberviolence a été utilisé ici pour rendre de compte de la diversité des situations de violence auxquelles les jeunes peuvent être confrontés en ligne. La notion de cyberharcèlement, qui fait partie des cyberviolences, est quant à elle plus spécifique et suppose à la fois une intention de nuire et la répétition des faits.

Dans le détail, les réponses formulées varient selon la situation de cyberviolence concernée ainsi que l'illustre le graphique ci-dessus. Les échanges menés avec plusieurs interlocuteurs et les *focus groups* ont permis de souligner que, si elle la moins fréquente des situations relevées (5 % des jeunes interrogés), la publication d'images intimes de la victime, ou *revenge porn*, aboutit souvent aux conséquences les plus graves et parfois même dramatiques. Cette fragilité est nourrie par le phénomène du *sexting*, c'est-à-dire l'envoi de textes ou de photographies à caractère sexuel, qui concerne en particulier les jeunes :

- peu d'études existent sur ce sujet en France. En 2013, un sondage IFOP[19] a permis de constater que parmi les jeunes de moins de 25 ans interrogés, 35 % déclaraient avoir déjà reçu de type de contenus, 26 % avoir déjà sollicité une autre personne pour qu'elle en envoie ou avoir déjà été sollicités pour en envoyer et 25 % avoir déjà envoyé ce type de contenus ;
- en 2017, Michelle Drouin, enseignante-chercheuse à l'université de l'Indiana, a mené une étude sur le *sexting* auprès d'étudiants de son établissement[20]. Sur son échantillon d'étudiants âgés en moyenne de 19,7 ans, 62 % disaient avoir envoyé ou reçu une « photo sexuellement explicite ».

Cette situation est rendue d'autant plus aiguë dans la situation actuelle, le confinement lié à la crise Covid-19 encourageant davantage une forme de violence gratuite s'appuyant sur les images intimes de jeunes filles en particulier. L'utilisation de comptes « fisha » consiste à publier les photos de jeunes filles jugées « faciles » ou, plus rarement, de garçons infidèles ou homosexuels. Souvent hébergés sur Snapchat, ces comptes fonctionnent de la manière suivante : « une publication tous les jours à 20 heures, avec des photos, le nom, le prénom, parfois le numéro de téléphone de la jeune fille. Parfois, ce sont des contenus qui ne sont pas des images de la victime, c'est une mise en scène ; mais ça peut aussi être du *revenge porn*, des clichés échangés dans le cadre d'une relation, et que le receveur diffuse à un tiers qui en fait une affiche »[21].

19 Kraus, François, *Le « sexe 2.0», Enquête sur le sexe virtuel via les webcams et les nouvelles technologies*, IFOP, 17 avril 2013.
20 Drouin, Michelle, Coupe, Manda and Temple, Jeff, *Is Sexting Good for Your Relationship? It Depends…* Computers in Human Behavior, juin 2017.
21 Propos de Justine Atlan dans Leloup Damien et Fischer Sofia, *Harcèlement sexuel : avec le confinement, le retour en force des comptes « fisha » sur les réseaux sociaux*, Le Monde, 7 avril 2020.

Des contrastes en termes d'âge sont à relever pour l'ensemble des situations de cyberviolence au sein de l'étude conduite par l'Institut Montaigne. Ainsi, le phénomène s'accroît logiquement avec l'âge puisque le fait d'être confronté au moins une fois à l'une des situations mentionnées est de 46 % pour les 11-14 ans, de 57 % pour les 15-17 ans et de 66 % pour les 18-20 ans. Par ailleurs, **la fréquence à laquelle les filles sont généralement confrontées aux différents cas est supérieure de 2 à 3 points par rapport à celle des garçons[22].** Les focus groupes réalisés dans la perspective de cette étude ont également fait apparaître que les jeunes filles subissent davantage de violence que les garçons et expriment spontanément des craintes assez fortes lorsqu'elles évoquent Internet et les réseaux sociaux.

D'autres études - qui ne portent pas spécifiquement sur les jeunes - font également apparaître la prégnance des LGBT[23]-phobies sur Internet. Ainsi, l'édition 2019 du rapport annuel de SOS-homophobie relève : « en 2018, 23 % des cas enregistrés par l'association font état de LGBT-phobies sur Internet. Cela fait plusieurs années que le Web, notamment les réseaux sociaux, demeure le principal contexte des LGBT-phobies. Viennent ensuite Lieux publics (13 %), Travail (11 %), Famille (10 %), Voisinage (9 %), Commerces (6 %) et Milieu scolaire (5 %) »[24].

Une étude récente de l'Institute for Strategic Dialogue, intitulée *Cartographie de la haine en ligne* montre également l'ampleur des discours misogynes et anti-LGBT sur Internet[25]. Cette étude vise en particulier à fournir des données de recherche factuelles sur les différentes formes de discours haineux en ligne en France sur différentes plateformes de réseaux sociaux. Pendant 5 mois, l'ISD a collecté des données, notamment des mots-clés utilisés, pour entraîner des algorithmes d'identification. Onze ensembles de données ont ainsi été créés,

22 Cet écart est assez proche de celui constaté, en matière de cyberviolences, dans les enquêtes de victimation menées par l'Éducation nationale auprès des collégiens et des lycéens.

23 Ce sigle désigne les personnes homosexuelles, bisexuelles, transgenres ou intersexes ainsi que celles qui s'interrogent sur leur identité sexuelle.

24 SOS homophobie, *Rapport sur l'homophobie 2019*, p. 15. Le rapport consacre un chapitre entier à « Internet, haine à haut débit ».

25 Gatewood Cooper, Guerin Cécile, Birdwell Jonathan , Boyer Iris et Fourel Zoé, *Cartographie de la haine en ligne*, Institut pour le Dialogue Stratégique (ISD), 2020.

en suggérant des termes fréquemment associés à des contenus ciblant des groupes à raison du sexe et de l'orientation sexuelle, de l'origine ethnique et raciale, de la religion et du handicap et dont l'intention était d'inciter à la haine, à la violence ou à la discrimination. Plusieurs résultats sont tirés :

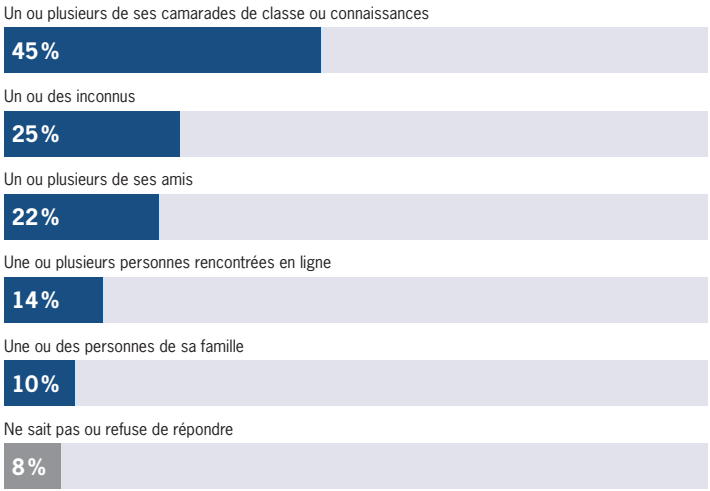
- 7 millions de cas certains de discours haineux en ligne contre les femmes, les personnes de la communauté LGBTQ, les personnes handicapées et les communautés arabes françaises ;
- la plupart des discours haineux en ligne comprenaient l'utilisation généralisée d'injures et d'insultes fondées sur des attaques visant des catégories protégées ;
- un faible pourcentage de discours haineux était constitué d'attaques ciblées contre des individus (5 %) ;
- parmi les comptes qui postent le plus souvent des propos haineux, 19 % présentaient un comportement automatisé ou de type bot ;
- des événements, tels que la journée internationale de la femme ou l'annonce de la nomination de Bilal Hassan à l'Eurovision, ont provoqué des pics de discours haineux ;
- l'approche fondée sur les mots-clés a mis en évidence une faible proportion d'efforts organiques et/ou coordonnés de contre-discours sur les réseaux sociaux (1 %) ;
- un recoupement important existe entre les différents types de discours haineux, ce qui démontre la nécessité d'une analyse plus transversale des discours de haine en ligne ;
- la recherche menée a démontré le potentiel et les limites que présentent les algorithmes de traitement du langage naturel pour identifier les discours de haine en ligne.

Le sondage réalisé dans la perspective de ce rapport examine également les réponses disponibles en cas de cyberviolences. 84 % des jeunes interrogés considèrent que leurs parents ont un rôle à jouer à cet égard. Toutefois, la difficulté majeure réside dans l'absence d'interlocuteurs clairement et spontanément identifiables vers lesquels se tourner. Ainsi, 61 % des parents sondés déclarent ne pas savoir vers quelle administration se tourner si leur enfant est victime.

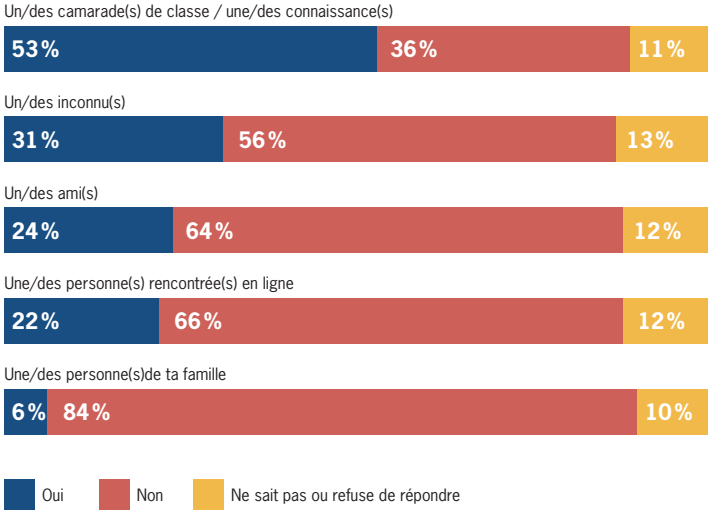
Comment ces constats peuvent-ils s'expliquer ? Le cyber(harcèlement) et les cyberviolences dont les jeunes peuvent être victimes et auteurs sont en premier lieu sujets à des divergences de définition. Ils ne font par ailleurs pas l'objet d'une politique publique unifiée et donnent lieu à plusieurs formes de réglementation et d'outils à l'efficacité variable. Les plateformes, dont la place est centrale, ont récemment mis en place des instruments mais leur responsabilité demeure largement à construire (cf. III).

Par ailleurs, si les parents de jeunes interrogés dans le cadre des *focus groupe* ont d'abord associé les risques d'Internet et des réseaux sociaux pour leurs enfants à des personnes inconnues - ce qui peut être vrai dans certaines situations - la plupart a ensuite décrit des cas où l'auteur des faits était un ami ou une connaissance de leur enfant. **De fait, le sondage fait apparaître que les cyberviolences que subissent certains jeunes trouvent en majorité naissance dans les relations qu'ils entretiennent avec ceux qu'ils fréquentent** à l'école, dans leurs activités sportives, parmi leurs amis, etc.

Auteurs de cyberviolences identifiés par les parents



Auteurs de cyberviolences identifiés par les jeunes



Ce prolongement dans le numérique des violences et du harcèlement vécus au quotidien, généralement dans un cadre scolaire, est aussi ce qui en rend la perception par les adultes souvent plus délicate. En effet, ces phénomènes existent de longue date et peuvent parfois trop rapidement être assimilés à des chamailleries entre jeunes.

En matière de cyberviolences touchant les jeunes, plusieurs traits spécifiques, qui conditionnent autant la compréhension du phénomène que la construction de solutions, méritent d'être relevés :

- le développement des cyberviolences touchant les jeunes[26] ;
- des mutations très rapides des formes et des canaux s'agissant des cyberviolences ainsi que des formes et des canaux qu'elles empruntent, avec des effets générationnels importants ;
- l'extension, signalée par plusieurs des interlocuteurs rencontrés dans le cadre de ce rapport, de ces phénomènes à des publics de plus en plus jeunes, suivant en cela l'extension des usages numériques[27].
- la diffusion rapide (« viralité ») des contenus, qui est imputable au moins autant à l'auteur initial qu'à ceux qui relaient ses comportements en ligne, d'où l'importance d'une formation suffisante (cf. partie I) ;
- le caractère éphémère des contenus sur certains réseaux sociaux qui sont précisément plébiscités par les jeunes pour cette raison (par exemple Snapchat) ;
- l'atténuation de la distinction entre violence et cyberviolence, entre harcèlement et cyberharcèlement (des violences réelles se prolongent dans le monde « réel » et inversement) ;
- l'existence occasionnelle d'une similitude entre le profil de la victime et celui de l'auteur.

26 Ainsi, l'enquête de climat scolaire et victimation réalisée par la direction de l'évaluation, de la performance et de la prospective du ministère de l'Éducation nationale montre que la proportion de lycéens se déclarant victime de vidéos, de photos ou de rumeurs humiliantes sur Internet est passée de 4,1 % en 2015 à 9 % en 2018 (9,9 % pour les filles et 8,1 % pour les garçons). En revanche, la proposition de lycéens injuriés ou moqués sur les réseaux sociaux est restée sable (7,5 % en 2015 et 7,6 % en 2018). L'Éducation nationale réalise également une enquête de victimation auprès des collégiens, mais les items relatifs aux cyberviolences testés en 2017 ne l'avaient pas été sous la même forme précédemment (en 2017, 9,1 % de collégiens se déclaraient victimes de diffusion de rumeurs par Internet et 8,3 % déclaraient avoir reçu des photos ou vidéos humiliantes).

27 L'enquête « #BornSocial » réalisée par l'agence Heaven en partenariat avec l'association Génération numérique indique que 54,1 % des élèves de 6e à la rentrée 2018 étaient inscrits sur un réseau social, en progression de 8,4 points par rapport à l'année précédente.

1. La prise en charge des cyberviolences, et notamment du cyberharcèlement, est récente au sein du monde éducatif

Parmi les cyberviolences, le cyberharcèlement est le plus pris en compte par les administrations. Ceci est notamment dû aux conséquences parfois dramatiques auxquelles il peut aboutir et au fait qu'il s'articule avec le harcèlement scolaire, phénomène désormais clairement identifié et combattu au sein de l'Éducation nationale, y compris dans sa composante numérique.

Le harcèlement scolaire, bien qu'ancien et analysé par le monde de la recherche, a été véritablement reconnu par l'Éducation nationale au début des années 2010, dans le prolongement d'actions initiées aux États-Unis sous la présidence Obama. Cette prise de conscience a résulté d'un rapport rédigé par Éric Debarbieux, président du Conseil scientifique des états généraux de la sécurité à l'école organisés par le ministre Luc Chatel. L'étude « Refuser l'oppression quotidienne : la prévention du harcèlement à l'École » a ainsi permis de faire le point sur la connaissance, au niveau international, des phénomènes de harcèlement à l'école et de mettre en évidence la nécessité d'une politique nationale impliquant l'ensemble de la communauté éducative.

Définition du harcèlement à l'École

Reprenant le terme de « *school bullying* », le rapport de 2011 définit ce harcèlement comme « une violence répétée, verbale, physique ou psychologique, perpétrée par un ou plusieurs élèves à l'encontre d'une victime qui ne peut se défendre, en position de faiblesse, l'agresseur agissant dans l'intention de nuire à sa victime ».

.../...

Les principales formes de ce harcèlement relevées sont les suivantes :
- physiques, verbales, relationnelles (ostracisme) et cyber (sur Internet et les téléphones portables) ;
- directes (face-à-face) ou indirectes (via un tiers, par le biais de rumeurs méchantes notamment) ;
- individuelles ou fondées sur l'identité d'un groupe (homophobie, sexisme, racisme, handicap), c'est-à-dire comme expression de discriminations.

Depuis 2011, le sujet du harcèlement scolaire a donné lieu à la définition et à la construction progressive et continue d'une véritable politique publique :
- le harcèlement scolaire a été reconnu officiellement dans la loi du 8 juillet 2013 d'orientation et de programmation pour la refondation de l'école de la République[28] ;
- le phénomène fait l'objet d'études statistiques régulières par le biais des enquêtes de victimation et de climat scolaire de la direction de l'évaluation, de la prospective et de la performance (DEPP) ;
- des actions de prévention sont menées sous la forme de campagnes de sensibilisation (« Non au harcèlement » en 2014, « Le harcèlement, pour l'arrêter, il faut en parler » en 2017), d'un site d'information « Non au harcèlement » impliquant des influenceurs et d'affichages ;
- la mise en place de deux numéros d'écoute : en juin 2011, le numéro vert « Net écoute » 0 800 200 000 pour agir contre le cyberharcèlement et les cyberviolences, géré par l'association e-Enfance et, en février 2012, le 3020 pour recueillir la parole des familles et des victimes de harcèlement scolaire ;

Par ailleurs, des associations comme *Marion Fraisse la main tendue* contribuent, par leurs interventions en milieu scolaire, à la sensibilisation des élèves.

28 Rapport annexé à la loi n° 2013-595 du 8 juillet 2013 *d'orientation et de programmation pour la refondation de l'école de la République.*

Les deux numéros nationaux de prise en charge du harcèlement scolaire et du cyberharcèlement

Le 3020 est la ligne d'écoute pour traiter les situations de harcèlement scolaire. Des psychologues et des professionnels des sciences de l'éducation répondent aux appels des jeunes et de leurs parents. Ces derniers sont ainsi accompagnés pour trouver un interlocuteur capable de les aider sur le territoire où ils résident et identifier les solutions à mettre en œuvre. Le 3020 assure le relais avec les référents « harcèlement » présents dans chacune des académies. Ce dispositif repose sur un Numéro vert gratuit disponible de 9 h 00 à 20 h 00 du lundi au vendredi et le samedi de 9 h à 18 h sauf jours fériés.

« Net Écoute 0 800 200 000 » est le numéro vert national destiné aux enfants et adolescents confrontés à des problèmes dans leurs usages numériques. Le contact est 100 % anonyme, gratuit et confidentiel. Outre le téléphone, plusieurs modes de contact sont possibles : email, chat, Messenger, être rappelé. Le service est ouvert du lundi au vendredi de 9 h 00 à 20 h 00 et le samedi de 9 h 00 à 18 h 00 sauf jours fériés. Des psychologues, juristes et spécialistes du numérique répondent aux jeunes, aux parents et aux professionnels.

Plusieurs objectifs sont poursuivis :
- écouter : l'équipe est composée de psychologues et de personnel spécialisés pour évaluer rapidement le niveau de détresse des enfants et adolescents et de leur apporter des réponses rapides et efficaces ;
- informer : une information claire et pertinente est apportée pour savoir comment réagir sur les outils numériques et hors ligne ;
- signaler : Net Écoute est un tiers de confiance auprès des réseaux sociaux et peut leur signaler des contenus de manière prioritaire, ce qui en permet le retrait ou le blocage ;

.../...

- conseiller/orienter : l'équipe travaille en relation étroite avec un certain nombre de plateformes officielles partenaires dont le 119 – numéro national de l'enfance en danger ; PHAROS et Fil Santé Jeunes ; la Brigade du numérique de la gendarmerie ; le cas échéant, l'équipe oriente vers le dépôt de plainte ou le signalement au Procureur de la République.

Depuis 2019, un renforcement des mesures déployées est à l'œuvre. À l'occasion de la remise du prix « Non au harcèlement » le 3 juin 2019, Jean-Michel Blanquer a annoncé dix nouvelles mesures pour renforcer la lutte contre le harcèlement scolaire par une approche plus globale qui passe notamment par :

- l'inscription dans le code de l'éducation du droit des enfants à suivre une scolarité sans harcèlement, concrétisée par la loi pour une École de la confiance du 26 juillet 2019[29] qui a créé un nouvel article L. 511-3-1 au sein du code de l'éducation, lequel dispose qu' *« aucun élève ne doit subir, de la part d'autres élèves, des faits de harcèlement ayant pour objet ou pour effet une dégradation de ses conditions d'apprentissage susceptible de porter atteinte à ses droits et à sa dignité ou d'altérer sa santé physique ou mentale »* ;
- la mise en place d'un programme anti-harcèlement « clé en main » à destination des écoles et collèges, avec des équipes ressources et 10 heures d'apprentissages par an pour les écoliers et les collégiens ainsi que des kits d'information destinés aux parents ;
- la formation de l'ensemble des acteurs à la prévention du harcèlement ;
- la constitution de réseaux départementaux d'intervention en cas de situation complexe et la création d'une plateforme nationale permettant d'identifier les intervenants à contacter.

Par ailleurs, le ministère entend développer le système des collégiens et lycéens « ambassadeurs » chargés de sensibiliser leurs camarades à la problématique du harcèlement.

29 Loi n° 2019-791 du 26 juillet 2019 *pour une école de la confiance*.

Le renforcement de cette politique publique apparaît d'autant plus nécessaire que le harcèlement scolaire concerne un nombre croissant de jeunes, avec une extension des cas dans le premier degré et que le harcèlement s'inscrit dans un mouvement plus large dépassant le seul univers de l'école (applications, sites Internet, séries télévisées). De plus, plusieurs interlocuteurs rencontrés dans le cadre de ce rapport ont indiqué que les numéros d'écoute demeurent mal connus des élèves et que les actions de sensibilisation (mobilisant par exemple des associations) sont souvent mises en place par les établissements scolaires à la suite de faits de harcèlement et non de manière préventive.

2. Les dispositifs pour traiter ce type de cyberviolences restent disparates

1/ D'autres dispositifs d'aide et d'accompagnement existent sans constituer une réponse immédiate à une situation de cyberviolence spécifique

C'est en particulier le cas de la **Brigade numérique de la Gendarmerie,** qui a pour objectif de donner de l'information générale aux internautes en matière de sécurité publique. Ce service, intitulé formellement « Contact numérique de la Gendarmerie nationale », est disponible à partir du site Internet de la Gendarmerie nationale et par l'intermédiaire de certains réseaux sociaux. Il a pour objectif de contribuer à faciliter les échanges entre la Gendarmerie nationale et ses usagers, notamment ceux qui sont rompus à des modes de communication numériques plutôt que physiques via un formulaire de contact et une messagerie instantanée disponible 7 jours sur 7. Toutefois, il est à noter que ce dispositif ne constitue pas un moyen de signaler des situations d'urgence, lesquelles font l'objet de modalités plus classiques exposées ci-après.

Par ailleurs, sur le terrain de la santé, **Filsantejeunes.com** (0 800 235 236), numéro vert, gratuit, réservé aux jeunes de 12 à 25 ans, tous les jours de 9 h à 23 h. Il peut être sollicité par les jeunes dont la santé serait affectée par des cyberviolences. Le service, géré par l'association Ecole des parents et des éducateurs d'Île-de-France, est composé d'adultes aux compétences

professionnelles complémentaires, habitués à répondre aux questions santé des jeunes.

Le rôle du présent rapport n'a pas été de procéder à une recension exhaustive des dispositifs en place, d'autant que ceux-ci peuvent considérablement varier d'un territoire à l'autre en fonction des partenariats et des initiatives locales.

2/ La possibilité de signaler des contenus en ligne est ouverte auprès d'une plateforme dédiée du ministère de l'Intérieur mais elle exclut en principe une affaire privée

Pour le signalement des contenus et comportements illicites en ligne existe la **plateforme PHAROS**[30] gérée par l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) et accessible via le site www.internet-signalement.gouv.fr ou par l'intermédiaire de certaines associations partenaires comme « Point de contact » ou « Net Écoute ». Cet outil a toutefois un objet plus large que la lutte contre le cyberharcèlement puisqu'il vise aussi à lutter contre les contenus illicites : contenus et comportements liés à la pédophilie et la pédopornographie, au terrorisme et à son apologie, aux arnaques financières, à l'incitation à la haine raciale, ethnique et religieuse et à l'expression du racisme, de l'antisémitisme et de la xénophobie. **Surtout, il est précisé que ce dispositif ne doit pas concerner une affaire privée ni même un contenu privé,** ce qui le disqualifie *a priori* dans le cas où le contenu jugé illicite concerne une victime déterminée. Si PHAROS est donc un outil pertinent pour signaler des contenus illicites, il ne l'est pas pour les faits de cyberviolences. Enfin, PHAROS ne prend en compte que les signalements avec un lien URL, or cela exclut structurellement les plateformes qui ne fonctionnent pas avec des liens, telles que Snapchat par exemple.

30 Plateforme d'Harmonisation, d'Analyse, de Recoupement et d'Orientation des Signalements.

Règles encadrant la saisie de la plateforme PHAROS

- Il doit s'agir d'un contenu ou d'un comportement illicite, c'est-à-dire qu'il doit être interdit et puni par une loi française. Les contenus ou comportements que l'utilisateur juge simplement immoraux ou nuisibles n'ont pas à être signalés sur PHAROS ;
- il doit s'agir d'un contenu public de l'Internet, auquel tout internaute peut se retrouver confronté : site Internet, blog, forum, propos sur un « *tchat* », agissement d'un « rôdeur » anonyme sur une messagerie, etc. ;
- il ne doit pas s'agir d'une affaire privée avec une personne que l'utilisateur connaît, même si elle utilise Internet pour lui nuire. Dans ce cas, il faut se présenter dans un Commissariat de Police ou une Brigade de Gendarmerie ;
- il ne doit en aucun cas s'agir d'une urgence nécessitant l'intervention de service de secours (accident, incendie, agression, etc.). Dans ce cas, il faut composer le 17.

3/ En cas d'urgence, les services de secours, les forces de l'ordre et de la protection de l'enfance sont les seuls compétents bien que leur champ d'action soit plus large

Ainsi que le précise les différents interlocuteurs animant les structures d'aide et d'accompagnement, le traitement de situations urgentes représentant une menace pour la sécurité des personnes et des biens n'est pas de leur ressort. Il convient alors pour le jeune victime et ses parents ainsi que pour les témoins éventuels de se tourner notamment vers :

- le **17 « police secours »** pour signaler une infraction nécessitant l'intervention immédiate de la police ;
- le **112,** numéro d'appel d'urgence européen en cas d'accident, et le **114** pour les personnes sourdes et malentendantes ;

Par ailleurs, les jeunes peuvent aussi le cas échéant composer le **119,** *Allô enfance en danger*, également accessible 24h/24 et 7 jours/7, qui est le numéro national d'accueil téléphonique de l'enfance en danger. Depuis le 3 avril 2020, cette ligne est doublée d'un service de signalement par écrit des violences, via un formulaire en ligne, afin de pouvoir aider les victimes qui, du fait du confinement, ne peuvent s'isoler pour appeler à l'aide. Cependant le formulaire impose de saisir un courriel afin de déposer sa demande de signalement, élément qui peut représenter une barrière pour des jeunes n'ayant pas d'adresse email ou bien les obligeant à utiliser celle de leurs parents. La mission du service gérant cette ligne est double : d'une part prévenir et protéger les enfants en danger ou en risque de l'être, d'autre part, transmettre les informations préoccupantes concernant ces enfants aux services départementaux compétents, les cellules de recueil des informations préoccupantes (CRIP), aux fins d'évaluation de la situation des jeunes concernés. De fait, certains jeunes victimes de cyberviolences ne trouvent pas, dans le cadre familial, le soutien dont ils ont besoin. Dans ces cas là, la mobilisation des services de protection de la jeunesse est essentielle pour leur venir en aide.

Ces services sont susceptibles de **prendre l'attache des services judiciaires,** en particulier le Procureur de la République en vertu des dispositions du second alinéa de l'article 40 du code de procédure pénale[31]. La saisine des services de police, qui s'adaptent à ces nouveaux phénomènes, mais aussi de la justice peut aussi être directement réalisée par la victime à condition de respecter les conditions de recevabilité.

31 *« Toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs ».*

La formation des gendarmes pour traiter la cyberdélinquance

La formation des gendarmes inclut désormais un volet cybercriminalité, décliné sur plusieurs niveaux.

- Les gendarmes disposent tous d'une formation de base sur ce volet, assurée par un enseignement à distance complété par des exercices pratiques en école de gendarmerie.
- Les gendarmes sont également sensibilisés à la manière de recueillir la plainte liée à la cybercriminalité afin d'obtenir tous les éléments de preuves nécessaires, en vue de transmettre un dossier complet à un agent plus spécialisé qui pourra assurer des investigations techniques plus poussées. À cet égard, une formation en école comporte des modules sur la téléphonie, les investigations Internet et la saisie des preuves numériques.
- Enfin, au niveau supérieur, le grade correspondant nouvelles technologies (CNTECH) est octroyé aux agents ayant reçu une formation de cinq jours.

3. Les plateformes proposent des outils de modération aux résultats encore largement perfectibles, elles travaillent également plus étroitement avec certains acteurs publics

Les différentes plateformes mettent à disposition de leurs utilisateurs des outils destinés à limiter les cyberviolences.

Twitter permet par exemple à l'utilisateur de bloquer des comptes ou de les empêcher de s'adresser à lui, de couper les notifications, de basculer le compte en privé ou de filtrer certains mots définis par lui. Chaque utilisateur a accès à une option de signalement afin d'informer les plateformes de l'existence de contenus problématiques, insultant ou violent, envers lui-même ou d'autres personnes.

La limite forte tient à la réponse standardisée : « *Nous avons constaté l'absence d'infraction aux règles de Twitter relatives aux comportements inappropriés* », qui ne permet pas de déterminer si Twitter a réalisé les diligences nécessaires . Twitter a également mis à jour ses règles en matière de discours haineux début juillet 2019 afin d'interdire les posts visant les groupes religieux et utilisant des termes insultants et déshumanisants pour les qualifier.

En juin 2019, YouTube a annoncé la mise en place d'une politique plus stricte en matière de discours haineux, notamment par :

- l'interdiction des contenus vidéo promouvant la supériorité d'un groupe d'individus pour justifier des discriminations, ségrégation ou exclusion sur le fondement de l'âge, du genre, du groupe, de la religion, de l'orientation sexuelle ou du statut de vétéran – l'idéologie Nazi est explicitement mentionnée – ou visant à dénier l'existence d'événements historiques violents prouvés et documentés – l'Holocauste ainsi que la fusillade à Sandy Hook Elementary sont visés ;
- la limitation de la propagation de contenus sujets à caution et la promotion de contenus provenant de sources sûres, en particulier par des recommandations adressées prioritairement aux utilisateurs consultant des contenus *borderline* ;
- la récompense et la rémunération des éditeurs de confiance contribuant à renforcer la qualité des contenus sur YouTube.

Les effectifs des plateformes dédiés à la modération des contenus

- 30 000 personnes sont déclarées par Facebook comme s'occupant de modération de contenus dont la moitié sur la partie opérationnelle.
- 10 000 personnes seront à terme chargées de lutter contre les contenus susceptibles d'être en violation avec le règlement chez Google et YouTube ; dans le cas plus particulier de YouTube, les signalements proviennent à la fois des membres de la communauté et d'un « apprentissage automatique », c'est-à-dire par algorithmes ; à titre d'illustration

.../...

entre janvier et mars 2019, ont été retirés de YouTube 8,3 millions de vidéos (en majorité relevant du *spam*) dont 89 000 représentant une incitation à la violence et 47 000 représentant une forme de cyber harcèlement, ainsi que 220 millions de commentaires supprimés ;

- Quelques centaines de personnes sur les 3 920 salariés travaillant chez Twitter.

En France, la loi du 22 décembre 2018 relative à la lutte contre la manipulation de l'information, a prévu que le CSA assure le suivi des actions mises en œuvre par les plateformes et leur adresse des recommandations (cf. encadré 20).

Les liens entre les plateformes et les autorités judiciaires et policières se resserrent.

Un groupe de contact permanent a été mis en place par la police nationale et la préfecture de police de Paris avec Google, Apple, Facebook et Microsoft, réuni chaque trimestre sous l'égide de la délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces (DEMISC). L'objectif est d'établir des standards de réquisitions afin de fluidifier les démarches de justice en cas de contenus ou de comportements illicites. Entre janvier et juin 2019, Facebook indique avoir reçu 5 782 requêtes de la part des autorités publiques en France, 70 % d'entre elles ayant donné lieu à une transmission d'informations. Ces chiffres sont à mettre en regard de ceux obtenus sur la même période en 2015, avec 2 520 requêtes dont 42,5 % ayant donné lieu à transmission d'informations[32].

En juin 2019, Facebook a annoncé qu'il allait davantage collaborer avec les autorités dans la transmission de données en cas de requêtes judiciaires sur les contenus haineux. Jusqu'alors, lorsque les adresses IP des suspects étaient localisées à l'étranger, les enquêteurs avaient du mal à remonter à la source et à récupérer les données personnelles : ils devaient pour cela s'appuyer sur des accords internationaux et traités d'assistance mutuelle avec un délai souvent très long. Toutefois

32 *France*, Facebook Transparency, juin 2019.

Facebook a assorti cette annonce de réserves tenant au caractère non systématique des transmissions et au droit de Facebook de refuser toute collaboration.

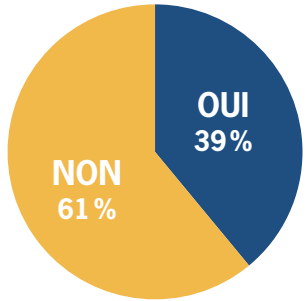
4. Le cadre actuel de prise en charge doit pouvoir évoluer vers une logique de guichet unique construite en partant de la situation et des usages des jeunes

Beaucoup des dispositifs en place illustrent le fait que les solutions demeurent construites à partir des structures et des services qui les assurent plutôt que du point de vue des utilisateurs. En effet, protéger les victimes suppose de bien identifier leur niveau d'information sur le phénomène, sur les interlocuteurs à solliciter et sur les bons réflexes à adopter. Dès lors, la lutte contre les cyberviolences est confrontée à plusieurs enjeux :

- l'accès à l'information, qui peut passer par des actions de prévention et une meilleure visibilité des supports et documentations ;
- la lisibilité de l'aide disponible, en particulier entre les différents sites Internet et lignes de contact à disposition, et la formation des adultes susceptibles d'apporter une aide ou une prise en charge ;
- la capacité à prendre en compte l'atténuation de la distinction entre harcèlement scolaire et cyberharcèlement en raison de sa faible pertinence et de l'organisation fragmentée et segmentée qu'elle entraîne et qui nuit à la meilleure prise en charge des victimes ;
- la mobilisation de l'ensemble des adultes susceptibles de détecter les signaux faibles de situations de harcèlement et de constituer des référents pour les jeunes, en particulier les acteurs du périscolaire (animateurs, assistants de vie scolaire, personnel de cantine, chauffeurs de bus scolaires, etc.) afin de tenir compte de l'ensemble des lieux où les jeunes évoluent au quotidien (classes, cours, cantine, couloir, chemin, commodités). Cela implique un travail avec les collectivités employeurs de ces personnels ;
- la confiance que doivent pouvoir avoir les jeunes dans les dispositifs d'accompagnement et d'aide, *a fortiori* pour ceux qui ne bénéficient pas ou peu du soutien d'un parent ou d'un proche, voire craignent leur réaction s'ils leur disent avoir été victimes de cyberviolences.

Preuve de la complexité très forte qui existe à ce jour, plus de **6 parents sur 10 indiquent qu'ils ne sauraient pas vers quelle administration se tourner** si leur enfant était victime de cyberviolence.

Réponse des parents à la question de savoir s'ils sauraient quelle administration contacter en cas de cyberviolence



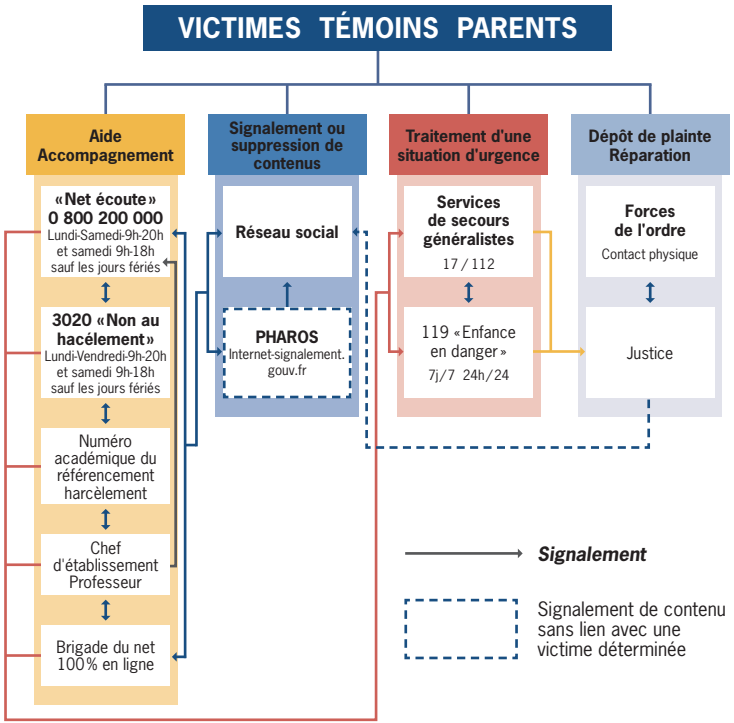
L'articulation entre les différents dispositifs d'écoute, de contact et de prise en charge, ainsi que la circulation de l'information entre eux, peuvent donc être améliorées

L'ensemble des dispositifs présentés, dont les missions et pouvoirs diffèrent très largement, ne fait pas pour l'heure l'objet d'une mise en cohérence d'ensemble. Le graphique ci-dessous l'illustre à plusieurs titres :

- **il existe au moins 4 grandes fonctions dans la prise en charge des cyberviolences** et celles-ci reposent sur des acteurs différents qui ne sont pas toujours connus ou identifiés par le grand public ;
- **les rôles respectifs entre les dispositifs dédiés aux jeunes ne sont pas toujours clairs,** notamment en termes d'aide et d'accompagnement dans le champ éducatif : qui fait quoi entre le 3020, Net Écoute et les numéros académiques ?
- **les liens entre les différents dispositifs dédiés aux jeunes sont parfois difficiles à établir,** en particulier entre l'accompagnement d'une part, et la modération des contenus et la prise en charge policière et judiciaire d'autre part ;

- **les modalités de suivi des cas détectés sont parfois absentes ou à sens unique (sans retour d'information à toute la chaîne de signalement),** ce qui ne permet pas une fluidité de circulation de l'information entre les différents acteurs ;
- **les relations entre les autorités publiques d'une part, et les plateformes, hébergeurs et fournisseurs d'accès Internet d'autre part,** demeurent encore largement à construire.

Cadre actuel de prise en charge et de signalement des cyberviolences



S'agissant de l'aide et de l'accompagnement, il existe une multitude de dispositifs, ce qui peut affaiblir leur efficacité respective. Ainsi le 3020 agit entièrement pour le compte de l'Éducation nationale et permet la collecte d'informations par des signalements traités par des spécialistes et assure une prise en charge des victimes et de leurs familles par l'un des 310 référents harcèlement soumis à l'obligation de contacter, sous moins de huit jours, le chef d'établissement de l'élève victime. Le numéro Net Écoute bénéficie d'une subvention de l'État et se présente comme un tiers de confiance vis-à-vis des opérateurs et des plateformes numériques, susceptible de solliciter le retrait sous bref délai d'un contenu en ligne et d'accompagner les familles dans les démarches de dépôt de plainte. Dans chaque académie, un numéro dédié permet de contacter directement le référent harcèlement mais il est rarement connu ou diffusé.

En termes de signalement et de suppression de contenus liés à un cas spécifique de cyberviolence, un rôle prépondérant est accordé aux plateformes, ce qui pose inévitablement la question de leur responsabilité (cf. partie III). Plus encore, le dispositif PHAROS proposé par le ministère de l'Intérieur ne concerne que les contenus publics et ne vise pas à couvrir des situations particulières.

Le traitement des situations d'urgence relève d'acteurs différents dont le rôle est bien plus large. C'est le cas de l'ensemble des services de secours mais aussi de l'aide sociale à l'enfance qui ne disposent pas toujours de l'expertise pour traiter les cyberviolence et se trouvent généralement contraints à prioriser les différentes situations qui leur sont soumises.

Une démarche d'adaptation constante aux mutations des formes de cyberviolence apparaît en outre nécessaire pour garantir une efficacité dans le temps.

Les formes mêmes de cyberviolence et le champ des victimes potentielles évoluent rapidement et impliquent une adaptation et une réactivité fortes. En particulier, les auteurs de cyberviolences ont tendance à se reporter vers de nouvelles plateformes lorsque celles auxquelles ils recouraient accroissent la modération des contenus. De plus, les victimes, mais aussi les auteurs de cyberviolences, ont également tendance à être de plus en plus jeunes, la

préoccupation qui portait notamment sur les collégiens et lycéens se trouvant désormais étendue aux élèves du premier degré.

La démarche d'adaptation nécessite :

- des capacités de veille portant sur les outils, plateformes et publics non couverts par les dispositifs en place, afin de tenir compte des évolutions souvent rapides qui peuvent se faire jour ;
- un travail associant experts et professionnels en lien avec les jeunes afin d'adapter la sensibilisation, la prévention et la prise en charge, notamment en fonction de l'âge – le premier degré étant ici visé ;
- des moyens techniques et humains permettant de répondre à l'accroissement du nombre de signalements et de requêtes adressés aux éditeurs de contenus et plateformes, en tenant compte du fait que le cyber harcèlement peut consister à utiliser des termes ou contenus qui sont en eux-mêmes légaux, mais dont le contexte d'utilisation peut conduire à en faire une utilisation détournée, ce qu'une intelligence artificielle n'identifie pas pour l'heure.

Proposition 4 : construire un véritable guichet unique clairement identifié pour la prise en charge des jeunes victimes de (cyber)violences, y compris dans un cadre scolaire

La construction de ce guichet unique suppose de partir de l'expérience utilisateur et de clarifier les compétences et les circuits d'informations :

→ **Une adaptation est nécessaire pour répondre aux besoins des jeunes et à leurs pratiques de communication,** ce qui suppose une disponibilité forte, surtout en dehors des horaires d'école (soirée, weekend), une diversification des canaux de contact (téléphone, interface web, appli, chat) et surtout un portail unique d'écoute et de prise en charge bien identifié, de type 3919, coordonnant les actuels numéros d'aide et d'accompagnement, et s'articulant avec les autres dispositifs de signalement, d'urgence et de plainte. …/…

→ **La clarification des compétences et du circuit d'information entre les différents acteurs est nécessaire.**

- L'objectif est de pouvoir garantir une réponse rapide, adaptée et proportionnée à chaque cas (accompagnement, soutien, suppression ou déréférencement de contenus, action répressive) associant l'Éducation nationale, les associations partenaires, les plateformes de réseaux sociaux ainsi que la protection de l'enfance, les forces de l'ordre et les magistrats ;
- Un circuit d'information précis entre ces acteurs doit être construit sur la base de conventions permettant la prise en charge des situations notamment les plus aiguës voire la mise en place d'un outil de signalement et de suivi partagé des cas individuels sous réserve de conformité aux règles posées par la CNIL en matière de protection des données à caractère personnel, notamment l'exigence de consentement des personnes accompagnées ;
- Des indicateurs de délai, pouvant être rendus publics, entre la prise de contact et les mesures prises par les différents acteurs responsables constitueraient un complément pour garantir une qualité et une célérité dans la réponse apportée.

5. La nécessité de donner une visibilité encore plus forte au phénomène des cyberviolences des jeunes impose de mobiliser largement les pouvoirs publics et la société civile

Ainsi que l'étude d'opinion a pu le démontrer, la conscience du phénomène des cyberviolences est souvent délicate pour les adultes qui entourent les jeunes, notamment leurs parents et leurs professeurs. L'Éducation nationale accentue ses efforts pour sensibiliser les élèves aux cyberviolences et former ses personnels, mais il convient désormais d'étendre cette mobilisation au-delà de l'école.

À cet égard, le dispositif « Grande cause nationale » paraît le plus choisi pour assurer la visibilité sur le phénomène et la mobilisation la plus forte. Il s'agit d'un label officiel attribué par le Premier ministre français à un organisme à but non lucratif ou un collectif d'associations. L'agrément permet, tout au long de l'année, d'organiser des campagnes de générosité publique et de diffuser gratuitement des messages sur les sociétés publiques de télévision et de radio. D'après la circulaire du 20 septembre 2010 qui encadre ce dispositif, « les présidents de ces sociétés déterminent les conditions dans lesquelles ils satisfont à cette obligation ». De plus « *les organismes ayant bénéficié de cette assistance doivent, par la même voie, radiophonique ou télévisée, informer le public du montant des collectes réalisées et de l'affectation des dons* ». À titre d'exemple, le label a été délivré en 2018 et 2019 aux organismes luttant contre les violences faites aux femmes.

Proposition 5 : faire de la lutte contre les cyberviolences des jeunes une « grande cause nationale » pour 2021, susceptible de mobiliser l'ensemble des acteurs responsables

Remonter la lutte contre les cyberviolences en haut de l'agenda politique impose de rechercher une visibilité et de mobiliser l'ensemble des acteurs les plus concernés.

.../...

- **Une campagne de communication et de sensibilisation à forte visibilité serait nécessaire,** relayée par les sociétés publiques de radio et de télévision ainsi que par les plateformes et réseaux sociaux. Celle-ci exposerait la réalité du phénomène, son étendue et ses victimes, en particuliers les jeunes filles et les jeunes LGBT. Elle s'adresserait aux jeunes mais aussi à leurs parents, souvent peu conscients du phénomène et de son acuité. La forme choisie serait percutante, à l'instar des plus récentes campagnes de la sécurité routières, et mobiliserait les leaders d'opinion et égéries des jeunes. Les messages adressés seraient notamment de rappeler qu'Internet n'est pas une zone de non-droit et que l'anonymat peut être levé en ligne, que celui qui relaye est aussi responsable que celui qui commet une cyberviolence. Enfin, cette campagne serait destinée à promouvoir le guichet unique de prise en charge des cyberviolences à l'encontre des jeunes ;
- La mobilisation de l'ensemble des administrations et des acteurs de la société civile devrait être assurée en parallèle. Elle pourrait s'appuyer sur un cadre interministériel de sensibilisation et de formation à la prise en charge des (cyber)violences dont peuvent être victimes les jeunes, construit à partir des plans et mesures d'ores et déjà développés par l'Éducation nationale, le Secrétariat d'État au numérique et le Secrétariat d'État à la protection de l'enfance. Enfin, un parcours de formation serait créé dans l'ensemble des écoles du service public et des cursus préparant à l'exercice de professions au contact des enfants et adolescents (éducateurs sportifs, animateurs de centre de loisir…).

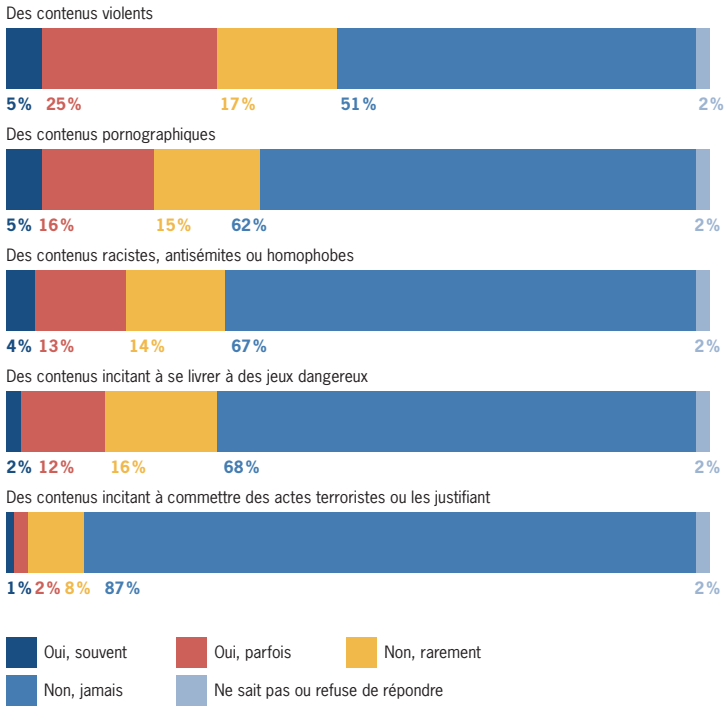
II. B. ACCOMPAGNER : PROTÉGER EFFECTIVEMENT LES JEUNES DES CONTENUS SUSCEPTIBLES DE LES CHOQUER

Ainsi qu'il ressort de l'enquête conduite auprès des jeunes, plus d'un sur deux déclare avoir déjà accédé à un contenu choquant (56 %). Ce type de situation est à distinguer de celui des cyberviolences où la malveillance concerne spécifiquement un jeune ; ici, les contenus en question sont généralement accessibles au public et ne présentent pas de liens avec les données personnelles relatives au jeune qui les consulte.

Parmi les contenus identifiés, il est nécessaire de distinguer plusieurs catégories par gravité décroissante, les enjeux attachés à chacune d'entre elles n'étant pas de même nature :

- **les contenus qui sont par nature illicites,** quel que soit l'âge de l'utilisateur qui les consulte. C'est ainsi le cas pour les contenus racistes, antisémites ou homophobes, de même que ceux incitant à commettre des actes terroristes ou les justifiant. Il peut aussi s'agir de certains contenus violents ;
- **les contenus qui sont interdits aux utilisateurs mineurs** et dont l'accès peut être insuffisamment protégé ou contrôlé. Sont concernés les contenus violents et pornographiques ;
- **les contenus qui, ni illicites ni réservés aux adultes, contribuent à favoriser des comportements dangereux** pour les mineurs. L'incitation à se livrer à des jeux dangereux est ici principalement visée.

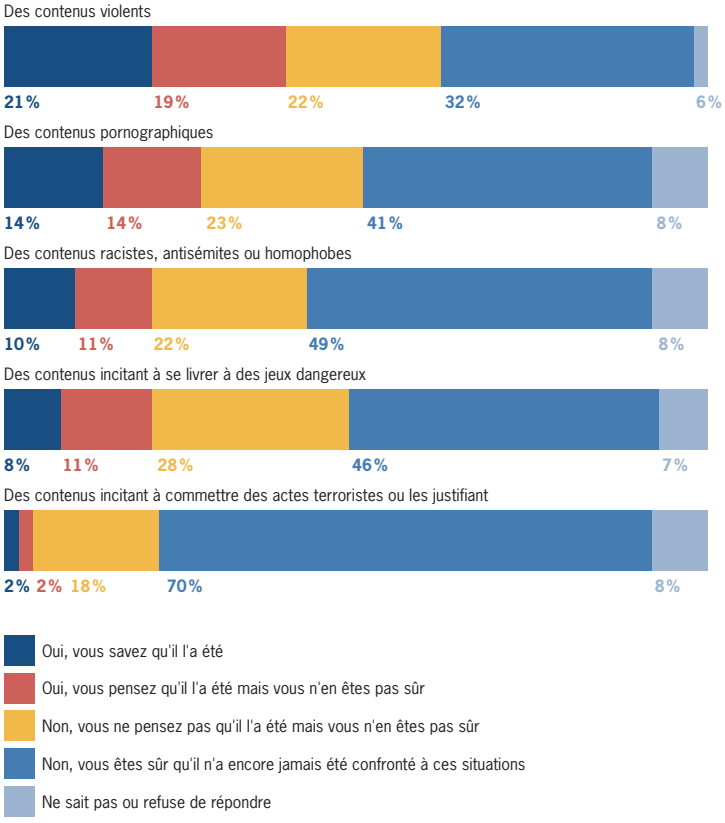
Part de jeunes déclarant avoir été confrontés à un contenu choquant



- Les parents sondés ont tendance à sous-estimer légèrement ce phénomène. 40 % des parents pensent que leur enfant a déjà été exposé à des contenus violents alors que 47 % des jeunes déclarent l'avoir été au moins une fois. Ils sont 28 % à le penser à propos des contenus pornographiques (contre 36 % des jeunes qui déclarent l'avoir été au moins une fois), 21 % pour les contenus racistes, antisémites ou homophobes (contre 31 % des jeunes qui déclarent l'avoir été au moins une fois), 19 % s'agissant des contenus incitant à se livrer

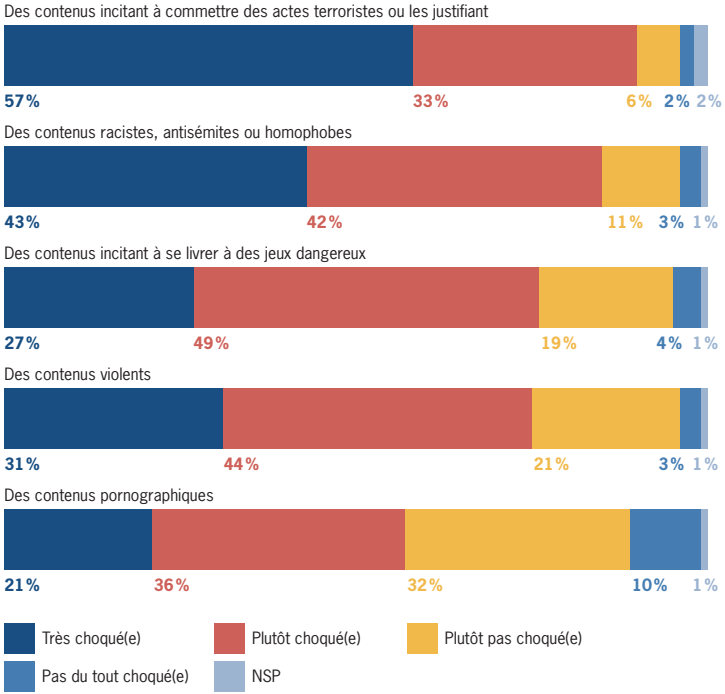
à des jeux dangereux (contre 30 % des jeunes qui déclarent l'avoir été au moins une fois).

Degré de connaissance par les parents de la confrontation de leur enfant à un contenu choquant

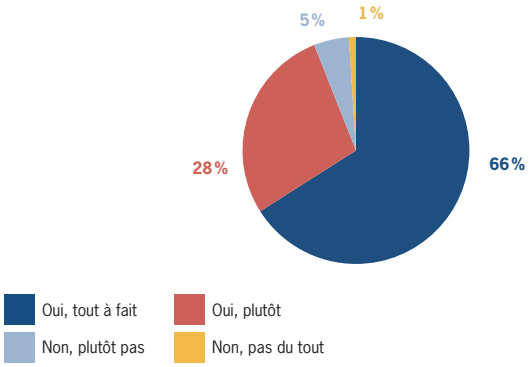


L'enquête conduite auprès des jeunes montre aussi qu'ils savent prendre une distance critique avec ces contenus et se déclarent majoritairement choqués par leur consultation, en particulier pour les contenus illicites. Si l'effet « choc » diminue avec l'âge, ces données viennent nuancer l'idée d'une jeunesse sans repère, qui aurait intégré la violence à force d'y être confrontée. Les jeunes expriment aussi clairement dans le cadre de cette étude leur souhait que les contenus choquants en ligne fassent l'objet d'un encadrement plus prononcé : ils sont 94 % à le penser !

Réactions suscitées chez les jeunes après consultation de contenus choquants



Réponses des jeunes à la question de savoir si l'accès aux contenus choquants en ligne devrait être davantage encadré



Ce constat peut apparaître rassurant. Pour autant, l'accès massif des jeunes générations aux images et aux contenus choquants doit constituer une préoccupation pour les pouvoirs publics, en raison des conséquences du phénomène.

- Les contenus incitant à se livrer à des jeux dangereux peuvent conduire jusqu'au décès de jeunes adolescents (Blue Whale Challenge en 2017, Momo challenge en 2018…) et contribuent plus généralement à accroître les formes de violence ;
- La pornographie peut conduire à des représentations dégradées du corps féminin et par la suite à des comportements violents.

1. Plusieurs travaux académiques ont mis en exergue l'impact de la consultation des images choquantes sur les jeunes générations

C'est le cas du rapport *Comprendre le rôle des images dans la construction identitaire et les vulnérabilités de certains jeunes*, publié en 2017 par Sophie Jehel, maîtresse de conférences à l'Université Paris 8. Il s'agit d'une enquête

auprès d'adolescents de 15 à 18 ans issus de milieux socio-culturels très différents. **L'auteur montre que la confrontation avec les images violentes, sexuelles ou haineuses constitue un choc culturel** « *pour tous les adolescents, au sens d'un écartèlement entre les normes de parité et de pacification des mœurs (interdiction des violences sexuelles, et des violences intrafamiliales) et un univers numérique dérégulé, facilitant l'accès à des représentations sexuelles qui s'y opposent et facilitant la montée en agressivité des échanges* »[33]. L'auteur montre que le milieu d'origine ou le prisme religieux ont un impact majeur sur les stratégies développées par les adolescents. L'enquête conduit à identifier quatre types d'attitudes face à ces images : l'adhésion ; l'indifférence ; l'évitement ; l'autonomie.

D'autres travaux ont montré le rôle des images choquantes dans les processus de manipulation et de radicalisation.

- Dans son ouvrage *La pensée extrême. Comment des hommes ordinaires deviennent des fanatiques*, publié en 2009, Gérald Bronner détaille le **cheminement incrémental pouvant conduire une personne à se radicaliser**[34]. L'un des aspects de ce cheminement consiste à enfermer l'individu dans une forme « d'oligopole cognitif », c'est-à-dire à restreindre son champ d'information pour emporter son adhésion. L'auteur mentionne le cas de Dylann Roof, un jeune homme raciste ayant tué neuf personnes dans l'église de Charleston en juin 2015. La radicalisation de cet individu s'est produite sur Internet, lorsqu'il a mené des recherches pour identifier les meurtres de personnes de peau blanche par des personnes de peau noire : en consultant le premier site Internet proposé par Google, c'est-à-dire la page du Council of Conservative Citizens, il a été volontairement confronté à des contenus choquants qui ont emporté son indignation et, par là, sa radicalisation violente ;

33 Jehel, Sophie, *Les adolescents face aux images violentes, sexuelles et haineuses : stratégies, vulnérabilités, remédiations. Comprendre le rôle des images dans la construction identitaire et les vulnérabilités de certains jeunes*, Misson de Recherche Droit et Justice, avril 2019, p. 189.

34 Bronner, Gérard, *La pensée extrême. Comment des hommes ordinaires deviennent des fanatiques*, Paris, Denoël, 2009.

- L'étude menée par Anne Muxel et Olivier Galland auprès de 7000 lycéens et restituée dans l'ouvrage *La tentation radicale* publié en 2018 a notamment analysé l'**impact des théories du complot et de la radicalité informationnelle sur les jeunes**[35]. Il est notamment relevé que *« l'émergence d'une véritable radicalité informationnelle »* concerne 9 % des lycéens, laquelle se traduit notamment par une participation active de rediffusion et de partage des contenus choquants permettant de susciter une adhésion à des thèses extrêmes ou complotistes.

2. Les réponses apportées s'agissant des contenus illicites relèvent du domaine pénal et dépassent très largement la spécificité du jeune public

Conformément aux dispositions de la directive européenne 2000/31 sur le commerce électronique[36], seuls les contenus faisant l'apologie du terrorisme, ou les contenus pédopornographiques, peuvent donner lieu à des retraits administratifs de contenus ou des blocages administratifs de sites ainsi qu'à des sanctions pénales.

Le dispositif mis en œuvre en France repose sur des solutions graduées relevant de l'OCLCTIC et qui concerne un champ plus étendu de contenus :

- un signalement en tout premier lieu (cf. partie II sur les cyberviolences) ;
- une mesure de retrait administratif ;
- une notification des adresses électroniques rendant accessibles les contenus incriminés en cas de non-exécution de la mesure de retrait (déréférencement).

35 Galland Olivier et Muxel Anne, *La tentation radicale. Enquête auprès des lycéens*, PUF, 2018.
36 Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur.

L'encadrement des contenus faisant l'apologie du terrorisme et des contenus pédopornographiques

Le cadre européen

La directive 2011/93 du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie, harmonise dans l'Union européenne les infractions pénales relatives aux abus sexuels commis contre des enfants. L'extrême gravité des crimes en cause et leur caractère universellement condamnables justifient l'interdiction expresse dont ils font l'objet sur Internet.

L'article 25§1 de la directive impose aux États membres de prendre les mesures nécessaires pour faire rapidement supprimer les pages Internet contenant de la pédopornographie lorsqu'elles sont hébergées sur leur territoire. Lorsqu'elles ne le sont pas, la directive dit que les États membres « s'efforcent » d'en obtenir la suppression. Celle-ci étant souvent difficile à obtenir, faute de coopération de la part des autorités publiques de l'État dans lequel les serveurs sont hébergés ou du fait de procédures longues et peu efficaces, l'article 25§2 laisse, en outre, la faculté aux États membres d'instaurer des mesures de blocage de l'accès par les internautes sur leur territoire aux sites contenant de la pédopornographie. Il est précisé que ces mesures doivent être établies en vertu de procédures transparentes et fournir des garanties suffisantes, et en particulier éviter que ces restrictions n'aillent au-delà de ce qui est nécessaire.

.../...

Le cadre français

La loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique prévoyait déjà une possibilité de blocage décidée par l'autorité judiciaire en matière civile. La loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme, a également prévu une mesure de blocage en matière pénale lorsque les faits *« constituent un trouble manifestement illicite, à la demande du ministère public ou de toute personne physique ou morale ayant intérêt à agir »*.

Pourtant propre à la matière terroriste, ce référé pénal n'a pas été jugé suffisant. Le blocage administratif mis en place s'est inséré dans une procédure déjà existante de signalement et de retrait, destinée à assainir les sites Internet de leurs contenus illicites. L'OCLCTIC est alors compétent : il s'agit de l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication.

Plusieurs mesures graduelles sont prévues mais ne concernent pas toutes le même champ de contenus.

La première mesure consiste en une procédure de signalement. Si les FAI et les hébergeurs ne sont pas soumis à une obligation générale de surveiller les informations qu'ils transmettent ou qu'ils stockent, ni à une obligation générale de rechercher des faits ou des circonstances révélant des activités illicites, ils doivent en revanche :

- mettre en place un dispositif facilement accessible et visible permettant à toute personne de porter à leur connaissance ce type de donnée ;
- informer promptement les autorités publiques compétentes de toutes activités illicites qui leur seraient signalées et qu'exerceraient les destinataires de leurs services ;
- rendre publics les moyens qu'ils consacrent à la lutte contre les activités illicites.

.../...

Les contenus visés sont l'apologie des crimes contre l'humanité, la provocation à la commission d'actes de terrorisme et leur apologie, l'incitation à la haine raciale, à la haine à l'égard de personnes à raison de leur sexe, de leur orientation ou identité sexuelle ou de leur handicap, la pornographie enfantine, l'incitation à la violence, notamment l'incitation aux violences faites aux femmes, ainsi que les atteintes à la dignité humaine.

La procédure de retrait se veut plus impérative, du moins quant à l'objectif poursuivi, à savoir la disparition du contenu entaché d'illicéité. Lorsque les nécessités de la lutte contre la provocation à des actes terroristes ou l'apologie de tels actes ou contre la diffusion des images ou des représentations de mineurs le justifient :

- l'autorité administrative peut demander à l'éditeur ou à l'hébergeur de retirer les contenus qui contreviennent aux dispositions du code pénal et elle en informe simultanément les FAI ;
- l'éditeur et l'hébergeur disposent d'un délai de vingt-quatre heures pour procéder au retrait.

Ce dispositif est plus limité dans son champ d'application que celui concernant la procédure de signalement. Outre le terrorisme, seule est concernée la diffusion d'images ou de représentations pornographiques de mineurs. Il en est de même de l'étape qui suit, à savoir le blocage proprement dit.

En l'absence de retrait, par l'éditeur ou l'hébergeur, des contenus illicites dans un délai de vingt-quatre heures, l'autorité administrative peut notifier aux FAI la liste des adresses électroniques des services de communication au public en ligne contrevenant aux dispositions du code pénal (déréférencement). Ces personnes doivent alors empêcher sans délai l'accès à ces adresses. L'autorité administrative peut également notifier les adresses électroniques aux moteurs de recherche ou aux annuaires, qui prennent toute mesure utile destinée à faire cesser le référencement du service de communication au public en ligne.

Il est confié à une personnalité qualifiée, désignée par la CNIL, pour une durée de trois ans non renouvelable, **la mission de vérifier au préalable que les contenus dont l'autorité administrative demande le retrait ou que les sites dont elle ordonne le blocage sont bien contraires aux dispositions du code pénal** sanctionnant la provocation au terrorisme, l'apologie du terrorisme ou la diffusion d'images pédopornographiques. Si elle constate une irrégularité, elle peut à tout moment recommander à l'autorité administrative d'y mettre fin. Si l'autorité administrative ne suit pas cette recommandation, la personnalité qualifiée peut saisir la juridiction administrative compétente, en référé ou sur requête. Le 4e rapport de la personnalité qualifiée de la CNIL a été présenté pour la période du 1er mars 2018 au 1er février 2019. Celui-ci a reçu 25 474 demandes (- 34 %) de l'OCLCTIC dont : 879 demandes de blocages de sites (+ 15 %) ; 18 014 demandes de retrait de contenus (- 48 %) ; 6 581 demandes de déréférencement d'adresses électroniques (+ 111 %).

3. La limitation de l'exposition des jeunes aux contenus réservés aux adultes demeure largement inefficace

Des initiatives ont récemment été prises pour mieux contrôler l'accès des jeunes aux contenus choquants, notamment pornographiques.

C'est le cas des plateformes elles-mêmes qui renforcent leurs politiques internes de protection de la jeunesse et collaborent plus étroitement avec les autorités (cf. partie II relative aux cyberviolences). Certaines solutions de contrôle parental et d'accès spécifiques sont également développées par les plateformes, à l'instar de ce qui est fait par Google. Toutefois, **ces solutions demeurent souvent dépendantes d'un écosystème d'applications et ne permettent pas de proposer un contrôle parental pour l'ensemble des applications tierces.**

Les solutions de contrôle parental et d'accès spécifique développées par Google

Deux solutions de contrôle parental ont été construites :

- **SafeSearch** est une fonctionnalité proposée depuis 2015 qui, lorsqu'elle est activée, filtre les images, vidéos et sites Web explicites dans les résultats de recherche Google. Cet outil est conçu pour bloquer l'affichage de ce type de contenus, notamment ceux à caractère pornographique. Il est possible d'activer SafeSearch notamment pour les comptes personnels et navigateurs ainsi que pour les appareils et réseaux professionnels ou scolaires.
- **Family Link** est une application offerte depuis 2018 qui permet aux parents de jeunes enfants ou d'adolescents d'établir des règles concernant l'utilisation des appareils numériques et de les accompagner dans l'ensemble de leurs activités, en particulier en ligne. Cet outil présente de multiples fonctionnalités pouvant être activées :
  - L'approbation de téléchargements et d'achats effectués par l'enfant sur Google Play, la limitation des contenus accessibles dans le Store en fonction de la classification par âge minimal ;
  - La gestion des paramètres tels que SafeSearch pour la recherche Google ;
  - La gestion des autorisations au sein des applications acceptées par l'enfant (accès au micro, à l'appareil photo, à la position géographique et aux contacts) ;
  - La modification du filtre de contenu paramétré pour l'application YouTube Kids ;
  - La définition de durées limites d'utilisation sur les appareils Android ou Chrome OS de l'enfant ;
  - La visualisation de la position géographique des appareils Android ou Chrome OS de l'enfant ;

.../...

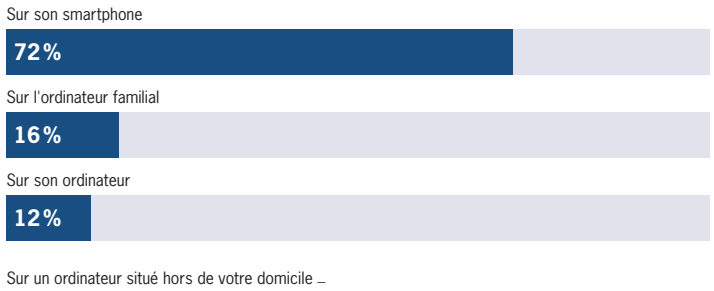
- La gestion des paramètres d'activité du compte Google de l'enfant ;
- La délégation des droits de supervision à un autre membre de la famille.

Par ailleurs, un accès spécifique à une partie des vidéos présentes sur la plateforme YouTube est prévu à destination des jeunes via la plateforme YouTube Kids. Ne sont présentes sur cette dernière que les vidéos approuvées pour un public jeune.

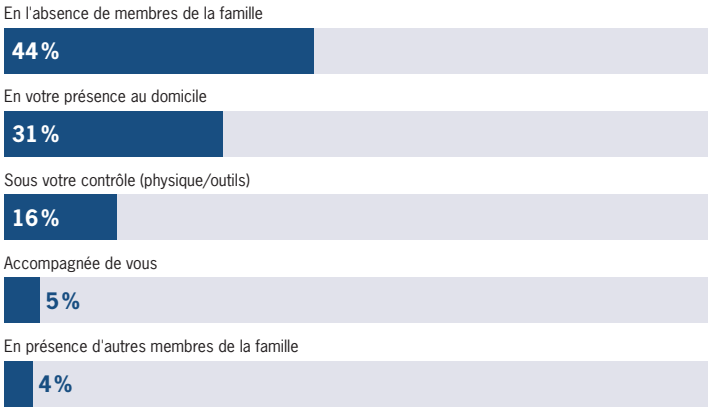
Ce type d'outils apparaît souhaitable même si l'étude d'opinion conduite auprès des parents de jeunes a aussi permis d'observer que ceux-ci privilégient plutôt des mesures nécessitant un contrôle pouvant être plus physique que numérique : limitation des plages horaires d'accès à Internet, contrôle de l'historique de navigation, sans garantie forte d'efficacité. Plus encore, les jeunes naviguent désormais sur Internet et sur les réseaux sociaux à partir de leur smartphone personnel, et non plus l'ordinateur familial. Ils sont aussi une majorité à le faire en dehors de la supervision de leur parents.

Mesures prises par les parents pour contrôler l'activité de leur enfant en ligne

Principal support utilisé par les enfants, selon leurs parents, pour aller sur Internet/les réseaux sociaux



Autonomie des jeunes dans leur navigation sur Internet et sur les réseaux sociaux, selon leurs parents



Certains États eux-mêmes tentent d'imposer des mesures plus fortes pour restreindre l'accès des mineurs à des contenus qui leur sont interdits, **avec des résultats qui demeurent encore en-deçà des attentes.**

C'est le cas du Royaume-Uni qui souhaitait dès la fin de l'année 2017 imposer aux internautes britanniques de devoir apporter la preuve de leur majorité par l'intermédiaire d'un document d'identité, d'un téléphone mobile ou via l'achat d'une carte d'accès dans un magasin physique. Ces nouvelles règles devaient s'appliquer aux plateformes offrant plus d'un tiers de contenu « pour adultes » et qui génèrent des revenus par la publicité ou des abonnements. Toutefois, le Royaume-Uni a été contraint d'abandonner ce projet dès l'automne 2019 en raison de critiques multiples portant sur l'atteinte forte à la vie privée et à une mise en œuvre très difficile du contrôle de l'âge en pratique.

En France, le Président de la République a posé l'exigence aux opérateurs de mettre en place sous six mois « le contrôle parental par défaut » à l'occasion de son discours à l'UNESCO du 20 novembre 2019 contre les violences faites aux

plus jeunes lors de la Journée internationale des droits de l'enfant. Plusieurs associations familiales et de protection de l'enfance ainsi que les régulateurs (ARCEP et CSA) et les professionnels du numérique (opérateurs, FAI, moteurs de recherche, éditeurs, plateformes) ont signé début 2020 un « protocole d'engagements pour la prévention de l'exposition des mineurs aux contenus pornographiques en ligne ».

Proposition 6 : rendre plus effective la protection des jeunes vis-à-vis des contenus réservés aux adultes susceptibles de les choquer, s'appuyant sur le rôle essentiel de leurs parents

À cette fin, un cadre clair et des dispositifs techniques simples sont nécessaires.

- **Des lignes directrices détaillées portant sur les modalités d'encadrement de l'accès** aux sites et applications comprenant des contenus réservés aux adultes doivent être établis à destination de ceux qui les produisent et les diffusent, en s'appuyant en particulier sur l'expertise du CSA en cette matière et sur les premiers engagements pris avec la signature du protocole d'engagements ;
- **La mise à disposition de dispositifs techniques clairs et respectueux de la vie privée** conditionne la possibilité de protéger la jeunesse en ligne. Dans cette mesure, il paraîtrait nécessaire d'étudier la faisabilité d'un dispositif de vérification de l'âge à l'achat entraînant un paramétrage non modifiable du système d'exploitation du *smartphone*, de la tablette ou de l'ordinateur bloquant l'accès aux sites Internet et contenus réservés au public majeur. Ce type de dispositif éviterait la transmission d'informations personnelles aux acteurs du numérique qui constitue précisément une des raisons des difficultés rencontrées au Royaume-Uni. En outre, des API *(Application Programming Interfaces)* pourraient être envisagées pour filtrer des contenus réservés aux adultes.

4. Mieux accompagner les jeunes et mieux prendre en charge la souffrance en cas de consultation d'images choquantes

Parallèlement à la question de l'accès aux images choquantes, un autre enjeu concerne l'accompagnement des jeunes dans leur apprentissage numérique. Il s'agit ici d'anticiper les situations où ils seraient confrontés à des images choquantes. Deux axes de réponse se dégagent : la prise de distance et le dialogue.

Cet enjeu est déjà largement identifié par les pouvoirs publics, même si de nombreux progrès peuvent encore être accomplis pour connaître l'impact des images choquantes sur les jeunes :

- Dans le cadre de l'éducation à la sexualité, dispensée à tous les niveaux de la scolarité à raison de trois séances annuelles, l'Éducation nationale insiste sur les risques d'une exposition aux images pornographiques. Cela permet aussi aux jeunes d'obtenir des réponses à certaines de leurs questions directement par des adultes formés à cet effet plutôt que de consulter des sites Internet dont le sérieux n'est pas garanti. Cette vigilance s'articule avec la lutte contre les violences sexuelles, les préjugés sexistes ou homophobes et la promotion du respect mutuel et de l'égalité entre les sexes. Mais en pratique, la mise en œuvre des trois séances annuelles d'éducation à la sexualité est hétérogène.
- À l'automne 2019, le CSA a diffusé, comme chaque année, une campagne sur le malaise des jeunes qui ont visionné des images choquantes. Le slogan est explicite « les images choquantes il faut les éviter, sinon il faut en parler » et la campagne invite au dialogue préventif entre parents et enfants et plus largement au dialogue pour aider à prendre de la distance avec les images visionnées.

Proposition 7 : mieux connaître les effets des contenus choquants sur les jeunes

Pour ce faire :

- **Le développement de la recherche médicale et en sciences humaines** est nécessaire, en s'appuyant sur les programmes de recherche nationaux et européens pouvant offrir un soutien financier à cet égard et en lien avec les travaux du Centre national de ressources et de résilience portant sur les psychotrauma ;
- **La réalisation d'une évaluation détaillée,** sur la base d'indicateurs établis par un comité d'experts indépendants, **de l'éducation à la sexualité** assurée par l'éducation nationale constituerait une perspective utile, en veillant à mesurer en particulier la prise en compte de l'expérience des jeunes sur Internet et sur les réseaux sociaux.

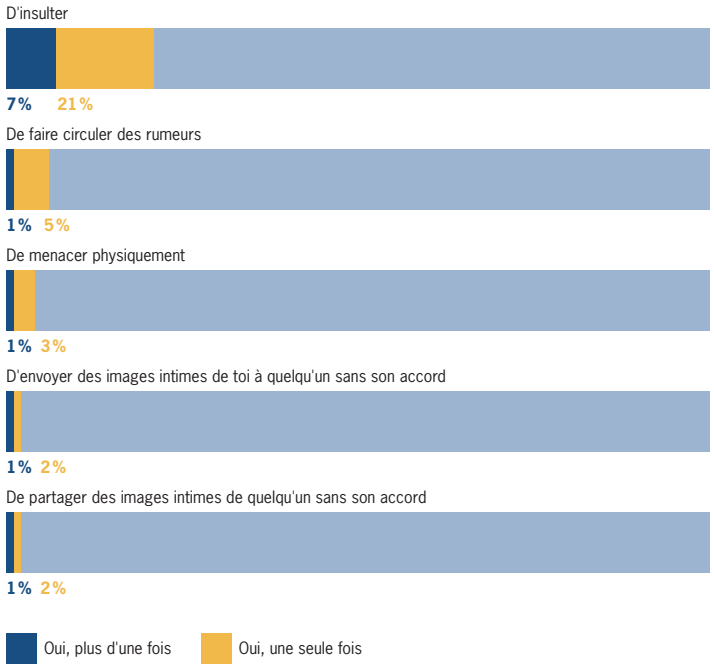
III. RESPONSABILISER LES JEUNES AINSI QUE LES ENTREPRISES QUI GÈRENT LES RÉSEAUX SOCIAUX

III. A. RESPONSABILISER : FAIRE DES JEUNES DES INDIVIDUS RESPONSABLES EN LIGNE

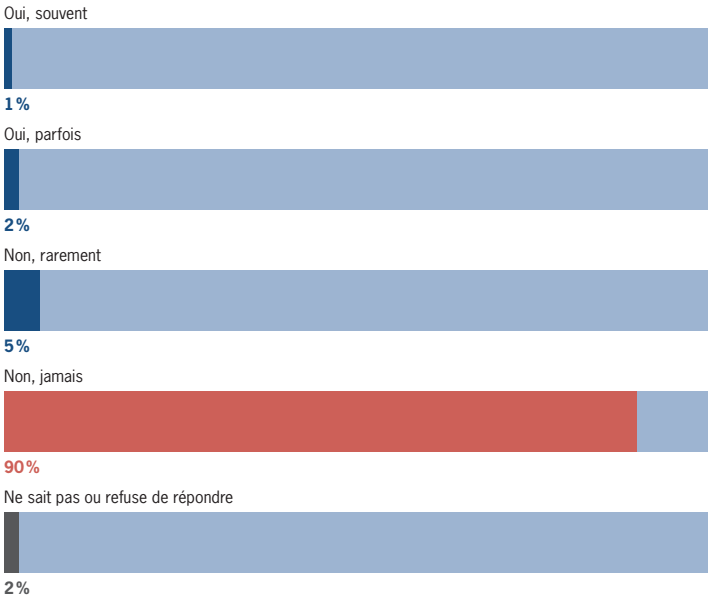
Former les jeunes à protéger leur vie privée en ligne et à faire preuve de recul par rapport aux informations qu'ils consultent, les aider et les accompagner lorsqu'ils sont victimes de cyberviolences ou confrontés à des contenus choquants sont deux dimensions essentielles pour aider les jeunes à grandir et acquérir une maturité numérique.

L'enquête d'opinion réalisée pour cette étude a permis de souligner que **les jeunes peuvent aussi être auteurs d'actes qui causent des torts à d'autres personnes en ligne.** 21 % des jeunes interrogés déclarent ainsi avoir déjà insulté d'autres personnes en ligne. De manière bien plus réduite, ils sont 6 % à avoir fait circuler des rumeurs, 4 % à avoir menacé d'autres personnes physiquement et 3 % à avoir partagé des images intimes d'une personne sans son accord.

Part de jeunes ayant déjà commis des cyberviolences en ligne

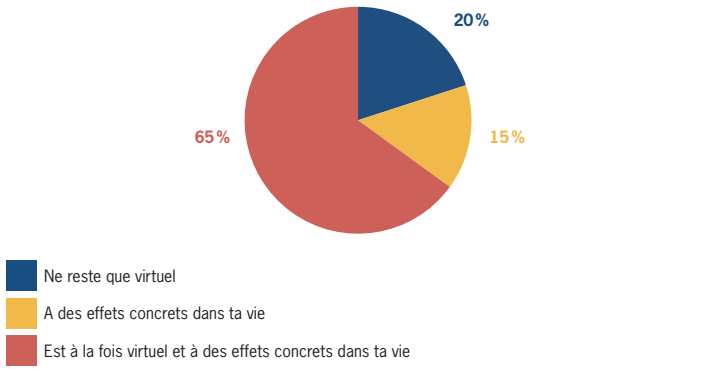


Part de jeunes ayant déjà écrit de fausses informations en ligne



L'ampleur du phénomène des cyberviolences (cf. partie II) apparaît donc aussi liée aux comportements de certains jeunes eux-mêmes. Par ailleurs, une part certainement plus importante de jeunes contribuent à renforcer les actes malveillants commis par d'autres en s'en faisant les relais : « liker » une publication, consulter une vidéo, réagir, rediffuser sont autant d'actions qui peuvent donner un écho considérable à un acte de cyberviolence. **Il apparaît donc essentiel que les jeunes puissent réaliser que celui qui consulte ou diffuse peut se faire le complice de l'auteur d'un acte malveillant.**

Regard porté par les jeunes sur l'impact de leur activité en ligne



Responsabiliser les jeunes constitue donc également une dimension à prendre en compte pour les aider à faire un usage responsable d'Internet et des réseaux sociaux.

1. Dans le champ scolaire, des premières initiatives sont conduites pour responsabiliser davantage les jeunes auteurs de (cyber) violences à l'encontre de leurs camarades

Les dix nouvelles mesures pour lutter contre le harcèlement entre élèves présentées par le ministre Jean-Michel Blanquer en 2019 intègrent des méthodes de traitement du harcèlement scolaire qui ont démontré leurs effets à l'étranger, en particulier le programme finlandais KiVa (voir encadré). L'objectif recherché est de permettre une prise de parole des jeunes et une logique de témoignage de l'ensemble des parties prenantes d'une situation de (cyber)violence.

Le focus groupe réalisé avec des parents a d'ailleurs confirmé que, dans plusieurs des cas rapportés par les participants, une action rapide associant les

adultes (parents, professeurs) ainsi que les jeunes tant victime, auteurs que témoins permettait la plupart du temps de faire cesser une situation pouvant s'aggraver. Cela suppose que les parents soient pleinement conscients des enjeux en matière de cyberviolence. Cette dimension peut être encore renforcée dans les différentes initiatives d'accompagnement à la parentalité, en articulation avec des acteurs qui œuvrent localement pour la diffusion de la culture numérique.

La méthode KiVa

KiVa est le nom d'un programme de lutte contre le harcèlement en milieu scolaire en Finlande. Il a été mis au point à l'Université de Turku.

Ce programme comprend à la fois des actions ciblées et d'autres d'ordre plus général, destinées tant à prévenir le phénomène qu'à traiter les cas de harcèlement relevés dans les établissements. Les actions générales s'adressent à tous les élèves d'une même école. Elles consistent en un certain nombre d'initiatives :

- **Des jeux de rôle :** dès la maternelle, les élèves apprennent à se mettre dans la peau de la victime, de l'agresseur et du témoin. L'objectif est ainsi de développer respectivement l'empathie, apprendre la responsabilisation et encourager à témoigner auprès des professeurs.
- **La confrontation :** lorsqu'il y a eu une agression, les professeurs organisent un dialogue entre la victime et l'auteur afin que la victime soit écoutée et que l'agresseur soit confronté à la parole d'un adulte ;
- **Des films et des jeux vidéo :** de nombreuses formes ludiques sont mises en place pour évoquer les intimidations et autres brimades ou encore les agressions verbales et physiques ainsi que le cyberharcèlement. Durant une dizaine de séances, à raison d'une par mois environ, les élèves sont amenés à regarder des courts-métrages et à jouer à des jeux vidéo qui évoquent le harcèlement.

.../...

L'efficacité de ce programme a été démontré par une étude contrôlée, réalisée de manière aléatoire et à grande échelle avec 117 écoles où il a été appliqué et 117 autres où il ne l'a pas été, constituant le groupe de contrôle. Il a été prouvé que son mode d'action réduisait de manière significative le nombre des cas de harcèlement et de victimisation rapportés par les victimes elles-mêmes ou par d'autres élèves. 85 % des cas de harcèlement ont été résolus.

Par ailleurs, ainsi qu'il a déjà été rappelé dans la partie II du présent rapport, le code de l'éducation a été enrichi dès 2019 pour inclure la lutte contre les phénomènes d'intimidation et de harcèlement parmi les objectifs de l'école. Pour mémoire, le nouvel article L. 511-3-1 du code de l'éducation dispose qu'*« aucun élève ne doit subir, de la part d'autres élèves, des faits de harcèlement ayant pour objet ou pour effet une dégradation de ses conditions d'apprentissage susceptible de porter atteinte à ses droits et à sa dignité ou d'altérer sa santé physique ou mentale »*.

Ces évolutions sont encore très récentes et il conviendra d'en analyser précisément les résultats avec un recul nécessaire, en particulier en vue de les amplifier si elles portent leurs fruits. De l'avis de plusieurs des interlocuteurs rencontrés, une prise en compte du phénomène dans un cadre scolaire est la réponse la plus adaptée pour permettre une responsabilisation des jeunes.

Le code de l'éducation prévoit par ailleurs, de manière plus générale, des mesures de responsabilisation des jeunes qui doivent être inscrites dans le règlement intérieur de chaque établissement :

- des mesures destinées à prévenir un acte répréhensible. Il s'agit notamment de la confiscation d'objets dangereux ou interdits dans l'établissement pouvant être décidée par un enseignant ou un personnel de l'établissement ;
- des mesures temporaires, dont le but est de garantir l'ordre au sein de l'établissement en cas de procédure disciplinaire engagée contre un élève et qui lui interdisent l'accès à l'établissement pendant une durée de 2 jours minimum,

ou jusqu'à la date du conseil de discipline, si celui-ci est saisi ;

- des sanctions, inscrites au dossier scolaire et qui punissent un manquement grave ou répété aux obligations de l'élève, notamment des atteintes aux personnes, sous la forme de violences verbales ou physiques par exemple (articles R. 511-12 à R. 511-19). Ces sanctions, décidées par le chef d'établissement ou le conseil d'établissement, sont de plusieurs types en fonction de la gravité :
  - l'avertissement ;
  - le blâme, sous la forme d'un rappel à l'ordre écrit et solennel ;
  - la mesure de responsabilisation, sous la forme d'activités éducatives, culturelles, de solidarité, de formation en dehors des heures d'enseignement, dans l'établissement ou à l'extérieur - 20 heures maximum, possiblement comme solution alternative à une exclusion temporaire ;
  - l'exclusion temporaire de la classe pour 8 jours au maximum ;
  - l'exclusion temporaire de l'établissement pour 8 jours au maximum avec information au maire de la commune du domicile de l'élève ;
  - l'exclusion définitive de l'établissement.

2. Le traitement des cyberviolences des jeunes repose principalement sur des dispositions pénales difficiles à mettre en œuvre et peu adaptées

1/ Le traitement pénal du harcèlement représente la principale réponse apportée

D'un point de vue pénal, depuis 2018, **le harcèlement** est un délit qui se définit à l'article 222-33-2-2 du code pénal comme le fait d'imposer à une personne de façon répétée certains propos ou comportements qui portent atteinte à son intégrité physique ou psychique. Cette définition se retrouve également pour deux catégories de harcèlement spécifiques prévues par le code pénal que sont le harcèlement sexuel (article 222-33) et le harcèlement moral dans un cadre professionnel (article 222-33-2 et suivants).

Définition du délit de harcèlement (article 222-33-2-2 du code pénal)

Le fait de harceler une personne par des propos ou comportements répétés ayant pour objet ou pour effet une dégradation de ses conditions de vie se traduisant par une altération de sa santé physique ou mentale est puni d'un an d'emprisonnement et de 15 000 € d'amende lorsque ces faits ont causé une incapacité totale de travail inférieur ou égale à huit jours ou n'ont entraîné aucune incapacité de travail.

L'infraction est également constituée :

a) Lorsque ces propos ou comportements sont imposés à une même victime par plusieurs personnes, de manière concertée ou à l'instigation de l'une d'elles, alors même que chacune de ces personnes n'a pas agi de façon répétée ;

b) Lorsque ces propos ou comportements sont imposés à une même victime, successivement, par plusieurs personnes qui, même en l'absence de concertation, savent que ces propos ou comportements caractérisent une répétition.

Les faits mentionnés aux premier à quatrième alinéas sont punis de deux ans d'emprisonnement et de 30 000 € d'amende :

1° Lorsqu'ils ont causé une incapacité totale de travail supérieur à huit jours ;

2° Lorsqu'ils ont été commis sur un mineur de quinze ans ;

3° Lorsqu'ils ont été commis sur une personne dont la particulière vulnérabilité, due à son âge, à une maladie, à une infirmité, à une déficience physique ou psychique ou à un état de grossesse, est apparente ou connue de leur auteur ;

4° Lorsqu'ils ont été commis par l'utilisation d'un service de communication au public en ligne ou par le biais d'un support numérique ou électronique ;

5° Lorsqu'un mineur était présent et y a assisté.

.../...

> Les faits mentionnés aux premier à quatrième alinéas sont punis de trois ans d'emprisonnement et de 45 000 € d'amende lorsqu'ils sont commis dans deux des circonstances mentionnées aux 1° à 5°.

Cette disposition du code pénal permet donc bien de sanctionner des comportements qui, bien que de niveau faible, constituent une violence portant atteinte à l'intégrité physique et psychique de la victime en raison de leur caractère répété. Ce délit permet en outre de faciliter la sanction de comportements dont la preuve est souvent difficile à apporter isolément : atteinte à la vie privée, *revenge porn*, diffamation, vol de données personnelles, usurpation d'identité numérique, c'est-à-dire l'ensemble des (cyber)violences testées dans le cadre de l'enquête d'opinion.

Il apparaît, à la lecture des dispositions en question, qu'il n'existe pas de définition autonome du cyberharcèlement d'un point de vue pénal, la dimension numérique d'un harcèlement constituant en réalité une circonstance aggravante en raison de l'effet amplificateur du vecteur numérique. Les éléments constitutifs de l'infraction permettent donc d'appréhender le cyberharcèlement de manière large, c'est-à-dire lorsque celui-ci est commis par une seule personne de manière répétée mais aussi lorsque plusieurs personnes y contribuent en parallèle, ce qui confirme la sensibilisation particulière des jeunes qui relaient des contenus sans en être les créateurs :

- les propos ou comportements imposés à une même victime par plusieurs personnes, de manière concertée ou à l'instigation de l'une d'elles, alors même que chacune n'a pas agi de façon répétée ;
- les propos ou comportements imposés à une même victime, successivement, par plusieurs personnes qui, même en l'absence de concertation, savent que ces propos ou comportements caractérisent une répétition.

En outre, il n'existe pas non plus de dispositions spécifiques aux jeunes. L'article 222-33-2-2 du code pénal prévoit l'existence de circonstances aggravantes lorsque la victime est âgée de quinze ans ou moins – en raison de la particulière vulnérabilité de cette victime – de même que lorsque des témoins mineurs sont

présents ou assistent aux faits de harcèlement. Si l'une de ces circonstances est caractérisée, les peines prononcées sont portées à deux ans d'emprisonnement et 30 000 € d'amende contre un an d'emprisonnement et 15 000 € d'amende et, lorsque les deux circonstances sont présentes, les peines sont portées à quatre ans d'emprisonnement et 45 000 € d'amende.

On trouve toutefois peu de cas d'application de ces dispositions, même s'agissant de victimes majeures. Cela tient en premier lieu au dépôt de plainte qui implique la présence d'un parent si la victime est mineure et qui s'inscrit dans un cadre de prise en charge qui n'est pas suffisamment clair (cf. partie II sur la prise en charge des jeunes victimes de cyberviolences). En outre, les preuves des actes de harcèlement et de leurs conséquences néfastes sur les conditions de vie mais surtout de l'identité du harceleur ne sont pas simples à rapporter.

2/ D'autres dispositions existent également mais présentent les mêmes limites

Le code pénal prévoit :

- **un délit de diffusion de contenus intimes :** l'article 226-2-1, alinéa 2 prévoit une peine de deux ans d'emprisonnement et de 60 000 € d'amende pour « le fait, en l'absence d'accord de la personne pour la diffusion, de porter à la connaissance du public ou d'un tiers tout enregistrement ou tout document portant sur des paroles ou des images présentant un caractère sexuel, obtenu, avec le consentement exprès ou présumé de la personne ou par elle-même » ;
- **un délit d'usurpation d'identité, y compris sur Internet,** qui est puni d'une peine d'un an de prison et de 15 000 € d'amende aux termes de l'article 226-4-1 ;
- **un délit de diffusion de contenu à caractère pornographique d'un mineur** puni d'une peine de cinq ans de prison et de 75 000 € d'amende (article 227-23) ;
- **un délit pour la diffusion de contenus choquants** prévu à l'article 227-24 du code pénal qui prévoit une peine de trois ans d'emprisonnement et de 75 000 € d'amende notamment pour ceux qui diffusent des messages à caractère violent, incitant au terrorisme, pornographique ou de nature à porter

gravement atteinte à la dignité humaine ou à inciter des mineurs à se livrer à des jeux les mettant physiquement en danger lorsqu'ils sont susceptibles d'être vus ou perçus par un mineur.

3. Le cadre légal et réglementaire applicable n'est pas toujours suffisamment clair et adapté

S'agissant particulièrement des jeunes, le constat est que le cadre légal en vigueur contribue à une segmentation entre harcèlement au sein de l'univers scolaire et harcèlement, notamment en ligne, en dehors. Une meilleure coordination des textes en vigueur faciliterait une appréhension uniforme et universelle du phénomène par l'ensemble des acteurs accompagnant les victimes et leurs proches ainsi qu'une plus grande lisibilité du droit applicable.

De plus, le dispositif pénal en place, s'il prévoit bien des mesures de sanction, n'inclut pour l'heure :

- ni présomptions prévues par les textes en matière de cyberharcèlement dès lors que la victime est âgée de moins de quinze ans ;
- ni peines complémentaires, pouvant être prononcées par le juge et qui pourraient consister à suivre des formations d'éducation aux médias, en particulier à destination d'auteurs de faits qui seraient eux-mêmes enfants ou adolescents.

Les mesures de référés judiciaires existantes[37], destinées notamment à faire face à des situations d'urgence, n'apparaissent pas pleinement adaptées aux situations de cyberviolence qui nécessitent une célérité très forte et la capacité du juge à imposer par exemple une mesure de retrait ou de déréférencement du contenu litigieux à son éditeur ou à la plateforme.

37 Sont notamment visés : 1/ le référé préventif (articles 835 alinéa 1er du code de procédure civile) qui permet de demander au juge des mesures conservatoires ou de remise en état afin de prévenir un dommage imminent ou arrêter un trouble manifestement illicite ; 2/ le référé vie privée (article 9 alinéa 2 du Code civil).

Proposition 8 : renforcer et adapter les instruments scolaires et judiciaires de traitement des (cyber)violences des jeunes

Ce renforcement et cette adaptation supposent :

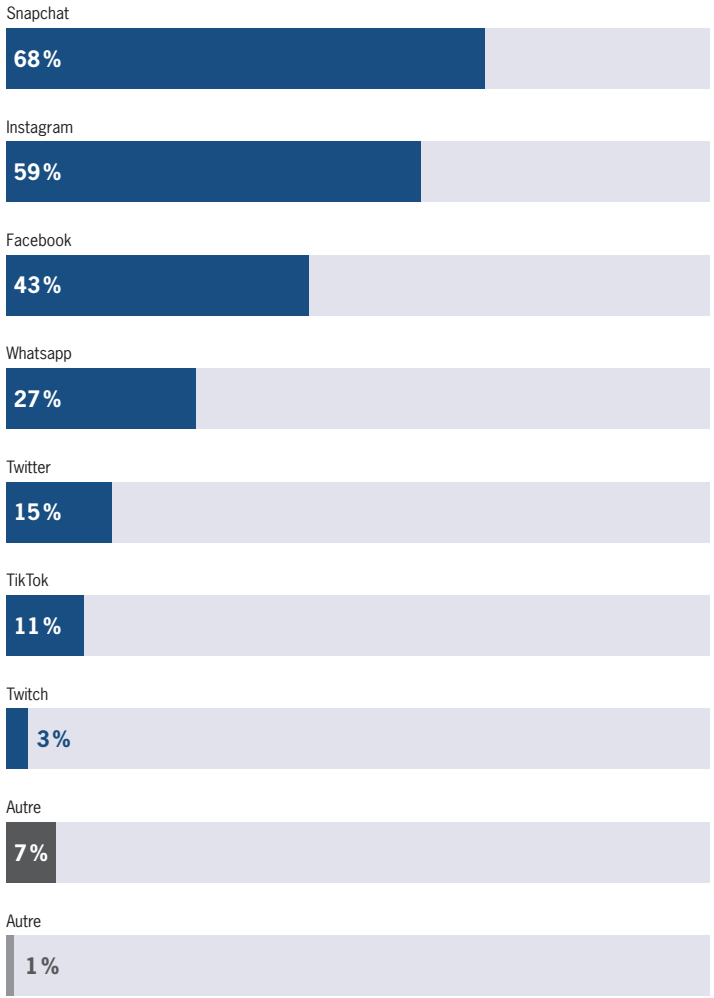
- **Une harmonisation des textes** qui concernent les (cyber)violences commises entre jeunes, afin de tenir compte des liens entre violences scolaires et cyberviolences. Un renvoi explicite à l'article 222-33-2-2 du code pénal dans l'article L. 511-3-1 du code de l'éducation permettrait de rendre compte d'un continuum entre les mesures de responsabilisation qui relèvent du cadre éducatif et celles qui sont du ressort de la justice dans les cas les plus graves ;
- **L'insertion de mesures de référé judiciaire spécifiques en matière de cyberviolences,** en complément de ce qui existe en matière de protection de la vie privée ou de prévention de troubles manifestement illicites, pour agir avec la célérité nécessaire afin de contraindre les éditeurs de contenus et, subsidiairement les plateformes, à supprimer ou bloquer l'accès à des contenus caractérisant des faits de cyberviolence. L'objectif recherché est de limiter au maximum tout phénomène collectif entre jeunes ;
- **La mobilisation de mesures de responsabilisation** pouvant être prononcées par le chef d'établissement ou le conseil de discipline dans le cas de cyberviolences qui se prolongent dans le cadre scolaire et pouvant imposer le suivi de séances de sensibilisation aux cyberviolences et de formations d'éducation aux médias et à la protection de la vie privée ;
- **La création de peines complémentaires pour les mineurs auteurs de cyberviolences** consistant notamment dans le suivi de séances de sensibilisation aux cyberviolences et de formations d'éducation aux médias et à la protection de la vie privée et permettant de s'inscrire dans l'objectif d'éducation propre à la justice des mineurs délinquants au sens de l'ordonnance 45-174 du 2 février 1945.

III. B. RESPONSABILISER : CONSTRUIRE UNE RESPONSABILITÉ RÉELLE POUR LES PLATEFORMES

Quand on parle de la navigation des jeunes sur Internet et sur les réseaux sociaux, on réalise que tous les acteurs sont concernés comme les développements précédents ont permis de le mesurer. C'est aussi le cas en termes de responsabilité. Bien sûr, il y a celle des adultes qui entourent les jeunes et les aident à grandir, c'est-à-dire leurs parents et leurs professeurs : leur responsabilité existe, elle doit désormais pouvoir s'enrichir dans la sphère numérique par une meilleure connaissance d'Internet et des réseaux sociaux. Il y a aussi la responsabilité des jeunes eux-mêmes, qui doit se construire (III.A).

Une autre responsabilité apparaît aussi largement à construire : celle des plateformes et des entreprises qui gèrent les réseaux sociaux où les jeunes se retrouvent de plus en plus. Plusieurs tentatives sont à l'œuvre mais butent encore sur deux difficultés majeures : **l'absence d'informations suffisantes et la réalité des mesures mises en œuvre par ces acteurs.** En d'autres termes, il n'existe que pas ou très peu de données qui soient produites de manière indépendante sur l'action des plateformes et des réseaux sociaux. Pour cette raison, une logique de « boîte noire » est encore à l'œuvre, ce qui limite considérablement la capacité à appréhender la responsabilité des plateformes.

Les réseaux sociaux les plus utilisés par les jeunes



1. La responsabilité des plateformes est engagée de manière disparate et souvent insuffisante

1/ Les plateformes, comme tout acteur traitant des données personnes, peuvent voir leur responsabilité engagée devant la CNIL en France

Les régulateurs, en France mais aussi à l'étranger, renforcent leurs actions tant préventives que répressives à l'égard de l'ensemble des professionnels qui traitent les données personnelles de leurs utilisateurs. Les plateformes et les réseaux sociaux sont particulièrement concernés à cet égard.

À titre d'illustration, au cours de l'année 2019, la CNIL a développé des actions d'accompagnement à l'égard des acteurs qui ne disposent pas nécessairement des ressources en interne pour appréhender les enjeux de protection des données personnelles, en l'occurrence les collectivités territoriales et les *start-up*. Elle a aussi élaboré des référentiels et des règlements types pour l'ensemble des professionnels et assuré une sensibilisation des délégués à la protection des données qui doivent obligatoirement être désignés dans les organismes publics et privés. Sur le plan répressif, la CNIL a mis en demeure plusieurs sociétés de se mettre en conformité avec le RGPD depuis son entrée en vigueur le 25 mai 2018 et, sans action de plusieurs d'entre-elles, a prononcé des sanctions. Le 21 janvier 2019, la CNIL a ainsi condamné la société Google à une amende de 50 M€, lui reprochant de ne pas informer de façon suffisamment claire ses utilisateurs quant à l'exploitation de leurs données personnelles[38].

La *Federal Trade Commission (FTC)* a également sanctionné plusieurs plateformes qui n'assurent pas la protection des données personnelles de leurs utilisateurs. À la suite d'une enquête ouverte en 2018 après le scandale *Cambridge Analytica*[39], Facebook a été condamné fin juillet 2019 à une amende de 5 Md$,

38 Pour rappel, le règlement permet d'infliger des sanctions allant jusqu'à 4 % du chiffre d'affaires mondial pour manquement aux obligations de protection des données personnelles des citoyens européens.

39 Ce scandale a éclaté quand il a été découvert que la société Cambridge Analytica avait recueilli les données personnelles de 87 millions d'utilisateurs Facebook dès 2014 et qu'elle les avait utilisées pour influencer les intentions de vote en faveur de personnalités politiques.

pour ne pas avoir su protéger les données personnelles de ses utilisateurs, et a pris plusieurs engagements pour éviter que cela ne se reproduise (comité indépendant, rapports réguliers). S'agissant des jeunes plus spécifiquement, YouTube a été condamné à une amende de 170 M$ pour avoir collecté les informations personnelles d'utilisateurs de moins de 13 ans sans l'accord de leurs parents, aux fins de revente à des sociétés dans un but publicitaire, alors même qu'une loi fédérale l'exige.

Ces actions participent à accroître les actions mises en œuvre par les plateformes. **Toutefois, des failles demeurent régulièrement pointées du doigt.** Instagram a fait l'objet d'une faille, révélée début septembre 2019 par Buzzfeed, permettant à n'importe quel follower d'un compte privé d'accéder aux contenus de celui-ci et de les partager librement en récupérant les URL des photos, vidéos ou stories dans le code source d'Instagram web et de copier ces liens. En outre, l'enquête menée a révélé que les membres d'Instagram dont les publications sont diffusées par ce biais ne disposent d'aucun moyen de savoir que d'autres personnes partagent ce qu'ils ont pourtant réservé à leur communauté restreinte. En 2015, les journalistes de Quartz avaient déjà démontré que les publications d'un compte public basculé en mode privé restaient en fait très facilement accessibles.

En outre, il paraît regrettable que la responsabilité des plateformes ne soit pas renforcée lorsque sont concernées les données d'utilisateurs mineurs. En effet, alors que le RGPD prévoit des adaptations en termes de consentement et de transparence à l'égard des publics vulnérables que sont notamment les jeunes, il n'inclut pas de sanctions renforcées lorsque ce sont leurs données qui ne sont pas ou sont insuffisamment protégées.

2/ En matière de contenus, la responsabilité des plateformes demeure principalement limitée et surtout subsidiaire par rapport à celle de ceux qui les créent et les diffusent

a) Sur le terrain juridique

Les plateformes sont soumises au sein de l'Union européenne à un **régime de responsabilité dérogatoire,** lequel signifie que les entreprises concernées ont un devoir de modération lorsqu'un contenu ou un comportement est porté à leur connaissance mais qu'elles n'ont pas un devoir de surveillance a priori. Dans le prolongement de la directive n° 2000/31 du 8 juin 2000 sur le commerce électronique qui prévoit un tel régime, la loi de 2004 pour la confiance dans l'économie numérique précise en son article 6 que :

- *« Les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des service de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services ne peuvent pas voir leur responsabilité civile engagée du fait des activités ou des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apparaître ce caractère ou si, dès le moment où elles en ont eu cette connaissance, elles ont agi promptement pour retirer ces données ou en rendre l'accès impossible » ;*
- *« [Ces personnes] ne peuvent voir leur responsabilité pénale engagée à raison des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de l'activité ou de l'information illicites ou si, dès le moment où elles en ont eu connaissance, elles ont agi promptement pour retirer ces informations ou en rendre l'accès impossible ».*

Enfin, la responsabilité tant civile que pénale des plateformes n'est que peu sollicitée en raison de leur caractère subsidiaire et elle n'est pas véritablement appréhendée au niveau européen, alors même que les plateformes interviennent à une échelle mondiale et se soumettent d'autant plus facilement et efficacement à des règles contraignantes à un niveau supranational. En outre, les initiatives prises par les plateformes octroient un droit de regard très limité de la part des autorités publiques et ne garantissent pas pleinement l'application

du droit applicable. Une exception à ce principe est prévue pour les cas d'incitation au terrorisme et de pédopornographie, notamment au bénéfice de règles européennes spécifiques.

La refonte des directives « services de médias audiovisuels (SMA) »[40] en 2018 et « droits d'auteur »[41] en 2019, qui n'a pas encore donné lieu à transposition en France[42], vise notamment à renforcer les obligations et la responsabilité des fournisseurs de plateformes de partage de contenus. La directive SMA révisée crée ainsi des obligations à la charge des fournisseurs de plateformes de partage de vidéos afin de protéger, d'une part, les mineurs contre certains contenus susceptibles de nuire à leur épanouissement physique, mental ou moral et, d'autre part, le grand public contre des contenus incitant à la violence, à la haine ou à la provocation publique à commettre une infraction terroriste. Le projet de loi relatif à la communication audiovisuelle et à la souveraineté culturelle à l'ère numérique transpose cette directive et confie par ailleurs ces pouvoirs à la future Autorité de régulation de la communication audiovisuelle et numérique qui disposera des compétences aujourd'hui dévolues au CSA et à la HADOPI.

La proposition de loi visant à lutter contre les contenus haineux sur Internet portée par la députée Laetitia Avia serait susceptible de renforcer également cet arsenal notamment par la création d'un nouveau régime de responsabilité administrative assortie de sanctions, jusqu'à 4 % de leur chiffre d'affaires annuel mondial total de l'exercice précédent, pour les opérateurs de plateformes à fort trafic s'agissant du retrait ou du masquage sous 24 h après notification de tout contenu comportant manifestement une incitation à la haine ou une

40 Directive (UE) 2018/1808 du Parlement européen et du Conseil du 14 novembre 2018 modifiant la Directive 2010/13/UE visant à la coordination de certaines dispositions législatives, réglementaires et administratives des États membres relatives à la fourniture services de médias audiovisuels (directive « Services de médias audiovisuels »), compte tenu de l'évolution des réalités du marché.

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

42 C'est l'objet des projets de loi organique et ordinaire relatifs à la communication audiovisuelle et à la souveraineté culturelle à l'ère numérique présentés le 5 décembre 2019 en Conseil des ministres.

injure discriminatoire à raison de la race, de la religion, du sexe, de l'orientation sexuelle ou du handicap.

Ces réglementations en cours d'élaboration viendront donc compléter les pouvoirs dont dispose déjà le CSA en matière de régulation des plateformes s'agissant de la lutte contre les fausses informations (cf. point 3/ ci-après).

b) Sur le terrain politique

Plus récemment, en 2016, et sur un terrain plus politique que juridique, Facebook, Twitter, YouTube et Microsoft se sont engagés devant la Commission européenne à **respecter un code de conduite** comprenant des mesures de lutte contre la diffusion en ligne de discours de haine illégaux (procédures internes, formation du personnel) avec pour objectif que la majorité des signalements valides puissent être examinés en moins de 24 heures et, s'il y a lieu, qu'ils donnent lieu au retrait des contenus visés ou au blocage d'accès à ceux-ci. En février 2018, le Haut Conseil à l'égalité entre les femmes et les hommes (HCE) observait que Facebook répondait en moyenne en deux jours tandis qu'il fallait environ une semaine à Twitter pour agir. Il reste que ce code de conduite n'est pas juridiquement contraignant pour les plateformes. **Dans cette mesure, les engagements pris permettent d'obtenir des données sur l'action des plateformes, sans toutefois qu'il s'agisse de mesures systématiques et surtout réalisées de manière totalement indépendantes des plateformes elles-mêmes.** En particulier, les plateformes demeurent décisionnaires en ce qui concerne les données qu'elles transmettent aux acteurs publics, ce qui souligne l'enjeu de la plus grande transparence des données pouvant être sollicitées de leur part à l'avenir.

Le code de conduite de la Commission européenne visant à combattre les discours de haine illégaux en ligne

Un code de conduite visant à combattre les discours de haine illégaux en ligne a été élaboré en mai 2016 par la Commission européenne avec quatre entreprises (Facebook, Microsoft, Twitter, YouTube). D'autres entreprises ont adhéré à ce code : Instagram, Google+, Dailymotion, Snapchat et Webedia (jeuxvideo.com).

L'objectif de ce code est de garantir un traitement rapide des demandes de suppression de contenu.

Il est précisé que *« lorsque les entreprises reçoivent une demande de suppression d'un contenu jugé illicite de leur plateforme en ligne, elles l'évaluent au regard de leurs règles, des lignes de conduite de leur communauté et, s'il y a lieu, des lois nationales qui transposent la législation de l'UE en matière de lutte contre le racisme et la xénophobie »*, ce qui est étonnant car les règles internes semblent primer sur les législations européenne et nationales.

Par ce code, les entreprises concernées ont pris l'engagement d'examiner la majorité des demandes en moins de 24 heures et à supprimer le contenu correspondant si nécessaire, tout en respectant le principe fondamental de la liberté d'expression.

Une évaluation de la mise en œuvre du code de conduite est réalisée par le biais d'un réseau d'organisations de la société civile situées dans plusieurs pays de l'UE s'appuyant sur une méthodologie commune : envoi régulier de demandes de suppressions de contenus, consignation de la durée nécessaire à l'évaluation de la demande par l'entreprise, du résultat apporté et du retour d'information.

Le Haut Conseil à l'égalité entre les femmes et les hommes a mené un testing en février 2018 pour mettre à l'épreuve la modération de Twitter, Facebook et Youtube à partir de contenus sexistes[43]. Le constat d'ensemble formulé par le HCE est que seuls 8 % des 545 contenus sexistes signalés ont été supprimés[44]. L'ONG Amnesty International a également mené une étude en décembre 2018 relative aux violences faites aux femmes sur Twitter en utilisant un logiciel d'intelligence artificielle dont la conclusion est identique sur l'absence d'entraves aux contenus haineux étudiés.

3/ Du fait de leur rôle systémique, les plateformes sont engagées à lutter plus activement contre la propagation de fausses informations, mais cela ne concerne que peu les pratiques des jeunes

Un code des bonnes pratiques contre la désinformation a été élaboré en septembre 2018 au niveau communautaire et signé par Youtube, Facebook et Google[45]. La Commission européenne a publié en avril 2019 un rapport faisant état d'un progrès continu de ces trois plateformes pour lutter contre les *fake news*[46]. À travers ce code, un meilleur engagement des plateformes est recherché, avec des points d'étapes réguliers.

43 Durand Edouard, Ronai Ernestine, Gayraud Alice et Guiraud Claire, *Rapport n° 2017-11-16-VIO-030*, En finir avec l'impunité des violences faites aux femmes en ligne : une urgence pour les victimes, 16 novembre 2017.

44 De façon plus détaillées, Facebook a modéré 11 % des messages signalés, Twitter 13 % et Youtube 0 %. Par ailleurs sur Twitter et Facebook, 100 % des menaces de violences crédibles ont disparu mais seulement 0,9 % des commentaires relevant d'une « incitation à la haine envers un genre » ont été supprimés sur Facebook et 17,4 % d'entre eux par Twitter.

45 Commission européenne, Code of Practice on Disinformation, 26 septembre 2018.

46 Commission européenne, Code of Practice against disinformation : Commission recognises platforms' efforts ahead of the European elections, 17 mai 2019.

Principales conclusions du rapport de la Commission européenne d'avril 2019

Google a fait part de mesures spécifiques prises pour améliorer le contrôle des placements de publicité dans l'UE, avec des informations détaillées par État membre. La plateforme a fait le point sur sa politique en matière de publicités électorales, dont la mise en œuvre a débuté le 21 mars 2019, et a annoncé le lancement de son rapport sur la transparence en matière de publicité électorale au sein de l'UE ainsi que la mise à disposition, en avril, de sa bibliothèque d'annonces dotée d'un moteur de recherche. Google n'a pas fait état de progrès supplémentaires en ce qui concerne la définition des publicités engagées. Comme dans le dernier rapport, des données mondiales ont également été fournies concernant la suppression d'un grand nombre de chaînes YouTube pour infraction à ses règles en matière de spams, de pratiques trompeuses et escroqueries et d'usurpation d'identité.

Facebook a fait part de mesures prises contre les publicités qui contrevenaient à ses règles pour cause de contenu médiocre, perturbateur, trompeur ou faux ou qui contournaient ses systèmes. La plateforme a fourni de plus amples informations sur ses règles en matière de publicités à caractère politique, qui s'appliqueront également à Instagram. L'entreprise a signalé le lancement à l'échelle mondiale, le 28 mars 2019, d'une nouvelle bibliothèque d'annonces *("Ad Library")* accessible au public, couvrant Facebook et Instagram, et a souligné l'extension de l'accès à son interface de programmation de cette bibliothèque. Facebook a communiqué le nombre de faux comptes fermés dans le monde au 1er trimestre de 2019 et fait état du démantèlement de huit réseaux à « comportement coordonné non authentique », originaires de la Macédoine du Nord, du Kosovo et de Russie. Le rapport n'indique pas si ces réseaux ont également affecté des utilisateurs dans l'UE.

.../...

Twitter a fait part d'une mise à jour de ses règles en matière de publicités de campagne politique et a fourni de plus amples informations sur la divulgation publique des publicités à caractère politique dans son centre pour la transparence publicitaire *("Ad Transparency Centre").* Twitter a fourni des chiffres sur les actions entreprises contre le spam et les faux comptes, mais n'a pas fourni d'informations supplémentaires sur ces actions ni sur la manière dont elles sont liées à des activités dans l'UE. Twitter n'a fait état d'aucune mesure visant à améliorer le contrôle des placements de publicité, ni fourni d'indicateurs relatifs à ses engagements dans ce domaine.

La France a construit un premier arsenal pour lutter contre la manipulation de l'information. La loi organique et la loi du 22 décembre 2018 relatives à la manipulation de l'information visent à lutter contre la manipulation de l'information à l'heure numérique et à endiguer la diffusion de fausses informations *("fake news")* pendant les campagnes électorales. Elles ont été promulguées le 22 décembre 2018. Toutefois, ces dispositions n'interviennent que dans un contexte spécifique qui ne concerne que très incidemment les phénomènes auxquels sont confrontés les jeunes en ligne.

Principales dispositions des lois visant à lutter contre la manipulation de l'information

Les lois visent à lutter contre la manipulation de l'information à l'heure numérique et à endiguer la diffusion de fausses informations *("fake news")* pendant les périodes de campagne électorale.

Elles créent une nouvelle voie de référé civil visant à faire cesser la diffusion de fausses informations durant les trois mois précédant un scrutin national. Quand il est saisi, le juge des référés doit apprécier, sous 48 heures, si ces fausses informations sont diffusées « de manière artificielle ou automatisée » et « massive ».

.../...

Dans sa décision du 20 décembre 2018, le Conseil constitutionnel a précisé que le juge ne pouvait faire cesser la diffusion d'une information que si le caractère inexact ou trompeur de l'information était manifeste et que le risque d'altération de la sincérité du scrutin était également manifeste.

Les plates-formes numériques (Facebook, Twitter, etc.) sont soumises à des obligations de transparence lorsqu'elles diffusent des contenus contre rémunération. Celles qui dépassent un certain volume de connexions par jour doivent avoir un représentant légal en France et rendre publics leurs algorithmes.

Le Conseil supérieur de l'audiovisuel (CSA) peut aussi empêcher, suspendre ou interrompre la diffusion de services de télévision contrôlés par un État étranger ou sous l'influence de cet État, et portant atteinte aux intérêts fondamentaux de la nation.

Il découle de cette loi de nouvelles compétences du CSA[47] en matière d'évaluation du caractère insuffisant ou excessif du comportement des plateformes en matière de retrait des contenus diffusant de fausses informations :

- En vertu de la loi du 22 décembre 2018 relative à la lutte contre la manipulation de l'information, le CSA contribue à la lutte contre la diffusion de fausses informations susceptibles de troubler l'ordre public ou de porter atteinte à la sincérité des scrutins. Pour ce faire, il assure un suivi des actions mises en œuvre par les plateformes et peut leur adresser des recommandations. Le CSA publie par ailleurs un bilan périodique et recueille à cette fin des informations auprès des plateformes en vertu des pouvoirs d'information et d'enquête qui lui sont dévolus aux termes de l'article 19 de la loi du 30 septembre 1986 relative à la liberté de communication.

47 Ou l'Autorité de régulation de la communication audiovisuelle et numérique prévue par le projet de loi relatif à *la communication audiovisuelle et à la souveraineté culturelle à l'ère numérique*.

- À ce titre, le CSA a adressé une recommandation aux plateformes le 15 mai 2019 pour qu'elles mettent en œuvre des actions concrètes (dispositif de signalement accessible et visible, transparence des algorithmes, promotion des contenus issus d'entreprises et d'agences de presse et de services de communication audiovisuelle, lutte contre les comptes propageant massivement de fausses informations, information sur les situations de rémunération en contrepartie de la promotion de contenus d'information, éducation aux médias et à l'information). Le 27 février 2020, le CSA a également mis au point un questionnaire à l'attention des plateformes pour les accompagner dans la préparation de leur déclaration annuelle s'agissant des mesures qu'elles mettent en place pour répondre à leurs nouvelles obligations, établi sur la base des réflexions des membres du Comité d'experts sur la désinformation en ligne auprès du CSA. Un premier rapport d'évaluation des mesures mises en place est attendu au cours des prochains mois.
- Par ailleurs, le CSA a renforcé sa coopération avec l'ARCEP via la création d'un pôle commun relatif aux marchés du numérique et aux nouvelles régulations[48]. Ainsi qu'il est précisé : « Le pôle commun s'intéressera également à la méthodologie, aux modalités et aux référentiels de supervision ainsi qu'aux outils de régulation par la donnée des plateformes numériques, portant notamment sur la collecte, l'exploitation et la restitution de données, l'analyse et les tests des algorithmes des plateformes, les modalités d'ouverture des APIs ou encore l'interaction avec des outils d'aide aux utilisateurs ». Il est précisé que dans le cadre de ce pôle commun, les deux régulateurs réuniront chaque mois le Comité de suivi sur la « Protection des mineurs contre la pornographie en ligne ».

Du fait de cette nouvelle réglementation, les plateformes (Google, Facebook, Twitter) sont devenues des interlocuteurs du CSA. Par conséquent sont mises en place des mesures contraignant les plateformes à mettre en œuvre des moyens de lutte contre les fausses informations, traduisant à la fois une obligation de moyens et une obligation de résultat. Le CSA accèdera ainsi à plusieurs moyens techniques que les plateformes sont obligées de mettre en place avec la loi de décembre 2018 et s'assurera des résultats auxquelles elles aboutissent.

48 Convention entre le Conseil supérieur de l'audiovisuel (CSA) et l'Autorité de régulation des communications électroniques et des postes et de la distribution de la presse (ARCEP), 2 mars 2020.

Aucune de ces réglementations ne prévoient de réelles spécificités lorsque des jeunes sont concernés, ce qui invite à conduire une revue de l'ensemble des textes et d'y inclure les évolutions pertinentes.

Proposition 9 : renforcer la responsabilité encourue par les plateformes s'agissant des utilisateurs mineurs, en particulier au niveau européen

Il s'agit de prévoir plusieurs évolutions :

- → **L'établissement d'un corpus de règles spécifiques de protection de la jeunesse qui s'insèreraient dans un texte européen de portée générale comme le *Digital Services Act*** couvrant l'ensemble des mesures de protection de l'enfance sur Internet et prévoyant, s'agissant des éditeurs de contenus et subsidiairement des plateformes, un régime de sanctions au niveau de l'Union européenne pour réprimer les violations à caractère systémique dépassant le cadre d'un seul État membre, en complément des pouvoirs de sanctions au niveau des régulateurs nationaux ;
- → **Des sanctions aggravées au titre du RGPD** en cas d'absence de protection ou de protection insuffisante des données à caractère personnel se rapportant à une personne dont la situation de minorité légale peut être raisonnablement connue ou identifiée.

2. Une nécessité forte est aussi de se donner les moyens d'évaluer de manière indépendante l'action des plateformes

En mai 2019, la mission confiée par le Secrétaire d'État chargé du Numérique à Benoît Loutrel a remis son rapport « Créer un cadre français de responsabilisation des réseaux sociaux en France avec une ambition européenne ». Ces travaux s'inscrivaient dans le prolongement de l'engagement pris entre le Président

de la République français et Mark Zuckerberg, en mai 2018, de lancer une telle mission. Ce rapport souligne notamment que « l'autorégulation est toujours en développement. Elle se contente trop souvent de proposer une réponse *ex-post* (après l'apparition du dommage). Elle manque de crédibilité, du fait de l'asymétrie extrême d'information, provoquant un sentiment de « *storytelling* » qui suscite une suspicion sur la réalité de l'action de la plateforme ». Ainsi que le rapport le précise, la mise en place d'une régulation *ex ante* devrait respecter trois conditions, la première consistant à « suivre une logique de conformité selon laquelle le régulateur supervise la bonne mise en œuvre de mesures préventives ou correctrices, sans se focaliser sur la matérialisation des risques ni chercher à réglementer lui-même le service fourni ».

Pour garantir une évaluation fiable, suivie et indépendante, il apparaît donc nécessaire, dans la suite du rapport Loutrel, d'envisager une nouvelle manière d'appréhender l'action conduite par les plateformes et les entreprises gérant les réseaux sociaux pour protéger les jeunes, et plus généralement l'ensemble de leurs utilisateurs, des risques qui peuvent leur causer préjudice (usurpation d'identité, fausses informations, cyberharcèlement, confrontation à des contenus choquants, diffusion de données à caractère personnel, etc.).

L'approche proposée consiste à compléter le cadre existant qui repose à la fois sur le droit dur et sur les bonnes pratiques déclarées par les plateformes :

- d'un côté, le droit dur présente souvent un temps de retard sur les pratiques des plateformes et ne joue qu'occasionnellement sur l'effet de réputation de celles-ci ; il est en outre limité par la connaissance limitée que le législateur, français comme européen, a de leurs actions effectives ;
- de l'autre, les bonnes pratiques sont à la main des plateformes et constituent généralement un instrument de communication de celles-ci, sans vraie capacité pour les pouvoirs publics d'en apprécier la réalité et l'efficacité.

Par conséquent, il est désormais nécessaire de pouvoir disposer d'instruments de régulation « démocratique », c'est-à-dire permettant de mettre fin à la logique de « boîte noire » des plateformes en produisant des informations par des sources externes et reconnues pour leurs compétences et leur honorabilité. L'objectif recherché est donc de confronter ces informations avec ce que

déclarent les plateformes, dans une logique de « *name and shame* », et de contribuer à construire un vrai régime de responsabilité des plateformes.

À cette fin, l'exemple des mesures prises en matière financière constitue une référence utile, incluant à la fois des audits réguliers et des *stress tests* permettant d'analyser la réaction des acteurs à plusieurs types d'*inputs*. Ce principe serait vraisemblablement adapté aux plateformes : ainsi, sans avoir besoin de communiquer aux autorités des informations couvertes par le secret commercial et notamment leurs algorithmes, les entreprises concernées seraient dans l'obligation de faire réaliser chaque année, selon un cadre général défini par les autorités publiques, des audits indépendants de leurs procédures afin d'évaluer si les mesures qu'elles mettent en œuvre fournissent des résultats satisfaisants en termes de minimisation des risques pour leurs utilisateurs, notamment les plus jeunes.

Par ailleurs, des *stress tests* seraient réalisés périodiquement par les pouvoirs publics ou sous leur contrôle pour évaluer la réponse fournie par les produits et services offerts par les plateformes et les réseaux sociaux. Ce type de test présente en outre l'avantage de demeurer pertinent, y compris lorsque les algorithmes et les technologies utilisés par les plateformes évoluent.

Principe des *stress tests* en matière financière

Les crises financières peuvent affecter profondément la dynamique de croissance. Pour cette raison, la sécurité des systèmes financiers, et en particulier le risque systémique, font l'objet de mesures spécifiques de surveillance.

Les mesures prévues par les accords de Bâle distinguent les dispositifs de supervision par les autorités publiques et les dispositifs de surveillance assurés par les acteurs de marché eux-mêmes. S'y ajoute par ailleurs une « discipline de marché » imposant une plus grande transparence de

.../...

la part des acteurs financiers, notamment s'agissant de leur gestion et de la communication d'informations. À cet égard, les informations exigées portent en particulier sur les méthodes utilisées par les banques. Pour que la pertinence des notations internes puisse être contrôlée, les banques doivent établir une unité indépendante de contrôle des risques et des programmes de tests rétroactifs et de *stress tests*.

Un test de résistance *(stress test)* consiste à simuler des conditions économiques et financières très défavorables afin d'en mesurer les conséquences sur le compte d'exploitation et le bilan des banques. Il vise à faire apparaître la possible sous-capitalisation de certaines d'entre elles et la fragilité éventuelle d'un système bancaire national s'il apparaît qu'une proportion non négligeable de ses banques n'obtient pas de résultats satisfaisants. Il conduit le cas échéant à obliger les banques défaillantes à se recapitaliser pour dissiper la méfiance sur leur état de santé et ainsi redonner vie au marché interbancaire des prêts, indispensable au fonctionnement normal d'un système bancaire et de l'économie réelle.

L'opération consiste à définir plusieurs *scenarii* à un horizon rapproché dont on mesurera l'impact sur les principaux postes à risque du bilan des banques (crédits, placements, dette). Un premier scénario, dit de base ou central, reprend les prévisions macroéconomiques existantes et sert de *benchmark* à un autre scénario dit dégradé ou extrême. Ce dernier incorpore généralement une récession, une hausse du chômage et des crédits non remboursés, une chute des marchés boursiers, une brutale hausse des taux, etc.

En outre, il pourrait être envisagé que les résultats de ces audits indépendants fassent l'objet d'une publicité à destination du grand public. Le **principe de *naming and shaming*** consistant à rendre visible la qualité des actions entreprises constituerait en effet une incitation très forte pour les plateformes à véritablement mettre en œuvre tout ce qui est possible pour lutter contre les risques que leurs utilisateurs peuvent courir à utilisant leurs produits et services.

Proposition 10 : tenir compte du caractère systémique des plateformes en prévoyant plusieurs mesures de surveillance inspirées du domaine financier et s'appuyant sur l'effet de réputation

Cela se déclinerait de deux manières :

- **Une obligation de réalisation d'audits indépendants** serait imposée aux plateformes et entreprises gérant des réseaux sociaux pour garantir qu'elles mettent en œuvre leurs obligations et engagements en matière de limitation des risques, spécifiquement à l'égard des jeunes (protection de la vie privée, lutte contre les fausses informations et les contenus choquants, accompagnement des victimes de cyberviolences). Par conséquent, et à leurs frais, ces entreprises devraient mandater chaque année des cabinets spécialisés opérant selon un cadre défini par les pouvoirs publics, notamment au niveau européen, et selon des standards de transparence sur la méthodologie de contrôle suivie et son adaptation régulière aux évolutions des pratiques. À cet égard, les travaux menés par le CSA en matière de contrôle des mesures prises par les plateformes pour lutter contre les fausses informations peuvent constituer un exemple utile pour construire ces matrices d'audit ;
- **La capacité pour les pouvoirs publics de réaliser ou de faire réaliser des *stress tests*** par des opérateurs présentant toutes les garanties de compétences et de déontologie professionnelles, notamment sous la supervision du pôle commun CSA/ARCOM - ARCEP relatif aux marchés du numérique et aux nouvelles régulations. Cela permettraitt d'évaluer les réponses des algorithmes des plateformes à des situations concrètes, ponctuelles ou plus systémiques, de cyberharcèlement, de diffusion de contenus choquants voire illégaux ou de fausses informations ainsi que de publication d'informations à caractère personnel.

.../...

Ces audits et *stress tests* pourraient notamment contribuer à enrichir la connaissance et l'action des régulateurs, notamment celle de la future Autorité de régulation de la communication audiovisuelle et numérique (ARCOM).

GLOSSAIRE

Algorithme : ensemble d'opérations ordonné et fini devant être suivi dans l'ordre pour résoudre un problème et pouvant être traduit, grâce à un langage de programmation, en un programme exécutable par un ordinateur.

API : *Application Programming Interface* ou Interface de programmation, c'est-à-dire une solution informatique qui permet à des applications de communiquer entre elles et de s'échanger mutuellement des services ou des données.

Bulle informationnelle : mécanismes de recommandation qui tendent à ne proposer à l'internaute que des contenus correspondant à ses centres d'intérêt et ses opinions.

CEPD : Comité européen de la protection des données, institué par le Règlement général sur la protection des données (RGPD) et dont la mission est d'en garantir l'application cohérente dans l'Union européenne.

Crowd-sourcing : méthode visant à utiliser l'intelligence, l'inventivité, les compétences et le savoir-faire du plus grand nombre d'utilisateurs pour atteindre un but, parfois en récompensant voire en rémunérant les participants.

Cyberharcèlement : actes agressifs, intentionnels perpétrés par un individu ou un groupe d'individus au moyen de formes de communication électroniques, de façon répétée à l'encontre d'une victime qui ne peut pas facilement se défendre seule. Ces actes peuvent être le prolongement des moqueries et des brimades en dehors de l'espace numérique ou inversement.

Cyberviolences : ensemble des actes agressifs et intentionnels, perpétrés par un individu ou un groupe au moyen d'outils numériques, envers une ou plusieurs personnes.

Deep fake : technique consistant à superposer des fichiers audio ou vidéo existants dans le but de créer de fausses informations ou de nuire à un individu.

Fake news : informations fallacieuses, destinées à tromper et qui rencontrent un large écho grâce à Internet et aux réseaux sociaux.

Fisha : expression qui désignent des comptes créés sur les réseaux sociaux pour « afficher » d'autres adolescents, notamment des jeunes filles, dans le but de leur nuire.

Infox : information mensongère ou délibérément biaisée. Synonyme de *fake news*.

Revenge porn : divulgation, dans le but de nuire à quelqu'un et sans son consentement, d'un document à caractère sexuel le concernant. Le terme français corresponsant est « pornodivulgation ».

TICE : technologies de l'information et de la communication pour l'éducation.

RGPD : Règlement général sur la protection des données du 27 avril 2016 dont l'objet est d'établir des règles de protection des personnes physiques à l'égard du traitement de leurs données à caractère personnel et des règles relatives à la libre circulation de ces données.

Sexting : action d'envoyer des messages (textes ou photos) sexuellement explicites, notamment via un téléphone portable.

ANNEXE

SONDAGE
INTERNET ET LES JEUNES

ODOXA
L'Opinion tranchée

Internet et les jeunes

Sondage réalisé pour INSTITUT MONTAIGNE dentsu AEGIS network AXA

Méthodologie

Recueil

Enquête réalisée auprès :

- d'un échantillon de Français interrogés par Internet les 16 et 17 octobre 2019.
- d'un échantillon de jeunes (de 11 à 20 ans) interrogés par Internet du 10 au 24 octobre 2019.
- d'un échantillon de parents de jeunes (de 11 à 20 ans) interrogés par Internet du 14 au 24 octobre 2019.

Echantillon

Echantillon de 1 001 Français représentatif de la population française âgée de 18 ans et plus

La représentativité de l'échantillon est assurée par la méthode des quotas appliqués aux variables suivantes : sexe, âge, niveau de diplôme et profession de l'interviewé après stratification par région et catégorie d'agglomération.

Echantillon de 3 004 jeunes âgées de 11 à 20 ans (quotas appliqués au sexe et à l'âge)

Dont : - 1211 jeunes âgés de 11 à 14 ans
- 895 jeunes âgés de 15 à 17 ans
- 898 jeunes âgés de 18 à 20 ans

Echantillon de 1 002 parents de jeunes de 11 à 20 ans (quotas appliqués au sexe et à l'âge de l'enfant)

ODOXA
L'Opinion tranchée

Précisions sur les marges d'erreur

Chaque sondage présente une incertitude statistique que l'on appelle marge d'erreur. Cette marge d'erreur signifie que le résultat d'un sondage se situe, avec un niveau de confiance de 95 %, de part et d'autre de la valeur observée. La marge d'erreur dépend de la taille de l'échantillon ainsi que du pourcentage observé.

	Si le pourcentage observé est de …					
Taille de l'Echantillon	5 % ou 95 %	10 % ou 90 %	20 % ou 80 %	30 % ou 70 %	40 % ou 60 %	50 %
100	4,4	6,0	8,0	9,2	9,8	10,0
200	3,1	4,2	5,7	6,5	6,9	7,1
300	2,5	3,5	4,6	5,3	5,7	5,8
400	2,2	3,0	4,0	4,6	4,9	5,0
500	1,9	2,7	3,6	4,1	4,4	4,5
600	1,8	2,4	3,3	3,7	4,0	4,1
800	1,5	2,5	2,8	3,2	3,5	3,5
900	1,4	2,0	2,6	3,0	3,2	3,3
1 000	1,4	1,8	**2,5**	2,8	3,0	3,1
2 000	1,0	1,3	1,8	2,1	2,2	2,2
3000	0,8	1,1	1,4	1,6	1,8	1,8

Lecture du tableau : Dans un échantillon de 1000 personnes, si le pourcentage observé est de 20 % la marge d'erreur est égale à 2,5 % : le pourcentage réel est donc compris dans l'intervalle [17,5 ; 22,5].

ODOXA
L'Opinion tranchée

Principaux enseignements (1/5)

I. L'activité en ligne n'est pas distincte de la vie réelle pour les jeunes comme pour leurs aînés

- Seuls 20 % des 11-20 ans affirment en effet que ce qu'ils font en ligne ne reste que virtuel ;
- 58 % des 11-20 ans préfèrent en effet voir leurs amis plutôt que de discuter avec eux sur Internet (9 %)
- 77 % des 11-20 ans préfèrent exprimer un désaccord en face-à-face.

II. Les réseaux sociaux les plus utilisés par les jeunes sont Snapchat (68 %) et Instagram (59 %) qui devancent Facebook (43 %)

- Le réseau n° 1 des Français est aujourd'hui devancé par Snapchat (68 %) et Instagram (59 %) chez les jeunes ;
- Les 11-14 ans citent en effet bien davantage TikTok (21 %) et se détournent bien plus de Facebook que leurs aînés (28 % seulement sont sur Facebook contre 61 % des 18-20 ans) ;
- En moyenne, les jeunes considèrent 47 % de leurs contacts comme des amis.

III. Pour les parents, Internet est synonyme de danger quand leur enfant a moins de 15 ans (59 %) et d'opportunité ensuite (60 % et 72 %). Les jeunes sont quant à eux parfaitement conscients des risques du web

- 79 % des 11-20 ans se rendent plusieurs fois par semaine sur Internet pour un usage scolaire ;
- Les jeunes utilisent essentiellement les moteurs de recherches (75 %) pour leurs recherches scolaires ;
- Harcèlement (97 %), contenus choquants (89 %) ou divulgations d'informations personnelles (93 %) : les jeunes ont conscience des risques du web qu'ils qualifient de « graves ».

Principaux enseignements (2/5)

IV. Pour les parents, l'usage d'Internet est devenu un processus d'apprentissage comme un autre, fait de libertés et de contraintes

- 31 % d'entre eux limitent les plages horaires d'accès à Internet (48 % chez les parents des 11-14 ans), 28 % contrôlent l'historique de navigation (45 % chez les parents des 11-14 ans) et 24 % ont mis en place un contrôle parental (40 % chez les parents des 11-14 ans) ;
- 72 % d'entre eux nous disent que leur enfant navigue principalement sur son propre *smartphone* (57 % chez les 11-14 ans).

V. Plus d'un jeune sur deux (56 %) dit avoir été victime de cyberviolences au moins une fois et plus d'un sur trois (35 %) y a déjà été confronté à plusieurs reprises

- Dans le détail, un jeune sur cinq déclare par exemple qu'il lui est déjà arrivé plus d'une fois d'être « victime d'insultes » (18 %), ou de « recevoir des images intimes non demandées » (17 %) ;
- Plus d'un jeune sur dix a été à plusieurs reprises victime « de rumeurs » (13 %) et même de « menaces » (9 %); plus d'un jeune sur cinq a plusieurs fois vu « un groupe se créer contre lui » (6 %) ou que « des images intimes de lui soient mises en ligne sans son accord » (5 %) ;
- Près d'un jeune sur quatre (24 %) reconnaît avoir commis des cyberviolences.

Principaux enseignements (3/5)

VI. Les parents ne savent pas vers quelle administration se tourner si leur enfant est victime de cyberharcèlement

- Les parents sont parfois démunis face aux actes de cyberharcèlement. La majorité d'entre eux (61 %) ne saurait d'ailleurs pas vers quelle administration se tourner si leur enfant en était victime.

VII. Les jeunes sont presque aussi exposés aux contenus choquants que les Français dans leur ensemble

- Plus d'un jeune sur deux a déjà accédé à un contenu choquant (56 %). Si l'on met de côté les réponses « non, rarement », cela représente un niveau toujours élevé de 39 % de jeunes ayant été exposés à plusieurs reprises à ce type de contenus ;
- 30 % des 11-20 ans déclarent avoir déjà accédé à des contenus violents, c'est-à-dire autant que les Français pris dans leur ensemble. 17 % des jeunes ont déjà été exposés à des contenus racistes, antisémites ou homophobes (contre 19 % observés sur la moyenne nationale) ;
- Ils sont même davantage confrontés aux contenus incitant à se livrer à des jeux dangereux (14 % contre 9 % des Français) ;
- Les jeunes âgés de 11 à 20 ans sont en revanche nettement moins nombreux à dire qu'il ont consulté des contenus pornographiques (21 %) que l'ensemble des Français (45 %).

Principaux enseignements (4/5)

VIII. Les parents surestiment légèrement l'accès de leurs enfants aux contenus choquants

- 40 % des parents pensent que leur enfant a déjà été exposé à des contenus violents alors que 30 % déclarent l'avoir été ;
- Ils sont 28 % à le penser à propos des contenus pornographiques (contre 21 %), 21 % pour les contenus racistes, antisémites ou homophobes (contre 17 %), 19 % s'agissant des contenus incitant à se livrer à des jeux dangereux (contre 14 %) et enfin 4 % des parents pensent que leur enfant a déjà été confronté à des contenus incitant ou justifiant des actes terroristes (contre 3 %).

IX. *Fake News* : les jeunes n'y échappent pas mais sont globalement sensibilisés et vigilants

- 74 % d'entre eux affirment qu'ils se sont souvent ou parfois rendus compte qu'ils avaient consulté des informations s'étant avérées fausses ;
- Lorsqu'ils souhaitent apprendre de nouvelles choses sur un sujet, ils se tournent en premier lieu vers leurs parents (51 %), notamment lorsqu'ils ont moins de 15 ans (70 %). Les sites web constituent leur deuxième source d'information (39 %), c'est même la première chez les 18-20 ans (55 %) ;
- Les sources d'information sur lesquelles les *fake news* sont les plus présentes arrivent aux deux dernières positions. 20 % des jeunes citent en effet YouTube et seulement 15 % les réseaux sociaux ;
- 83 % des 11-20 ans et 82 % des Français jugent en effet qu'elles doivent être encadrées par la loi. Ils sont respectivement 73 % et 79 % à considérer qu'elles représentent un grave problème pour la démocratie et 57 % et 65 % à juger que c'est un problème qui ne peut pas être résolu facilement.

Principaux enseignements (5/5)

X. Protection de la vie privée en ligne : les jeunes sont encore plus soucieux que leurs aînés même s'ils rejettent moins le marketing personnalisé

- 94 % des jeunes âgés de 11 à 20 ans affirment que protéger leur vie privée en ligne est pour eux un sujet important ;
- Question technique, les jeunes sont plutôt bien informés, surtout lorsqu'ils avancent dans l'âge. 63 % des 11-20 ans déclarent connaître les moyens de protéger leur vie privée sur Internet (74 % des 18-20 ans) et 54 % d'entre eux ont déjà utilisé des outils pour limiter leurs traces sur le web (70 % des 18-20 ans) ;
- 52 % des 11-20 ans pensent que c'est bien d'utiliser les informations sur leur âge, leurs goûts ou l'endroit où ils habitent pour leur proposer des produits qui leur plairont.

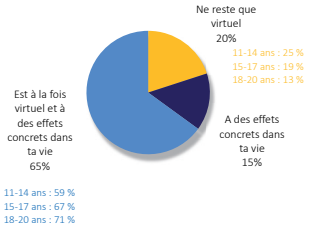
XI. Apprentissage d'Internet : forte défiance (66 %) des parents à l'égard de l'Éducation nationale alors que les jeunes apprécient massivement la formation de leurs professeurs (67 %)

- 77 % d'entre eux jugent qu'ils aident leur enfant à naviguer sur Internet sans prendre de risques ;
- 66 % d'entre eux considèrent que l'Éducation nationale ne forme pas leur enfant à naviguer sur Internet sans prendre de risques ;
- Les jeunes battent cette idée en brèche : ils apprécient les explications données par leurs professeurs. 67 % les ont jugées bonnes ;
- 64 % des jeunes de 11-20 ans et 77 % de leurs parents déclarent ne pas faire confiance à l'État pour protéger la vie privée. Ils font encore moins confiance aux entreprises qui gèrent les réseaux sociaux (79 % et 85 %).

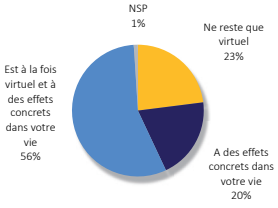
Rapport au numérique

Regard porté sur l'impact de son activité en ligne

Aux jeunes :
À ton avis, ce que tu fais en ligne…

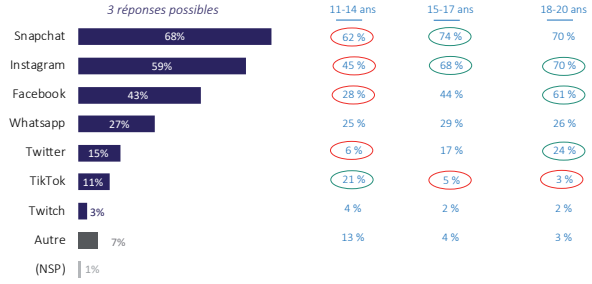


Aux Français :
Selon vous, ce que vous faites en ligne…



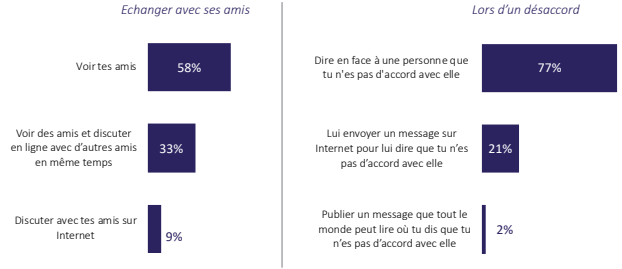
Les réseaux sociaux les plus utilisés par les jeunes

Aux jeunes :
Quels sont les réseaux sociaux sur lesquels tu te connectes le plus souvent ?



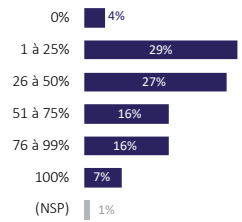
Recours au réel vs virtuel pour échanger et s'expliquer

Aux jeunes :
Pour chacun des cas suivants, choisis ce que tu ferais ?



Proportion d'amis dans les contacts en ligne des jeunes

Aux jeunes :
Sur ces réseaux, quelle proportion de tes contacts en ligne considères-tu comme des amis ? (réponse en %)



En moyenne, les jeunes considèrent **47 %** de leurs contacts en ligne comme des amis

11-14 ans : 51 %
15-17 ans : 47 %
18-20 ans : 41 %

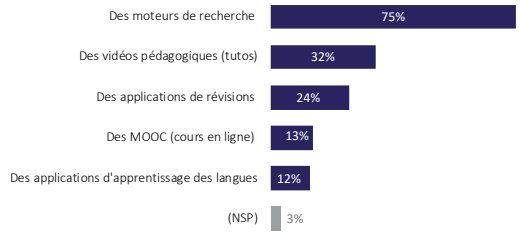
Internet : avant tout une opportunité ou un danger pour son enfant ?

Aux parents de jeunes (11-20 ans) :
Vous considérez que Internet et les réseaux sociaux sont avant tout, pour votre enfant :

Types de sites/applis les plus utilisés par les jeunes dans le cadre du travail scolaire

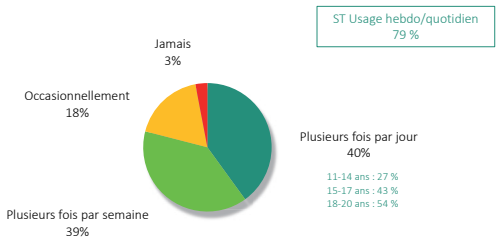
Aux jeunes :
Quels types de sites ou d'applications utilises-tu le plus dans le cadre de ton travail scolaire ?

2 réponses possibles



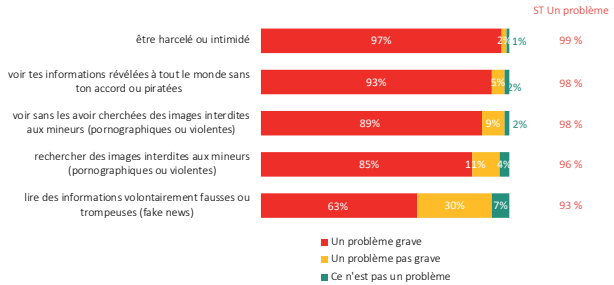
Usage scolaire et éducatif d'Internet par les jeunes

Aux jeunes :
À quelle fréquence utilises-tu Internet pour un usage scolaire et éducatif ?



Gravité perçue par les jeunes de certaines situations

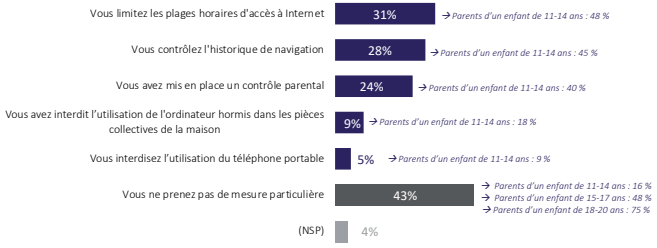
Aux jeunes :
Pour chacune des situations suivantes qu'on peut vivre en ligne, tu estimes que c'est ...



Mesures parentales adoptées pour la navigation sur Internet

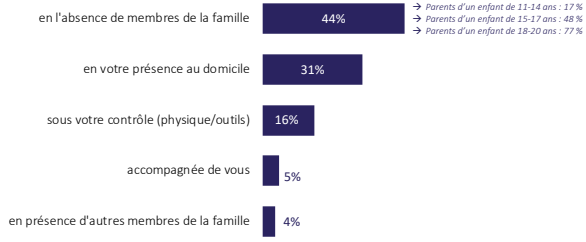
Aux parents de jeunes (11-20 ans) :
Quelles mesures adoptez-vous concernant la navigation de votre enfant sur Internet et les réseaux sociaux ?

Plusieurs réponses possibles



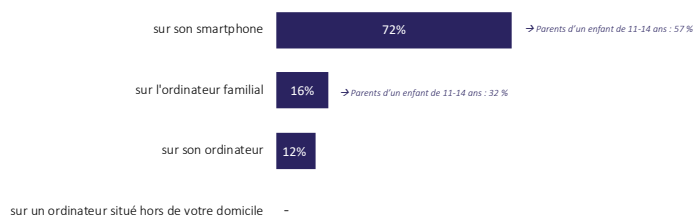
Navigation des jeunes sur Internet : autonomes ou accompagnés ?

Aux parents de jeunes (11-20 ans) :
Cette navigation se fait principalement…



Principal support utilisé par son enfant pour aller sur Internet/les réseaux sociaux

Aux parents de jeunes (11-20 ans) :
Lorsque votre enfant se rend sur Internet ou sur les réseaux sociaux, c'est principalement…



Synthèse du chapitre (1/4)

Activité en ligne : un prolongement de la vie réelle pour les jeunes comme pour leurs aînés

On prétend souvent que les jeunes ne sont pas suffisamment vigilants aux effets de leur vie en ligne sur leur vie réelle. Les résultats de notre sondage montrent que c'est faux. Ou en tout cas qu'ils n'en sont pas moins conscients que leurs aînés. Seuls 20 % des 11-20 ans affirment en effet que ce qu'ils font en ligne ne reste que virtuel, soit une proportion parfaitement comparable à celle des Français dans leur ensemble (23 %).
La majorité des jeunes (65 %) et des Français (56 %) considèrent au contraire que leur activité en ligne est certes virtuelle mais qu'elle a aussi des effets concrets dans leur vie. Ils sont même 15 % et 20 % à déclarer que cela a des effets concrets, mettant totalement de côté son caractère virtuel.
Cela étant dit, le fait qu'un jeune sur cinq estime que sa vie en ligne reste exclusivement virtuelle peut inquiéter, d'autant que les plus jeunes d'entre eux (les 11-14 ans) sont 25 % à le dire (contre 13 % des 18-20 ans).
Un autre cliché sur la jeunesse est battu en brèche dans notre enquête : non, les jeunes ne vivent pas leurs relations amicales exclusivement en ligne. 58 % des 11-20 ans préfèrent en effet voir leurs amis plutôt que de discuter avec eux sur Internet (9 %). 33 % d'entre eux profitent même des outils numériques pour multiplier les communications avec leurs amis : ils en voient certains et discutent sur Internet avec d'autres en même temps.
De même, lors d'un désaccord avec une personne, 77 % des 11-20 ans préfèrent l'exprimer en face-à-face plutôt qu'en lui envoyant un message (21 %) ou en publiant un message public (2 %).

Réseaux sociaux les plus utilisés par les jeunes : Snapchat (68 %) et Instagram (59 %) devancent Facebook (43 %)

Après la démocratisation d'Internet dans les années 2000, les années 2010 ont été marquées par l'émergence et le développement exceptionnel des réseaux sociaux, au point que, d'après Médiamétrie, 30 millions de Français s'y connectent quotidiennement (2018).
En une décennie, Facebook a fait des émules, qui le détrônent désormais chez les plus jeunes. Cité comme l'un des trois réseaux sur lequel ils se connectent le plus par 43 % des 11-20 ans, le réseau n° 1 des Français est aujourd'hui devancé par Snapchat (68 %) et Instagram (59 %) chez les jeunes.

Synthèse du chapitre (2/4)

La messagerie WhatsApp se classe en 4ème position avec 27 % des citations et devance Twitter (15 %), TikTok (11 %) et Twitch (3 %).
Notons qu'au sein même de la génération des 11-20 ans, les préférences évoluent. Les 11-14 ans citent en effet bien davantage TikTok (21 %) et se détournent bien plus de Facebook que leurs aînés (28 % seulement sont sur Facebook contre 61 % des 18-20 ans) ou d'Instagram (45 % vs 70 % des 18-20 ans).
Sur ces réseaux, les jeunes se connectent autant avec leurs amis qu'avec de simples connaissances ou inconnus. En moyenne, ils considèrent en effet la moitié de leurs contacts en ligne comme des amis (47 %). Plus ils avancent dans l'âge, plus cette proportion baisse (51 % chez les 11-14 ans contre 41 % chez les 18-20 ans).
Surtout, nous constatons de fortes disparités dans les comportements des jeunes. Ainsi, certains ne se connectent qu'avec des amis ou presque (7 % nous disent que tous leurs contacts sont des amis et 16 % qu'ils représentent au moins les trois-quarts de leurs contacts). D'autres en revanche se connectent avec des contacts qu'ils ne considèrent pas comme des amis : 4 % répondent aucun et 29 % moins d'un quart de l'ensemble de leurs contacts. Ces chiffres soulignent l'hétérogénéité des comportements mais aussi des règles d'usage propres à chaque réseau. Sur Facebook, il faut accepter qu'une personne entre dans notre réseau, ce n'est par exemple pas le cas de Twitter ou d'Instagram dans le cas de profils publics.

Pour les parents, Internet est synonyme de danger quand leur enfant a moins de 15 ans (59 %) et d'opportunité ensuite (60 % et 72 %). Les jeunes sont quant à eux parfaitement conscients des risques du web

Les parents des jeunes d'aujourd'hui n'ont pour la plupart pas connu Internet avant l'âge adulte. Comment perçoivent-ils cet outil entre les mains de leur enfant ?
Globalement, les parents de jeunes de 11 à 20 ans y voient plutôt une opportunité (56 %) qu'un danger (44 %) pour leurs enfants. Mais ces chiffres masquent assez logiquement des perceptions très différentes selon l'âge de l'enfant. Les parents d'enfants âgés de 11 à 14 ans considèrent en effet qu'Internet et les réseaux sociaux représentent un danger (59 %). Ils y voient ensuite plutôt une opportunité : 60 % des parents d'enfants de 15-17 ans et 72 % de ceux âgés de 18 à 20 ans le disent.
Ces résultats soulignent les paradoxes d'Internet : formidable accès aux savoirs et à des contenus choquants à la fois.

Synthèse du chapitre (3/4)

De fait, les jeunes d'aujourd'hui utilisent massivement le web pour un usage scolaire. 79 % des 11-20 ans se rendent plusieurs fois par semaine sur Internet pour cette raison. 40 % le font même quotidiennement. Et plus ils grandissent, plus cet usage se développe. 27 % des 11-14 ans se connectent chaque jour pour un usage scolaire et éducatif, une proportion qui s'élève à 43 % chez les 15-17 ans et même à 54 % chez les 18-20 ans.
Pour accéder aux contenus nécessaires à leur travail scolaire, les jeunes utilisent essentiellement les moteurs de recherches (75 %). Ces derniers devancent les vidéos pédagogiques, aussi appelées « tutos » (32 %) et les applications de révisions (24 %). Les MOOC (cours en ligne) sont moins souvent utilisés par les jeunes (13 %), tout comme les applications d'apprentissage des langues (12 %).
Si Internet est leur allié dans le cadre de leurs études, les jeunes ont aussi parfaitement conscience des risques qu'il peut engendrer. Ils ne les dédramatisent pas du tout.
97 % des 11-20 ans affirment en effet qu'être harcelé ou intimidé en ligne représente un « problème grave ». Très massivement aussi (93 %), les jeunes jugent que voir leurs informations révélées à tout le monde sans leur accord est grave. Il en va de même quant au fait d'être confronté à des images interdites aux mineurs (pornographiques ou violentes) que ce soit en les recherchant volontairement (85 %) ou sans les avoir recherchées (89 %).
Les *fake news* représentent le seul risque relativisé par une partie des jeunes. Si 63 % des 11-20 ans déclarent qu'il est « grave » de lire des informations volontairement fausses ou trompeuses, 30 % jugent que c'est certes un problème mais qu'il n'est « pas grave » et 7 % estiment même que « ce n'est pas un problème ».

Pour les parents, l'usage d'Internet est devenu un processus d'apprentissage comme un autre, fait de libertés et de contraintes

Face aux risques, les parents adoptent des stratégies de protection, essentiellement quand leur enfant a moins de 15 ans. 31 % d'entre eux limitent les plages horaires d'accès à Internet (48 % chez les parents des 11-14 ans), 28 % contrôlent l'historique de navigation (45 % chez les parents des 11-14 ans) et 24 % ont mis en place un contrôle parental (40 % chez les parents des 11-14 ans). Plus radicaux, 9 % des parents ont interdit l'utilisation de l'ordinateur hormis dans les pièces collectives de la maison (18 % chez les parents des 11-14 ans) et 5 % d'entre eux interdisent l'utilisation du téléphone portable (9 % chez les parents des 11-14 ans).

Synthèse du chapitre (4/4)

L'avènement du *smartphone* rend encore plus difficile la surveillance des parents sur l'activité en ligne de leur progéniture. 72 % d'entre eux nous disent en effet que leur enfant navigue principalement sur son *smartphone*. C'est le cas de quasiment tous les jeunes à partir de 15 ans. Avant cet âge, le *smartphone* est aussi le moyen d'accès n° 1 au web (57 %) mais un tiers des 11-14 ans se connectent principalement sur l'ordinateur familial selon leurs parents. Seuls 17 % de ces parents déclarent que la navigation se fait en l'absence de membres de la famille contre 48 % des parents d'enfants de 15-17 ans et 77 % à partir de 18 ans.
À travers ces résultats, on comprend aisément que l'accès à Internet et aux réseaux sociaux est devenu un processus d'apprentissage fait de libertés et de contraintes aux yeux des parents. Plus les jeunes grandissent, moins les parents contrôlent leur activité en ligne.

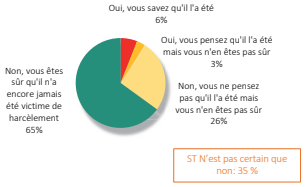
Cyberviolences

Cyberviolences : situation et auteur(s) connu(s) par les parents ?

Aux parents de jeunes (11-20 ans) :
Savez-vous si votre enfant a déjà été victime de harcèlement en ligne ?

ST Oui : 9 %

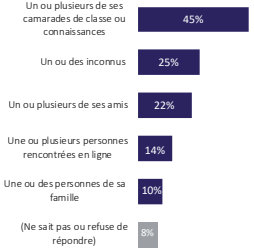
Rappel ST Oui Jeunes : 41 %



ST N'est pas certain que non: 35 %

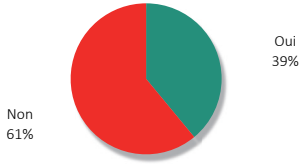
Aux parents de jeunes (11-20 ans) :
Si oui, qui était selon vous l'auteur de la situation de harcèlement vécue par votre enfant ?

Plusieurs réponses possibles



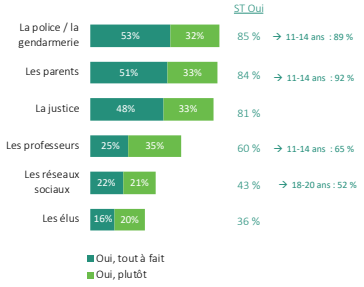
Cyberharcèlement : connaissance de l'administration vers laquelle se tourner ?

Aux parents de jeunes (11-20 ans) :
Si votre enfant était harcelé en ligne, sauriez-vous à quelle administration vous adresser pour trouver une solution ?

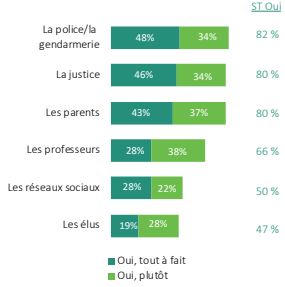


Interlocuteurs pouvant aider à réduire le harcèlement en ligne

Aux jeunes :
Selon toi, les interlocuteurs suivants peuvent-ils aider à réduire le harcèlement en ligne ?

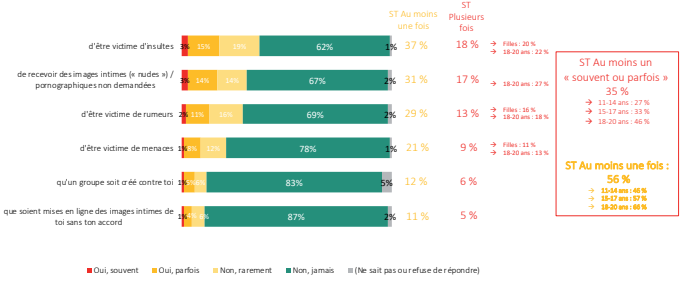


Aux Français :
Selon vous, les interlocuteurs suivants peuvent-ils aider à réduire le harcèlement en ligne ?



Part de jeunes ayant été victimes de formes de cyberviolences

Aux jeunes :
Sur Internet et les réseaux sociaux, t'est-il déjà arrivé…



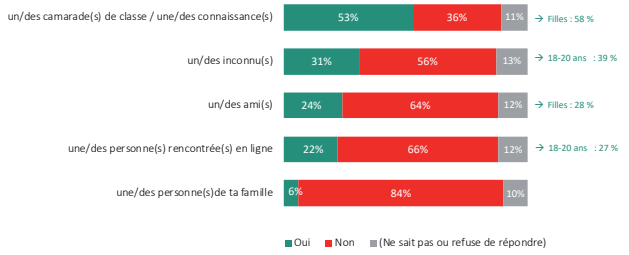
Part de jeunes ayant été victimes de formes de cyberviolences
Détail par sexe et âge

Aux jeunes :
Sur Internet et les réseaux sociaux, t'est-il déjà arrivé...

	Garçons	11-14 ans	15-17 ans	18-20 ans	Filles	11-14 ans	15-17 ans	18-20 ans
d'être victime d'insultes	**35 %**	31 %	34 %	42 %	**39 %**	31 %	42 %	46 %
de recevoir des images intimes (« nudes ») / pornographiques non demandées	**29 %**	22 %	30 %	40 %	**33 %**	18 %	35 %	49 %
d'être victime de rumeurs	**25 %**	20 %	25 %	32 %	**33 %**	26 %	36 %	39 %
d'être victime de menaces	**19 %**	16 %	19 %	24 %	**24 %**	17 %	26 %	30 %
qu'un groupe soit créé contre toi	**11 %**	9 %	11 %	12 %	**15 %**	14 %	15 %	16 %
que soient mises en ligne des images intimes de toi sans ton accord	**12 %**	9 %	14 %	16 %	**10 %**	8 %	13 %	10 %
ST Au moins une fois	**53 %**	**46 %**	**55 %**	**63 %**	**58 %**	**46 %**	**61 %**	**69 %**
ST Au moins un « Souvent ou parfois »	**32 %**	**27 %**	**31 %**	**40 %**	**38 %**	**27 %**	**36 %**	**52 %**

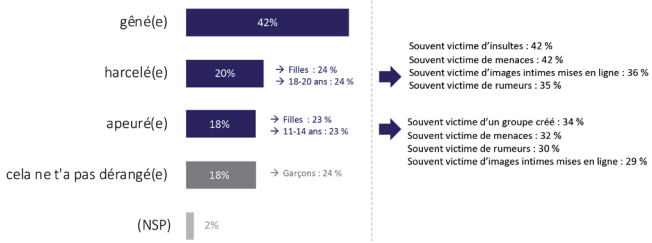
Capacité des jeunes à identifier les auteurs de leur cyberviolence

Aux jeunes concernés :
Si l'une de ces situations t'est arrivée, le ou les auteurs étaient...



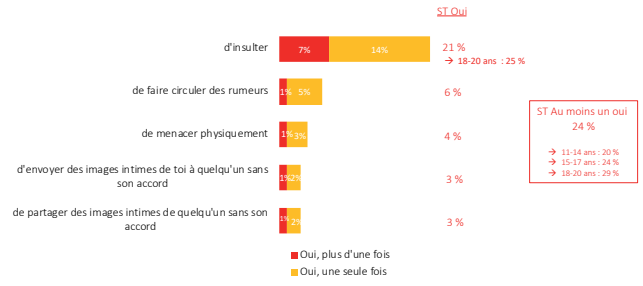
Ressenti des jeunes ayant été victimes de formes de cyberviolences

Aux jeunes concernés :
Si l'une de ces situations t'est arrivée, tu t'es senti(e) plutôt :



Part de jeunes ayant déjà harcelé sur Internet/les réseaux sociaux

Aux jeunes :
Sur Internet et les réseaux sociaux, il t'est déjà arrivé...



Synthèse du chapitre (1/3)

Cyberviolences : Plus d'un jeune sur 2 (56 %) dit en avoir été victime au moins une fois et 35 % y ont déjà été confrontés à plusieurs reprises

Le cyberviolence est une réalité pour bon nombre de jeunes : la part de jeunes ayant déjà été victimes – au moins « rarement », c'est-à-dire au moins une fois – de l'une des situations testées dans l'enquête est vertigineuse : plus d'un jeune sur deux est concerné (56 %). Ainsi, dans le détail sur Internet, 37 % des jeunes ont déjà été victimes d'insultes, 29 % de rumeurs et 21 % de menaces !

Même si l'on exclut les réponses « rarement » pour ne retenir dans nos mesures que les jeunes ayant été confrontés plus d'une fois à ces situations, nous aboutissons à des niveaux très spectaculaires : 35 % des 11-20 ans ont en effet été victimes à plusieurs reprises d'au moins une forme de cyberviolence détaillée ci-après. 48 % des 18-20 ans y ont même déjà été confrontés. Pour les autres, les taux sont moins élevés mais restent importants : 33 % des 15-17 ans et – tout de même – 27 % des très jeunes (âgés de 11 à 14 ans) y ont déjà été confrontés eux-aussi.

Dans le détail, un jeune sur cinq déclare par exemple qu'il lui est déjà arrivé plus d'une fois d'être « victime d'insultes » (18 %), ou de « recevoir des images intimes non demandées » (17 %). Plus d'un jeune sur dix a été à plusieurs reprises victime « de rumeurs » (13 %) et même de « menaces » (9 %). Enfin, plus d'un jeune sur cinq a plusieurs fois vu « un groupe se créer contre lui » (6 %) ou que « des images intimes de lui soient mises en ligne sans son accord » (5 %).

Notons que les filles sont davantage touchées que les garçons par pratiquement toutes les dimensions testées de la cyberviolence : que ce soit le fait d'être victimes d'insultes (20 %), de rumeurs (16 %) et de menaces (11 %).

Face à cela, les jeunes se sont essentiellement sentis gênés (42 %) plutôt que véritablement harcelés (20 %) ou apeurés (18 %). 18 % nous indiquent même que cela ne les a pas spécialement dérangés. Le plus souvent, les faits de cyberviolence proviennent de personnes bien connues et proches : ainsi 53 % des « bourreaux » étaient des camarades de classe ou connaissances, et 3 fois sur 10 il s'agissait d'amis (24 %) ou même de personnes de leur famille (6 %).

Synthèse du chapitre (2/3)

Les proches ne sont pas les seuls en cause. 3 jeunes sur 10 (31 %) ont été victimes d'inconnus et 2 sur 10 (22 %) de personnes rencontrées en ligne.

La généralisation du problème du harcèlement est bien illustrée par d'autres résultats de notre étude : les « victimes » ne sont pas les seul(e)s à s'exprimer, les auteurs se reconnaissent aussi … et si leur nombre est logiquement bien moindre (un seul auteur pouvant faire plusieurs victimes), il est tout de même tout à fait conséquent.

Près d'un jeune sur quatre (24 %) reconnait avoir été un cyberharceleur. Chiffre à mettre en relation avec les 56 % de jeunes ayant eu à subir ces violences. Dans le détail « nos jeunes auteurs » sont 21 % à avoir déjà insulté en ligne. Plus rares sont ceux qui ont fait circuler des rumeurs (6 %), qui ont menacé physiquement (4 %), envoyé des images intimes d'eux sans accord (3 %) ou partagé des images intimes de quelqu'un (3 %).

9 % des parents pensent que leur enfant a déjà été victime de cyberviolences

Les parents sous-estiment le harcèlement dont peuvent être victimes leurs enfants. Ils ne sont en effet que 9 % à penser que ça a déjà été le cas, 6 % en étant même certains. En comparaison du résultat observé chez les jeunes (56 % victimes au moins une fois et 35 % à plusieurs reprises), l'écart est donc compris entre 26 et 47 points !
Certains parents ont tout de même des doutes : 26 % d'entre eux pensent que leur enfant n'a pas été victime de cyberviolence mais ils n'en sont pas sûrs. Même en intégrant cette part de doute ou cette zone grise, les pauvres parents sont encore bien en dessous de la réalité…
S'ils sous-estiment les cyberviolences, les parents devinent assez bien qui peuvent être les auteurs des brimades infligées à leurs enfants. Ils pensent en effet d'abord (et à raison) qu'il s'agit des camarades de classe et connaissances (45 %) devant les inconnus (25 %), les amis (22 %), les personnes rencontrées en ligne (14 %) et la famille (10 %).

Synthèse du chapitre (3/3)

Nos résultats montrent donc combien les jeunes peuvent être confrontés à des cyberviolences dont ils ne parlent pas toujours à leurs parents.

Pourtant, ces mêmes jeunes sont convaincus que les parents ont un rôle à jouer pour réduire le harcèlement en ligne. 84 % des jeunes le pensent. Ils estiment aussi massivement que la police (85 %) et la justice (81 %) peuvent aider à réduire le harcèlement en ligne. Dans une moindre mesure, ils comptent aussi sur les professeurs (60 %). Les jeunes âgés de 11 à 20 ans doutent en revanche davantage de la capacité des réseaux sociaux (43 %) et des élus (36 %) à participer efficacement à ce combat.

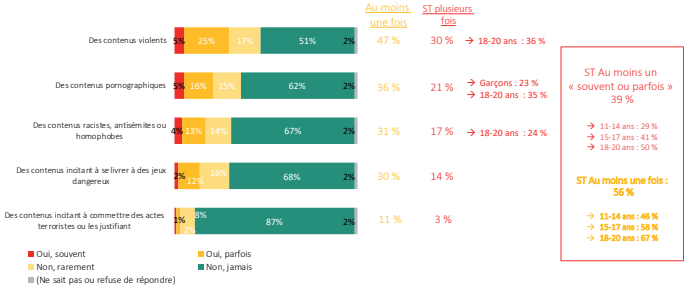
Les Français expriment globalement le même avis que les jeunes. Ils font massivement confiance à la police (82 %), à la justice (80 %) et aux parents (80 %). Les deux tiers d'entre eux (66 %) jugent que les professeurs peuvent aider à réduire le harcèlement en ligne mais sont loin d'être convaincus par les réseaux sociaux (50 %) et les élus (47 %).

Les parents sont parfois démunis face aux actes de cyberviolence. La majorité d'entre eux (61 %) ne saurait d'ailleurs pas vers quelle administration se tourner si leur enfant en était victime.

Contenus choquants

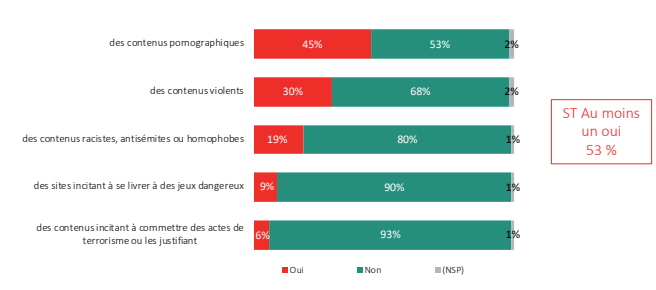
L'accès à des contenus choquants en ligne

Aux jeunes :
As-tu déjà accédé à l'un des contenus suivants sur Internet ?



L'accès à des contenus choquants en ligne

Aux Français :
Avez-vous déjà accédé à...



L'accès à des contenus choquants en ligne

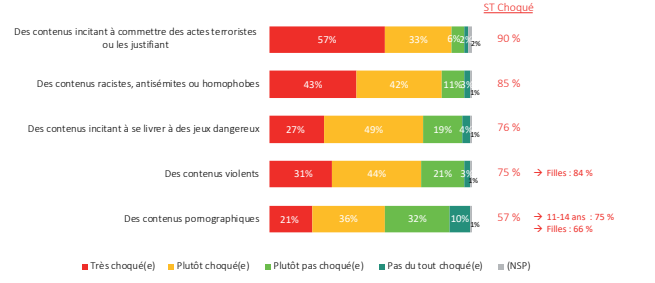
Détail par sexe et âge

Aux jeunes :
As-tu déjà accédé à l'un des contenus suivants sur Internet ?

	Garçons	11-14 ans	15-17 ans	18-20 ans	Filles	11-14 ans	15-17 ans	18-20 ans
Des contenus violents	**49 %**	42 %	50 %	59 %	**46 %**	36 %	51 %	53 %
Des contenus pornographiques	**38 %**	24 %	41 %	57 %	**33 %**	20 %	33 %	50 %
Des contenus racistes, antisémites ou homophobes	**28 %**	19 %	31 %	39 %	**34 %**	24 %	37 %	43 %
Des contenus incitant à se livrer à des jeux dangereux	**31 %**	25 %	34 %	38 %	**30 %**	26 %	31 %	34 %
Des contenus incitant à commettre des actes terroristes ou les justifiant	**11 %**	8 %	11 %	15 %	**12 %**	8 %	12 %	16 %
ST Au moins une fois	**56 %**	**47 %**	**56 %**	**70 %**	**55 %**	**44 %**	**59 %**	**64 %**

Choc suscité par ces contenus

Aux jeunes :
Si oui, tu dirais que tu as été très, plutôt, plutôt pas, ou pas du tout choqué par ces contenus ?

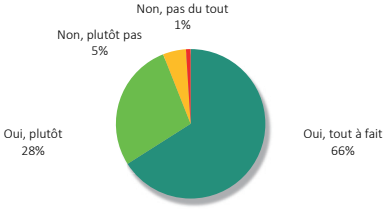


Nécessité de mieux encadrer l'accès aux contenus choquants en ligne

Aux jeunes :
Penses-tu que l'accès à ces contenus devrait être plus encadré sur Internet et les réseaux sociaux ?

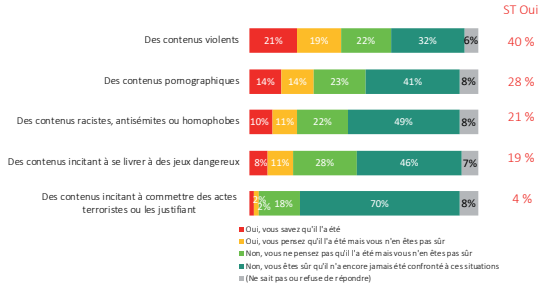
ST Non : 6 %

ST Oui : 94 %



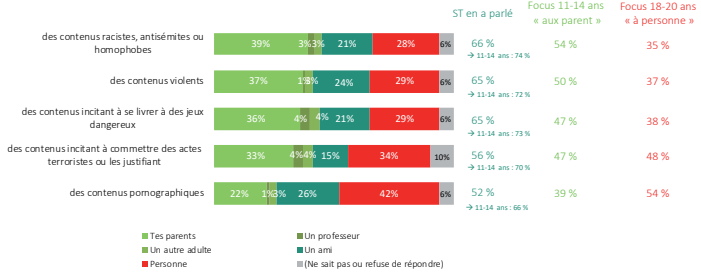
L'accès à des contenus choquants en ligne : connaissance des parents sur la situation de leur enfant

Aux parents de jeunes (11-20 ans) :
Votre enfant a-t-il été confronté aux situations suivantes ?



Part de jeunes ayant parlé de leur exposition à ces contenus choquants

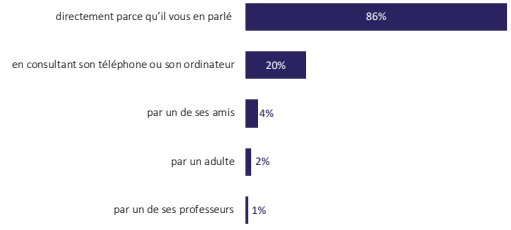
Aux jeunes :
Si oui, en as-tu parlé à ...



L'accès à des contenus choquants en ligne : connaissance des parents sur la situation de leur enfant

Aux parents de jeunes (11-20 ans)
Si oui, comment l'avez-vous appris...

Plusieurs réponses possibles



Synthèse du chapitre (1/2)

Contenus choquants : les jeunes sont presque aussi exposés que les Français pris dans leur ensemble

En dépit des protections mises en place par leurs parents, les jeunes âgés de 11 à 20 ans se trouvent confrontés à des contenus potentiellement choquants. La comparaison des résultats observés avec ceux des Français montre que, pornographie mise à part, les jeunes sont globalement aussi exposés que leurs aînés.

Plus d'un jeune sur deux a déjà accédé à un contenu choquant (56 %). Si l'on met de côté les réponses « non, rarement », cela représente un niveau toujours élevé de 39 % de jeunes ayant été exposés à plusieurs reprises à ce type de contenus.
30 % des 11-20 ans déclarent avoir déjà accédé à des contenus violents, c'est-à-dire autant que les Français pris dans leur ensemble. 17 % des jeunes ont déjà été exposés à des contenus racistes, antisémites ou homophobes (contre 19 % observés sur la moyenne nationale).
Ils sont même davantage confrontés aux contenus incitant à se livrer à des jeux dangereux (14 % contre 9 % des Français). Enfin, 3 % des jeunes ont déjà été exposés à des contenus incitant à commettre des actes terroristes ou les justifiant (6 % chez les Français).
Les jeunes âgés de 11 à 20 ans ont en revanche nettement moins consulté de contenus pornographiques (21 %) que l'ensemble des Français (45 %).

Face à ces différents contenus, les jeunes se déclarent très majoritairement choqués. Ils sont même unanimes lorsqu'ils ont été exposés à des contenus terroristes (90 %) ou à des contenus racistes, antisémites ou homophobes (85 %). Les trois-quarts des jeunes confrontés à des contenus incitant à se livrer à des jeux dangereux (76 %) et à des contenus violents (75 %) se disent choqués. Les contenus pornographiques choquent moins les jeunes qui y ont accédé (57 %) mais ils le sont bien davantage entre 11 et 14 ans (75 %). Pour éviter cela, les jeunes sont unanimes : 94 % d'entre eux estiment que l'accès à ces contenus devrait être plus encadré sur Internet et les réseaux sociaux.

Les jeunes âgés de 11 à 20 ans ont majoritairement tendance à parler des contenus choquants qu'ils ont vu sur Internet. 66 % des jeunes exposés à des contenus racistes en ont parlé, 65 % pour les contenus violents, 65 % s'agissant des contenus incitant à se livrer à des jeux dangereux, 56 % pour les contenus terroristes et 52 % pour la pornographie. Notons que les 11-14 ans ont encore davantage tendance à parler des différents contenus choquants auxquels ils ont pu être confrontés.

Rapport à la vérité

Synthèse du chapitre (2/2)

À l'exception des contenus pornographiques, les premières oreilles vers lesquelles les jeunes se tournent sont celles de leurs parents (de 33 à 39 %) puis celles de leurs amis (de 15 à 24 %). Les plus jeunes se tournent encore davantage vers leurs parents quand les 18-20 ans ont davantage tendance à garder pour eux les contenus potentiellement choquants qu'ils ont vus sur Internet.

Les parents surestiment légèrement l'accès de leurs enfants aux contenus choquants

Comme nous l'avons constaté, les parents ont tendance à sous-estimer le cyberviolence dont leurs enfants peuvent être victimes mais, à l'inverse, ils surestiment leur accès aux contenus choquants.

40 % des parents pensent que leur enfant a déjà été exposé à des contenus violents alors que 30 % déclarent l'avoir été. Ils sont 28 % à le penser à propos des contenus pornographiques (contre 21 %), 21 % pour les contenus racistes, antisémites ou homophobes (contre 17 %), 19 % s'agissant des contenus incitant à se livrer à des jeux dangereux (contre 14 %) et enfin 4 % des parents pensent que leur enfant a déjà été confronté à des contenus incitant ou justifiant des actes terroristes (contre 3 %).

86 % des parents déclarent avoir eu connaissance des contenus choquants auxquels leur enfant a été exposé directement parce qu'il leur en a parlé. La seule autre source qui permet aux parents de le savoir est la consultation du téléphone ou de l'ordinateur de l'enfant mais elle ne culmine qu'à 20 %.

Ce résultat confirme les dires des enfants qui n'hésitent pas à parler des contenus choquants à leurs parents. Il souligne aussi l'importance du dialogue parents-enfants car même si la surveillance et les moyens de protection mis en place peuvent s'avérer efficaces, ils ne font pas le poids face à la confiance des enfants vis-à-vis de leurs parents.

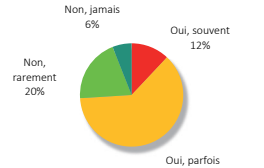
Consultation d'informations fausses et réaction adoptée par les jeunes

Aux jeunes :
T'es-tu déjà rendu compte que les informations que tu consultais étaient fausses ?

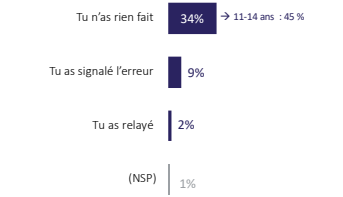
ST Non : 26 %

ST Oui : 74 %

→ 18-20 ans : 84 %

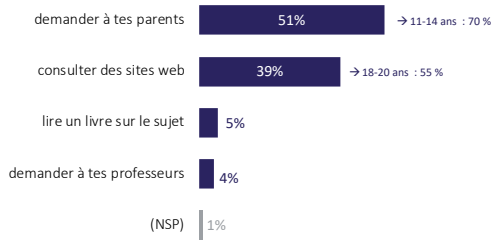


Aux jeunes :
Si oui, comment as-tu réagi ?



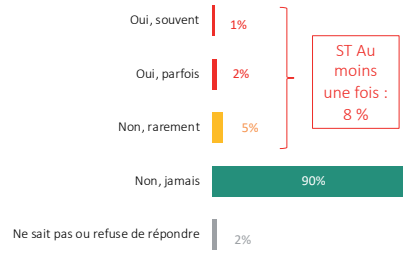
Méthode privilégiée par les jeunes pour apprendre de nouvelles choses

Aux jeunes :
Si tu souhaites apprendre de nouvelles choses sur un sujet, tu préfères d'abord…



Part de jeunes ayant déjà écrit de fausses informations sur Internet ou les réseaux sociaux

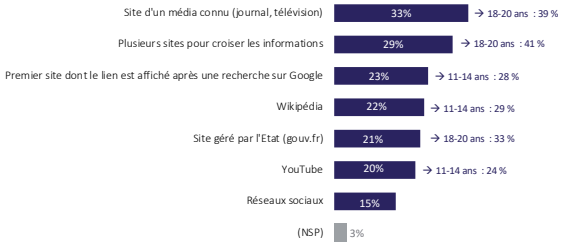
Aux jeunes :
As-tu déjà utilisé Internet ou les réseaux sociaux pour écrire des choses fausses sur des personnes ou des événements ?



Site consulté par les jeunes pour trouver des informations fiables

Aux jeunes :
Si tu as besoin de trouver des informations fiables sur un événement qui vient de se produire, où te rends-tu ?

Plusieurs réponses possibles

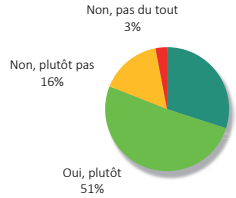


Des enfants suffisamment sensibilisés à la nécessité de vérifier les informations consultées ?

Aux parents de jeunes (11-20 ans) :
Estimez-vous que votre enfant est suffisamment sensibilisé à la nécessité de vérifier si les informations qu'il consulte sur Internet sont vraies ?

ST Non : 19 %

ST Oui : 81 %



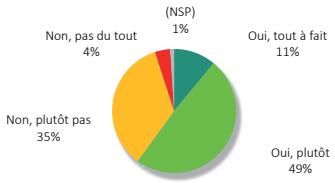
- *Parents d'un enfant de 11-14 ans : 21 %*
- *Parents d'un enfant de 15-17 ans : 32 %*
- *Parents d'un enfant de 18-20 ans : 42 %*

Vérification des informations consultées en ligne

Aux Français :
Pensez-vous vérifier suffisamment si les informations que vous consultez en ligne sont vraies ?

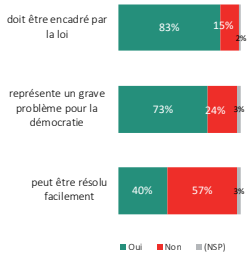
ST Non : 39 %

ST Oui : 60 %

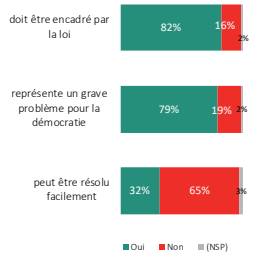


Regard porté sur les *fake news*

Aux jeunes :
Penses-tu que le phénomène des *fake news*…



Aux Français :
Pensez-vous que le phénomène des *fake news*…



Synthèse du chapitre (1/2)

***Fake News* : les jeunes n'y échappent pas mais sont globalement sensibilisés et vigilants**

Les jeunes ne sont pas à l'abri des fausses informations. 74 % d'entre eux affirment qu'ils se sont souvent ou parfois rendus compte qu'ils avaient consulté des informations s'étant avérées fausses. Ils sont même 84 % à le dire chez les 18-20 ans.
Face à cela, le premier réflexe des jeunes est de chercher d'autres sources d'information (54 %), même s'ils sont 34 % à déclarer n'avoir rien fait. Lorsqu'ils souhaitent apprendre de nouvelles choses sur un sujet, ils se tournent en premier lieu vers leurs parents (51 %), notamment lorsqu'ils ont moins de 15 ans (70 %). Les sites web constituent leur deuxième source d'information (39 %), c'est même la première chez les 18-20 ans (55 %).

Lorsqu'un événement vient de se produire et qu'ils recherchent des informations fiables, les 11-20 ans consultent d'abord le site d'un média connu (33 %) et 29 % consultent plusieurs sites pour croiser les informations. Ces deux sources sont encore plus utilisées par les 18-20 ans (39 % et 41 %).
Le premier site affiché sur Google représente leur troisième source d'information (23 %), devant Wikipédia (22 %) et les sites gérés par l'État (21 %).

Les sources d'information sur lesquelles les *fake news* sont les plus présentes arrivent aux deux dernières positions. 20 % des jeunes citent en effet YouTube et seulement 15 % les réseaux sociaux.

Dans leur grande majorité, les jeunes ne propagent pas de *fake news* : 90 % n'ont jamais utilisé le web ou les réseaux sociaux pour écrire des choses fausses sur des personnes ou des événements… mais tout de même, près d'un jeune sur dix (8 %) reconnaît l'avoir déjà fait. Dans le détail 1 % avoue le faire « souvent », 2 % « parfois » et 5 % « rarement » (ce qui suggère au moins une fois).

Synthèse du chapitre (2/2)

Les parents sensibilisent leurs enfants sur la question. 81 % d'entre eux jugent que leur enfant est suffisamment sensibilisé à la nécessité de vérifier si les informations qu'il consulte sur Internet sont vraies. 30 % sont même catégoriques, une proportion augmentant avec l'âge de l'enfant (de 21 % chez les parents des 11-14 ans à 42 % chez ceux de 18-20 ans), signe qu'il s'agit là aussi d'un processus d'apprentissage de l'usage d'Internet intégré par les parents.

Les pratiques des jeunes sont donc globalement assez vertueuses, surtout si on les compare à celles de leurs aînés. Seuls 60 % des Français affirment en effet vérifier suffisamment si les informations qu'ils consultent en ligne sont vraies.

Toutes les générations se rejoignent sur le regard qu'ils portent sur les *fake news*. 83 % des 11-20 ans et 82 % des Français jugent en effet qu'elles doivent être encadrées par la loi. Ils sont respectivement 73 % et 79 % à considérer qu'elles représentent un grave problème pour la démocratie et 57 % et 65 % à juger que c'est un problème qui ne peut pas être résolu facilement.

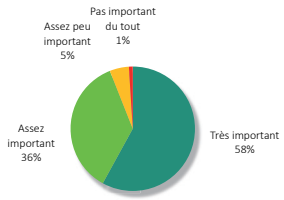
Vie privée

L'importance de protéger sa vie privée sur Internet

Aux jeunes :
Protéger ta vie privée en ligne est pour toi un sujet…

ST Pas important : 6 %

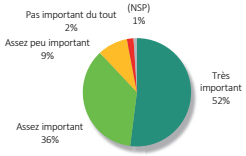
ST Important : 94 %



Aux Français :
La protection de votre vie privée sur Internet est pour vous un sujet…

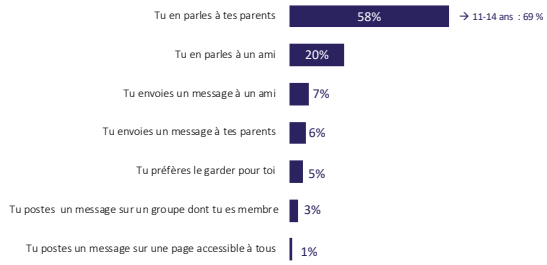
ST Pas important : 11 %

ST Important : 88 %



1ère réaction des jeunes après avoir vécu quelque chose d'important

Aux jeunes :
Tu viens de vivre quelque chose d'important, que fais-tu en premier ?



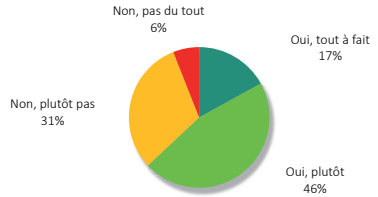
Connaissance des moyens de protéger sa vie privée sur Internet auprès des jeunes

Aux jeunes :
Connais-tu les moyens de protéger ta vie privée sur Internet ?

ST Non : 37 %

ST Oui : 63 %

→ 18-20 ans : 74 %



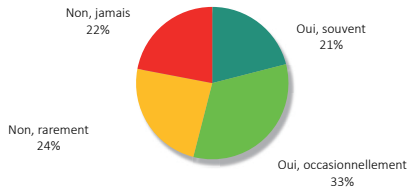
Utilisation d'outils par les jeunes pour limiter leurs traces sur Internet

Aux jeunes :
As-tu déjà utilisé des outils pour limiter tes traces sur Internet (suppression des cookies, demande de suppression de données, etc.) ?

ST Non : 46 %

ST Oui : 54 %

→ 18-20 ans : 70 %

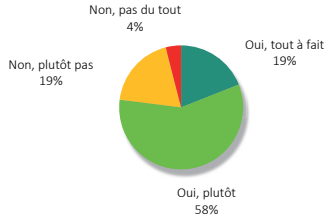


Aide parentale apportée à son enfant pour naviguer sur Internet sans risques

Aux parents de jeunes (11-20 ans) :
Considérez-vous que vous aidez votre enfant à naviguer sur Internet sans prendre de risques ?

ST Non : 23 %

ST Oui : 77 %

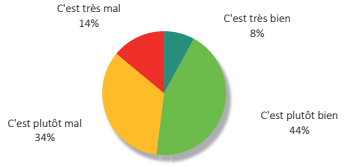


Regard des jeunes sur l'utilisation de leurs informations personnelles pour leurs proposer des produits ciblés

Aux jeunes :
Si on utilise des informations sur ton âge, tes goûts ou l'endroit où tu habites pour te proposer des produits qui te plairont, tu penses que…

ST C'est mal : 48 %

ST C'est bien : 52 %

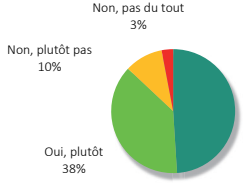


Connaissance des comptes en ligne de son enfant

Aux parents de jeunes (11-20 ans) :
Avez-vous connaissance des comptes en ligne dont dispose votre enfant sur Internet et les réseaux sociaux ?

ST Non : 13 %

ST Oui : 87 %



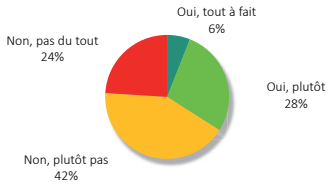
- *Parents d'un enfant de 11-14 ans : 64 %*
- *Parents d'un enfant de 15-17 ans : 43 %*
- *Parents d'un enfant de 18-20 ans : 36 %*

Sentiment que l'Éducation nationale forme son enfant à naviguer sur Internet sans prendre de risques

Aux parents de jeunes (11-20 ans) :
Considérez-vous que l'Éducation nationale forme votre enfant à naviguer sur Internet sans prendre de risques ?

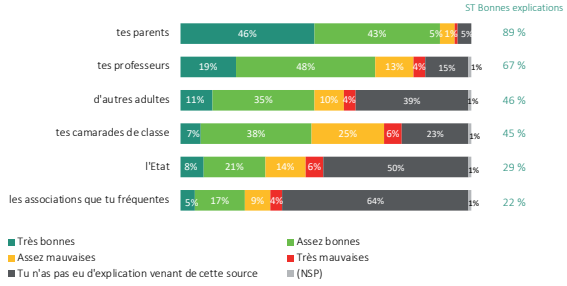
ST Non : 66 %

ST Oui : 34 %



Qualité des explications reçues par les jeunes pour naviguer sans danger sur Internet

Aux jeunes :
Les explications données par les personnes suivantes pour naviguer sans danger sur Internet ont été...

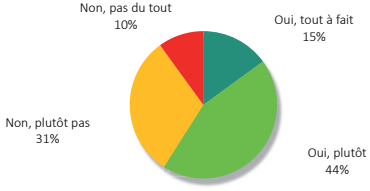


Sentiment des jeunes d'avoir été formés à un usage responsable d'Internet

Aux jeunes :
Estimes-tu avoir été formé à un usage responsable d'Internet ?

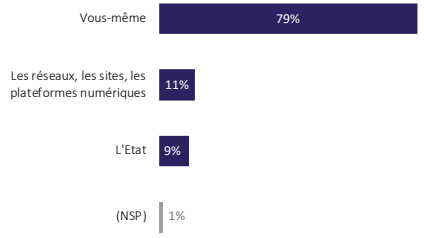
ST Non : 41 %

ST Oui : 59 %



Acteur de confiance pour protéger sa vie privée en ligne

Aux Français :
À qui faites-vous le plus confiance pour protéger votre vie privée en ligne ?

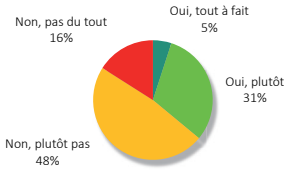


Confiance accordée par les jeunes à l' État et aux entreprises/réseaux sociaux pour protéger la vie privée en ligne

Aux jeunes :
As-tu confiance dans l'État pour protéger ta vie privée en ligne ?

ST Non : 64 %

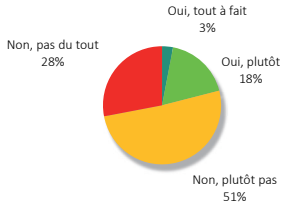
ST Oui : 36 %



Aux jeunes :
As-tu confiance dans les entreprises qui gèrent les réseaux sociaux pour protéger ta vie privée en ligne ?

ST Non : 79 %

ST Oui : 21 %

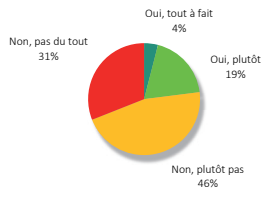


Confiance accordée par les parents à l' État et aux entreprises/réseaux sociaux pour protéger la vie privée en ligne

Aux parents de jeunes (11-20 ans) :
Faites-vous confiance à l'État pour protéger la vie privée de votre enfant en ligne ?

ST Non : 77 %

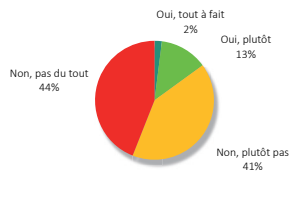
ST Oui : 23 %



Aux parents de jeunes (11-20 ans) :
Faites-vous confiance aux entreprises qui gèrent les réseaux sociaux pour protéger la vie privée de votre enfant en ligne ?

ST Non : 85 %

ST Oui : 15 %

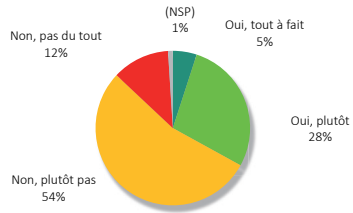


Connaissance de ses droits pour défendre/protéger sa vie privée en ligne

Aux Français :
Connaissez-vous vos droits pour protéger et défendre votre vie privée en ligne ?

ST Non : 66 %

ST Oui : 33 %



Synthèse du chapitre (1/2)

Protection de la vie privée en ligne : les jeunes sont encore plus soucieux que leurs aînés même s'ils rejettent moins le marketing personnalisé

94 % des jeunes âgés de 11 à 20 ans affirment que protéger leur vie privée en ligne est pour eux un sujet important, 58 % le considérant même comme « très » important. C'est encore davantage que l'ensemble des Français (88 %).

Dans les faits, lorsque les jeunes viennent de vivre quelque chose d'important, ils diffusent l'information essentiellement en physique et dans un cercle très restreint. 58 % nous disent qu'ils en parlent en premier lieu à leurs parents (69 % des 11-14 ans) et 20 % à un ami. Ils sont 7 % à envoyer un message à un ami et 6 % à leurs parents. Seuls 3 % des jeunes postent un message sur un groupe dont ils sont membres et 1 % sur une page accessible à tous.

Question technique, les jeunes sont plutôt bien informés, surtout lorsqu'ils avancent dans l'âge. 63 % des 11-20 ans déclarent connaître les moyens de protéger leur vie privée sur Internet (74 % des 18-20 ans) et 54 % d'entre eux ont déjà utilisé des outils pour limiter leurs traces sur le web (70 % des 18-20 ans).

Concernant le marketing personnalisé, 52 % des 11-20 ans nous disent en effet qu'ils pensent que c'est bien d'utiliser les informations sur leur âge, leurs goûts ou l'endroit où ils habitent pour leur proposer des produits qui leur plairont. Déjà, dans une enquête menée par Odoxa pour Emakina et BFM Business en mai 2018, nous constations que la majorité des 18-24 ans (53 %) appréciaient les suggestions de produits correspondant à leur profil et à leurs goûts. Une position qui décroissait avec l'âge pour se situer à 23 % chez les 65 ans et plus.

Synthèse du chapitre (2/2)

Apprentissage d'Internet : forte défiance (66 %) des parents à l'égard de l'Éducation nationale alors que les jeunes apprécient massivement la formation de leurs professeurs (67 %)

Les parents jouent un rôle central dans l'apprentissage d'Internet. Ils s'auto-congratulent d'ailleurs assez largement sur la question : 77 % d'entre eux jugent qu'ils aident leur enfant à naviguer sur Internet sans prendre de risques. Pour ce faire, ils font en sorte de savoir quels sont les comptes de leur enfant sur les réseaux sociaux : 87 % d'entre eux déclarent en avoir connaissance.

Les parents expriment toutefois une très forte défiance à l'égard de l'école pour les accompagner dans ce rôle : 66 % d'entre eux considèrent que l'Éducation nationale ne forme pas leur enfant à naviguer sur Internet sans prendre de risques.

Les jeunes battent cette idée en brèche. Si les choses sont encore perfectibles (seuls 59 % des 11-20 ans estiment avoir été formés à un usage responsable d'Internet), ils apprécient les explications données par leurs professeurs. 67 % les ont jugées bonnes contre 17 % mauvaises, 15 % n'ayant jamais eu d'explications de la part de leurs professeurs.

L'explication de ce sentiment des parents vient peut-être du fait que les Français, pris dans leur ensemble, comptent essentiellement sur eux-mêmes pour protéger leur vie privée en ligne (79 %), bien davantage que sur les réseaux sociaux, les sites et les plateformes numériques (11 %) ou l'État (9 %).

Parents et jeunes se rejoignent en effet sur l'idée que ces derniers ne sont pas dignes de confiance en la matière. 64 % des jeunes de 11-20 ans et 77 % de leurs parents déclarent ainsi ne pas faire confiance à l' État pour protéger la vie privée. Ils font encore moins confiance aux entreprises qui gèrent les réseaux sociaux (79 % et 85 %).

Pourtant, depuis l'instauration du RGPD, les choses sont nettement plus encadrées, mais encore faut-il que les Français en soient bien informés : 66 % d'entre eux nous disent qu'ils ne connaissent pas leurs droits pour protéger et défendre leur vie privée en ligne.

REMERCIEMENTS

L'Institut Montaigne remercie particulièrement les personnes suivantes pour leur contribution à ce travail.

Présidents du groupe de travail

- **Gilles Babinet,** vice-président du Conseil national du numérique et conseiller numérique, Institut Montaigne (co-président)
- **Thierry Jadot,** président, Dentsu Aegis Network France, MENA et Turquie (co-président)

Rapporteurs

- **Raphaël Muller,** haut fonctionnaire (rapporteur général)
- **Julien Chartier,** haut fonctionnaire (rapporteur)
- **Théophile Lenoir,** responsable du programme Numérique, Institut Montaigne

Membres du groupe de travail

- **Michael Antioco,** professeur et responsable de faculté (marketing), EDHEC Business School
- **Justine Atlan,** directrice générale, e-Enfance
- **Annie Blandin,** professeure, IMT Atlantique
- **Olivier Bonnot,** psychiatre de l'enfant et de l'adolescent, CHU et Université de Nantes
- **Clotilde du Fretay,** secrétaire générale adjointe, AXA Prévention
- **David Giblas,** *Chief Innovation, Health, Digital, Data and AI Officer,* Malakoff Médéric
- **José Giudicelli,** délégué académique au Numérique, Académie de Corse
- **Valérie Marty,** ancienne présidente, Fédération des parents d'élèves de l'enseignement public (PEEP)

- **Anne Muxel,** directrice de recherches en sociologie et en science politique, CNRS (CEVIPOF/Sciences Po)
- **François-Xavier Petit,** directeur général, Matrice
- **Hugo Roy,** *Associate,* Baker & McKenzie

Ainsi que

- **Joan Elbaz,** assistante chargée d'études, Institut Montaigne
- **Margaux Tellier,** assistante chargée d'études, Institut Montaigne
- **Paula Martinez,** assistante chargée d'études, Institut Montaigne
- **Julie Van Muylders,** assistante chargée d'études, Institut Montaigne

Les personnes auditionnées ou rencontrées dans l'élaboration de ce travail

- **Serge Abiteboul,** membre du collège, ARCEP
- **Imanne Agha,** chargée de mission « prévention et violence », Ministère de l'Éducation nationale
- **Delphine Auffret,** directrice de programme, Internet Sans Crainte
- **Erwan Balanant,** député de la huitième circonscription du Finistère
- **Serge Barbet,** directeur, Centre de liaison de l'enseignement et des médias de l'information
- **Vincent Barbey,** sous-directeur de la sécurité publique et de la sécurité routière, Ministère de l'Intérieur
- **Laurent Bitouzet,** chef du SIRPA, Gendarmerie nationale
- **Alice Bougnères,** déléguée générale, Alma
- **Manuel Bouvard,** professeur au Pôle universitaire de psychiatrie de l'enfant et de l'adolescent, Hôpital Charles Perrens
- **Thierry Dor,** associé, Gide Loyrette Nouel
- **Emmanuel Durand,** président-directeur général, Snap Inc. France
- **Deborah Elalouf,** présidente fondatrice, TRALALERE
- **Cathy Excoffier,** directrice déléguée RSE, Orange France
- **Elise Fajgeles,** chargée de mission Lutte contre les discriminations et contre la haine en ligne, Délégation interministérielle à la lutte contre le racisme, l'antisémitisme, et la haine anti-LGBT
- **Nora Fraisse,** présidente-fondatrice, Marion Fraisse la main tendue
- **Édouard Geffray,** directeur général de l'enseignement scolaire, Ministères de l'Éducation nationale et de l'Enseignement supérieur
- **Benoit Gobin,** proviseur adjoint du lycée Le Corbusier, Aubervilliers
- **Jean Gonié,** directeur Europe, Affaires Publiques, Snap Inc.
- **Jérôme Grondeux,** inspecteur général de l'Éducation nationale
- **Yohannes Hommel,** conseiller « Numérique et réseaux sociaux », Délégation interministérielle à la lutte contre le racisme, l'antisémitisme, et la haine anti-LGBT
- **Jean-Marc Huart,** recteur, Académie de Nancy-Metz
- **Julian Jaursch,** *Project Director "Strengthening the Digital Public Sphere | Policy",* Stiftung Neue Verantwortung
- **Vincent Laprévote,** professeur de psychiatrie, Centre Psychothérapique de Nancy
- **Donatien Le Vaillant,** conseiller « Justice et relations internationales », Délégation interministérielle à la lutte contre le racisme, l'antisémitisme, et la haine anti-LGBT
- **Wassef Lemouchi,** chargé de mission sur le digital, Alma
- **Benoît Loutrel,** responsable de la Mission de régulation des réseaux sociaux
- **Roch-Olivier Maistre,** président, Conseil supérieur de l'audiovisuel
- **Stéphane Martin,** directeur général, Autorité de régulation professionnelle de la publicité
- **Jean-Marc Merriaux,** directeur du numérique pour l'éducation, Ministère de l'Éducation nationale
- **Aurélie Pacaud,** avocate, Gide Loyrette Nouel
- **Françoise Pétreault,** sous-directrice de la vie scolaire, des établissements et des actions socio-éducatives, Direction générale des affaires scolaires
- **Frédéric Potier,** délégué interministériel à la lutte contre le racisme, l'antisémitisme et la haine anti-LGBT
- **Elian Potier,** président, Urgence harcèlement
- **Hector de Rivoire,** responsable des affaires publiques, Microsoft France

- **Raymund Schwan,** chef du pôle hospitalo-universitaire de psychiatrie d'adultes du Grand Nancy, Centre Psychothérapique de Nancy
- **Nathalie Sonnac,** membre, Conseil supérieur de l'audiovisuel
- **Xavier Vialenc,** chef du bureau image, Gendarmerie nationale
- **Sophie Vulliet-Tavernier,** directeur des relations avec les publics et la recherche, CNIL
- **Jean-Sébastien Wallez,** *Part-Time Director*, The Family

Les opinions exprimées dans ce rapport n'engagent ni les personnes précédemment citées ni les institutions qu'elles représentent.

LES PUBLICATIONS DE L'INSTITUT MONTAIGNE

- Covid-19 : l'Asie orientale face à la pandémie (avril 2020)
- Algorithmes : contrôle des biais S.V.P. (mars 2020)
- Retraites : pour un régime équilibré (mars 2020)
- Espace : le réveil de l'Europe ? (février 2020)
- Données personnelles : comment gagner la bataille ? (décembre 2019)
- Transition énergétique : faisons jouer nos réseaux (décembre 2019)
- Religion au travail : croire au dialogue - Baromètre du Fait Religieux Entreprise 2019 (novembre 2019)
- Taxes de production : préservons les entreprises dans les territoires (octobre 2019)
- Médicaments innovants : prévenir pour mieux guérir (septembre 2019)
- Rénovation énergétique : chantier accessible à tous (juillet 2019)
- Agir pour la parité : performance à la clé (juillet 2019)
- Pour réussir la transition énergétique (juin 2019)
- Europe-Afrique : partenaires particuliers (juin 2019)
- Media polarization « à la française » ? Comparing the French and American ecosystems (mai 2019)
- L'Europe et la 5G : le cas Huawei (partie 2, mai 2019)
- L'Europe et la 5G : passons la cinquième ! (partie 1, mai 2019)
- Système de santé : soyez consultés ! (avril 2019)
- Travailleurs des plateformes : liberté oui, protection aussi (avril 2019)
- Action publique : pourquoi faire compliqué quand on peut faire simple (mars 2019)
- La France en morceaux : baromètre des Territoires 2019 (février 2019)
- Énergie solaire en Afrique : un avenir rayonnant ? (février 2019)
- IA et emploi en santé : quoi de neuf docteur ? (janvier 2019)
- Cybermenace : avis de tempête (novembre 2018)
- Partenariat franco-britannique de défense et de sécurité : améliorer notre coopération (novembre 2018)
- Sauver le droit d'asile (octobre 2018)

- Industrie du futur, prêts, partez! (septembre 2018)
- La fabrique de l'islamisme (septembre 2018)
- Protection sociale : une mise à jour vitale (mars 2018)
- Innovation en santé : soignons nos talents (mars 2018)
- Travail en prison : préparer (vraiment) l'après (février 2018)
- ETI : taille intermédiaire, gros potentiel (janvier 2018)
- Réforme de la formation professionnelle : allons jusqu'au bout! (janvier 2018)
- Espace : l'Europe contre-attaque? (décembre 2017)
- Justice : faites entrer le numérique (novembre 2017)
- Apprentissage : les trois clés d'une véritable transformation (octobre 2017)
- Prêts pour l'Afrique d'aujourd'hui? (septembre 2017)
- Nouveau monde arabe, nouvelle « politique arabe » pour la France (août 2017)
- Enseignement supérieur et numérique : connectez-vous! (juin 2017)
- Syrie : en finir avec une guerre sans fin (juin 2017)
- Énergie : priorité au climat! (juin 2017)
- Quelle place pour la voiture demain? (mai 2017)
- Sécurité nationale : quels moyens pour quelles priorités? (avril 2017)
- Tourisme en France : cliquez ici pour rafraîchir (mars 2017)
- L'Europe dont nous avons besoin (mars 2017)
- Dernière chance pour le paritarisme de gestion (mars 2017)
- L'impossible État actionnaire? (janvier 2017)
- Un capital emploi formation pour tous (janvier 2017)
- Économie circulaire, réconcilier croissance et environnement (novembre 2016)
- Traité transatlantique : pourquoi persévérer (octobre 2016)
- Un islam français est possible (septembre 2016)
- Refonder la sécurité nationale (septembre 2016)
- Bremain ou Brexit : Europe, prépare ton avenir! (juin 2016)
- Réanimer le système de santé - Propositions pour 2017 (juin 2016)
- Nucléaire : l'heure des choix (juin 2016)
- Un autre droit du travail est possible (mai 2016)
- Les primaires pour les Nuls (avril 2016)
- Le numérique pour réussir dès l'école primaire (mars 2016)
- Retraites : pour une réforme durable (février 2016)
- Décentralisation : sortons de la confusion / Repenser l'action publique dans les territoires (janvier 2016)
- Terreur dans l'Hexagone (décembre 2015)
- Climat et entreprises : de la mobilisation à l'action / Sept propositions pour préparer l'après-COP21 (novembre 2015)
- Discriminations religieuses à l'embauche : une réalité (octobre 2015)
- Pour en finir avec le chômage (septembre 2015)
- Sauver le dialogue social (septembre 2015)
- Politique du logement : faire sauter les verrous (juillet 2015)
- Faire du bien vieillir un projet de société (juin 2015)
- Dépense publique : le temps de l'action (mai 2015)
- Apprentissage : un vaccin contre le chômage des jeunes (mai 2015)
- Big Data et objets connectés. Faire de la France un champion de la révolution numérique (avril 2015)
- Université : pour une nouvelle ambition (avril 2015)
- Rallumer la télévision : 10 propositions pour faire rayonner l'audiovisuel français (février 2015)
- Marché du travail : la grande fracture (février 2015)
- Concilier efficacité économique et démocratie : l'exemple mutualiste (décembre 2014)
- Résidences Seniors : une alternative à développer (décembre 2014)
- Business schools : rester des champions dans la compétition internationale (novembre 2014)
- Prévention des maladies psychiatriques : pour en finir avec le retard français (octobre 2014)
- Temps de travail : mettre fin aux blocages (octobre 2014)
- Réforme de la formation professionnelle : entre avancées, occasions manquées et pari financier (septembre 2014)
- Dix ans de politiques de diversité : quel bilan? (septembre 2014)
- Et la confiance, bordel? (août 2014)
- Gaz de schiste : comment avancer (juillet 2014)
- Pour une véritable politique publique du renseignement (juillet 2014)

- Rester le leader mondial du tourisme, un enjeu vital pour la France (juin 2014)
- 1 151 milliards d'euros de dépenses publiques : quels résultats ? (février 2014)
- Comment renforcer l'Europe politique (janvier 2014)
- Améliorer l'équité et l'efficacité de l'assurance-chômage (décembre 2013)
- Santé : faire le pari de l'innovation (décembre 2013)
- Afrique-France : mettre en œuvre le co-développement Contribution au XXVIe sommet Afrique-France (décembre 2013)
- Chômage : inverser la courbe (octobre 2013)
- Mettre la fiscalité au service de la croissance (septembre 2013)
- Vive le long terme ! Les entreprises familiales au service de la croissance et de l'emploi (septembre 2013)
- Habitat : pour une transition énergétique ambitieuse (septembre 2013)
- Commerce extérieur : refuser le déclin
  Propositions pour renforcer notre présence dans les échanges internationaux (juillet 2013)
- Pour des logements sobres en consommation d'énergie (juillet 2013)
- 10 propositions pour refonder le patronat (juin 2013)
- Accès aux soins : en finir avec la fracture territoriale (mai 2013)
- Nouvelle réglementation européenne des agences de notation : quels bénéfices attendre ? (avril 2013)
- Remettre la formation professionnelle au service de l'emploi et de la compétitivité (mars 2013)
- Faire vivre la promesse laïque (mars 2013)
- Pour un « New Deal » numérique (février 2013)
- Intérêt général : que peut l'entreprise ? (janvier 2013)
- Redonner sens et efficacité à la dépense publique 15 propositions pour 60 milliards d'économies (décembre 2012)
- Les juges et l'économie : une défiance française ? (décembre 2012)
- Restaurer la compétitivité de l'économie française (novembre 2012)
- Faire de la transition énergétique un levier de compétitivité (novembre 2012)
- Réformer la mise en examen Un impératif pour renforcer l'État de droit (novembre 2012)
- Transport de voyageurs : comment réformer un modèle à bout de souffle ? (novembre 2012)
- Comment concilier régulation financière et croissance : 20 propositions (novembre 2012)
- Taxe professionnelle et finances locales : premier pas vers une réforme globale ? (septembre 2012)
- Remettre la notation financière à sa juste place (juillet 2012)
- Réformer par temps de crise (mai 2012)
- Insatisfaction au travail : sortir de l'exception française (avril 2012)
- Vademecum 2007 – 2012 : Objectif Croissance (mars 2012)
- Financement des entreprises : propositions pour la présidentielle (mars 2012)
- Une fiscalité au service de la « social compétitivité » (mars 2012)
- La France au miroir de l'Italie (février 2012)
- Pour des réseaux électriques intelligents (février 2012)
- Un CDI pour tous (novembre 2011)
- Repenser la politique familiale (octobre 2011)
- Formation professionnelle : pour en finir avec les réformes inabouties (octobre 2011)
- Banlieue de la République (septembre 2011)
- De la naissance à la croissance : comment développer nos PME (juin 2011)
- Reconstruire le dialogue social (juin 2011)
- Adapter la formation des ingénieurs à la mondialisation (février 2011)
- « Vous avez le droit de garder le silence… » Comment réformer la garde à vue (décembre 2010)
- Gone for Good ? Partis pour de bon ?
  Les expatriés de l'enseignement supérieur français aux États-Unis (novembre 2010)
- 15 propositions pour l'emploi des jeunes et des seniors (septembre 2010)
- Afrique - France. Réinventer le co-développement (juin 2010)
- Vaincre l'échec à l'école primaire (avril 2010)

- Pour un Eurobond. Une stratégie coordonnée pour sortir de la crise (février 2010)
- Réforme des retraites : vers un big-bang ? (mai 2009)
- Mesurer la qualité des soins (février 2009)
- Ouvrir la politique à la diversité (janvier 2009)
- Engager le citoyen dans la vie associative (novembre 2008)
- Comment rendre la prison (enfin) utile (septembre 2008)
- Infrastructures de transport : lesquelles bâtir, comment les choisir ? (juillet 2008)
- HLM, parc privé. Deux pistes pour que tous aient un toit (juin 2008)
- Comment communiquer la réforme (mai 2008)
- Après le Japon, la France…
  Faire du vieillissement un moteur de croissance (décembre 2007)
- Au nom de l'Islam… Quel dialogue avec les minorités musulmanes en Europe ? (septembre 2007)
- L'exemple inattendu des Vets
  Comment ressusciter un système public de santé (juin 2007)
- Vademecum 2007-2012
  Moderniser la France (mai 2007)
- Après Erasmus, Amicus. Pour un service civique universel européen (avril 2007)
- Quelle politique de l'énergie pour l'Union européenne ? (mars 2007)
- Sortir de l'immobilité sociale à la française (novembre 2006)
- Avoir des leaders dans la compétition universitaire mondiale (octobre 2006)
- Comment sauver la presse quotidienne d'information (août 2006)
- Pourquoi nos PME ne grandissent pas (juillet 2006)
- Mondialisation : réconcilier la France avec la compétitivité (juin 2006)
- TVA, CSG, IR, cotisations…
  Comment financer la protection sociale (mai 2006)
- Pauvreté, exclusion : ce que peut faire l'entreprise (février 2006)
- Ouvrir les grandes écoles à la diversité (janvier 2006)
- Immobilier de l'État : quoi vendre, pourquoi, comment (décembre 2005)
- 15 pistes (parmi d'autres…) pour moderniser la sphère publique (novembre 2005)
- Ambition pour l'agriculture, libertés pour les agriculteurs (juillet 2005)
- Hôpital : le modèle invisible (juin 2005)
- Un Contrôleur général pour les Finances publiques (février 2005)
- Les oubliés de l'égalité des chances (janvier 2004 - Réédition septembre 2005)

Pour les publications antérieures se référer à notre site internet :
www.institutmontaigne.org

ABB FRANCE
ABBVIE
ACCURACY
ACTIVEO
ADIT
ADVANCY
AIR FRANCE - KLM
AIR LIQUIDE
AIRBUS
ALLEN & OVERY
ALLIANZ
ALVAREZ & MARSAL FRANCE
AMAZON WEB SERVICES
AMBER CAPITAL
AMUNDI
ARCHERY STRATEGY CONSULTING
ARCHIMED
ARDIAN
ASTORG
ASTRAZENECA
AUGUST DEBOUZY
AVRIL
AXA
BAKER & MCKENZIE
BANK OF AMERICA MERRILL LYNCH
BEARINGPOINT
BESSÉ
BNP PARIBAS
BOLLORÉ
BOUGARTCHEV MOYNE ASSOCIÉS
BOUYGUES
BROUSSE VERGEZ
BRUNSWICK
CAISSE DES DÉPÔTS
CANDRIAM
CAPGEMINI
CAPITAL GROUP
CAREIT
CARREFOUR

INSTITUT
MONTAIGNE

CASINO
CHAÎNE THERMALE DU SOLEIL
CHUBB
CIS
CISCO SYSTEMS FRANCE
CMA CGM
CNP ASSURANCES
COHEN AMIR-ASLANI
COMPAGNIE PLASTIC OMNIUM
CONSEIL SUPÉRIEUR DU NOTARIAT
CORREZE & ZAMBEZE
CRÉDIT AGRICOLE
CRÉDIT FONCIER DE FRANCE
D'ANGELIN &CO.LTD
DASSAULT SYSTÈMES
DE PARDIEU BROCAS MAFFEI
DENTSU AEGIS NETWORK
DRIVE INNOVATION INSIGHT - DII
EDF
EDHEC BUSINESS SCHOOL
EDWARDS LIFESCIENCES
ELSAN
ENEDIS
ENGIE
EQUANCY
ESL & NETWORK
ETHIQUE & DÉVELOPPEMENT
EURAZEO
EUROGROUP CONSULTING
EUROSTAR
FIVES
FONCIA GROUPE
FONCIÈRE INEA
GALILEO GLOBAL EDUCATION
GETLINK
GIDE LOYRETTE NOUEL
GOOGLE
GRAS SAVOYE
GROUPAMA

SOUTIENNENT L'INSTITUT MONTAIGNE

GROUPE EDMOND DE ROTHSCHILD
GROUPE M6
HAMEUR ET CIE
HENNER
HSBC FRANCE
IBM FRANCE
IFPASS
ING BANK FRANCE
INKARN
INSEEC
INTERNATIONAL SOS
INTERPARFUMS
IONIS EDUCATION GROUP
ISRP
JEANTET ASSOCIÉS
KANTAR
KATALYSE
KEARNEY
KEDGE BUSINESS SCHOOL
KKR
KPMG S.A.
LA BANQUE POSTALE
LA PARISIENNE ASSURANCES
LAZARD FRÈRES
LINEDATA SERVICES
LIR
LIVANOVA
L'ORÉAL
LOXAM
LVMH
M.CHARRAIRE
MACSF
MALAKOFF MÉDÉRIC
MAREMMA
MAZARS
MCKINSEY & COMPANY FRANCE
MÉDIA-PARTICIPATIONS
MEDIOBANCA
MERCER

INSTITUT
MONTAIGNE

MERIDIAM
MICHELIN
MICROSOFT FRANCE
MITSUBISHI FRANCE S.A.S
MOELIS & COMPANY
NATIXIS
NEHS
NESTLÉ
NEXITY
OBEA
ODDO BHF
ONDRA PARTNERS
ONEPOINT
ONET
OPTIGESTION
ORANGE
ORANO
ORTEC GROUPE
OWKIN
PAI PARTNERS
PERGAMON
PRICEWATERHOUSECOOPERS
PRUDENTIA CAPITAL
RADIALL
RAISE
RAMSAY GÉNÉRALE DE SANTÉ
RANDSTAD
RATP
RELX GROUP
RENAULT
REXEL
RICOL LASTEYRIE CORPORATE FINANCE
RIVOLIER
ROCHE
ROLAND BERGER
ROTHSCHILD MARTIN MAUREL
SAFRAN
SANOFI
SAP FRANCE

SCHNEIDER ELECTRIC
SERVIER
SGS
SIA PARTNERS
SIACI SAINT HONORÉ
SIEMENS FRANCE
SIER CONSTRUCTEUR
SNCF
SNCF RÉSEAU
SODEXO
SOFINORD - ARMONIA
SOLVAY
SPRINKLR
SPVIE
STAN
SUEZ
TALAN
TECNET PARTICIPATIONS SARL
TEREGA
THE BOSTON CONSULTING GROUP
TILDER
TOTAL
TRANSDEV
UBER
UBS FRANCE
UIPATH
VEOLIA
VINCI
VIVENDI
VOYAGEURS DU MONDE
WAVESTONE
WAZE
WENDEL
WILLIS TOWERS

SOUTIENNENT L'INSTITUT MONTAIGNE

INSTITUT
MONTAIGNE

COMITÉ DIRECTEUR

Imprimé en France
Dépôt légal : avril 2020
ISSN : 1771-6764

INSTITUT
MONTAIGNE

IL N'EST DÉSIR PLUS NATUREL QUE LE DÉSIR DE CONNAISSANCE

Internet : le péril jeune ?

Les enfants et adolescents grandissent en ligne comme hors ligne. Si les applications de communication peuvent renforcer les liens sociaux, elles posent également des questions pour la protection des mineurs. Cyberviolences, contenus problématiques, rapport à la vérité, protection des données personnelles : voici les quatre thèmes explorés dans ce rapport.

Sur la base des résultats de trois focus groupes et d'un sondage réalisé auprès de 3 000 enfants et adolescents âgés de 11 à 20 ans, de 1 000 parents et d'un échantillon de 1 000 personnes représentatives de la population générale, nous avons réuni un groupe de travail afin de formuler des recommandations pour protéger les enfants et adolescents en ligne - comme ils le sont hors-ligne.

Institut Montaigne
59, rue La Boétie - 75008 Paris
Tél. +33 (0)1 53 89 05 60
www.institutmontaigne.org

10 €
ISSN 1771-6764
AVRIL 2020