Point clé 11

Monde numérique : quels droits ?

Objectifs pédagogiques

Connaître ses droits en matière de protection des données personnelles

Appréhender le cyber-harcèlement et connaître les moyens de le prévenir et de le sanctionner

Repérer les contenus dangereux (fausses informations, images violentes, etc.)

Comprendre la notion de droit d'auteur

Bibliographie indicative :

- *Les réseaux sociaux, comment ça marche ?,* E. Trédez, Fleurus, 2016
- *Internet et les réseaux sociaux : que dit la loi ?,* F. Mattatia, Editions Eyrolles, 2019
- *Le droit d'auteur,* Fabrice Neaud, Emmanuel Pierrat, Lombard, 2016
- *Harcèlement en milieu scolaire, Victimes, auteurs : que faire ?,* Hélène Romano, Dunod, 2019

Ce chapitre est le fruit d'un travail collaboratif, copiloté avec la Commission Nationale de l'Informatique et des Libertés (CNIL), et associant les principaux acteurs du champ : la Haute autorité pour la diffusion des œuvres et la protection des droits sur Internet (Hadopi), l'association Génération Numérique, l'Union Nationale des Associations Familiales (UNAF), le Centre de Liaison de l'Enseignement et des Médias d'Information (CLEMI), l'association e-Enfance, le think tank Renaissance Numérique, la clinique de légistique de Université Versailles Saint-Quentin, Paris-Saclay, le Centre de Recherches Interdisciplinaires (CRI).

Monde numérique : quels droits ?

Fiche thématique 11

Cette fiche a pour objectif de faire comprendre de façon pédagogique les droits et les devoirs de chacun·e, adultes, parents, enseignant·e·s, éducateur·rice·s, animateur·rice·s, enfants et adolescent·e·s, dans un monde numérique, en particulier en matière de traitement des données personnelles et de diffusion de contenus. Elle donne également des clés pour mieux appréhender le phénomène du cyber-harcèlement, des signes annonciateurs jusqu'aux sanctions, en passant par les réflexes à adopter quand on y est confronté.

Internet constitue non seulement une source d'information sans limite, mais est également devenu un mode important d'expression et d'échanges entre les personnes. Il contribue à l'effectivité de certains droits : en favorisant l'accès aux savoirs et aux loisirs, il participe par exemple au droit à l'éducation. Il peut également constituer une voie pertinente pour faire du droit à la participation une réalité. Néanmoins, s'il est incontestablement un facteur de progrès et d'émancipation, Internet est aussi souvent le théâtre d'atteintes aux droits, notamment à la vie privée, et de violences. Qui ne connaît pas un cas de divulgation d'informations personnelles ou de cyber-harcèlement sur Internet ?

Aujourd'hui, le numérique est partout : à chaque instant, des milliards de données sont collectées, traitées, échangées à travers le monde.

Dans le cadre de ces échanges, nos données personnelles sont diffusées et font l'objet d'exploitations commerciales et ce, sans que nous en soyons toujours pleinement informés. Ces « traces numériques » rendent également possible une surveillance accrue des comportements, des faits et gestes de chacun·e, susceptible de porter atteinte aux libertés individuelles.

Face à ces enjeux réels, comment protéger nos données personnelles ? Quels sont nos droits ?

Par ailleurs, la diffusion d'informations personnelles sur Internet peut notamment donner lieu à du cyber-harcèlement. Les humiliations physiques et harcèlements subis à l'école peuvent se poursuivre sur les réseaux sociaux. Comment réagir face à ces agissements ? Quelles sont les sanctions ?

Parmi le flux de contenus qui circulent sur Internet, il n'est pas évident de démêler le vrai du faux : comment repérer les fausses informations ? Comment également se protéger face aux images choquantes ?

Enfin, derrière les publications et partages d'images, de clips musicaux à ses ami·e·s sur les réseaux, se cachent des auteurs et des autrices. Quels sont leurs droits et les droits de celles et ceux qui diffusent leurs œuvres ?

1. C'est quoi la protection des données personnelles ?

Le droit à la protection des données personnelles est un droit fondamental, consacré par la **Charte des droits fondamentaux de l'Union Européenne** (article 8).

Le Règlement général sur la protection des données (RGPD) adopté par le Parlement européen le 27 avril 2016, est entré en application dans les Etats membres le 25 mai 2018. Il s'agit, au plan européen, du principal texte de référence, intégré dans la législation française par la loi Informatique et Libertés. Ces textes ont pour objectif d'assurer à chacun·e une meilleure maîtrise de ses données personnelles en renforçant ses droits sur celles-ci (comme par exemple, le droit à l'effacement).

Premièrement, ce règlement encadre les conditions dans lesquelles les données personnelles peuvent être traitées, c'est-à-dire recueillies, enregistrées, conservées, communiquées ou même seulement consultées. Le **RGPD** prévoit, à cet effet, des règles à respecter par tous les acteurs qui traitent ces données (entreprises, administrations, écoles, responsables de sites, de réseaux sociaux, associations, etc.) et les oblige à être transparents, c'est-à-dire à informer les personnes auprès desquelles sont recueillies les données, de l'utilisation qui en sera faite.

A. Qu'est-ce qu'une donnée personnelle ?

Une donnée personnelle est toute information relative à une personne physique identifiée ou permettant de l'identifier.

Par exemple, les informations que l'on est susceptible de renseigner en ouvrant un compte sur un réseau social, en installant une application ou en allant sur un site, pour faire un achat, ou encore lors d'une simple visite ou consultation de page(s), sont des données personnelles. Il peut s'agir du nom et du prénom, d'une photo, d'une date de naissance, d'une adresse, d'un numéro de téléphone, d'un mail. Le numéro d'identification de notre ordinateur (quand il est connecté), appelé « adresse IP », fait également partie des données personnelles. Avec ces informations, on peut identifier une personne physique.

Parmi ces données personnelles, certaines sont considérées par la loi comme particulièrement « sensibles », parce qu'elles touchent à l'intimité de la personne, et que leur traitement est susceptible de donner lieu à des discriminations et à l'exclusion. Leur traitement est interdit sauf exceptions prévues par la loi. Il s'agit des données qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses, l'appartenance syndicale, les données génétiques et biométriques, les données concernant la santé, l'orientation sexuelle. Elles correspondent d'ailleurs directement à certains des 25 critères de discrimination interdits en droit français (voir la fiche thématique n°3 « Tous égaux devant la loi ? »).

B. Comment peuvent être utilisées les données personnelles ?

Les sites, applications et réseaux sociaux sur lesquels on s'inscrit ou que l'on visite simplement, peuvent conserver la trace de notre passage : soit parce qu'on leur a donné nos informations, soit parce qu'ils repèrent que l'adresse de notre ordinateur se connecte régulièrement sur telle page, soit grâce à l'utilisation de cookies, ces suites d'informations transmises par notre navigateur à un site (ils peuvent servir à mémoriser notre identifiant client auprès d'un site marchand, le contenu courant de notre panier d'achat, etc.). Ils vont utiliser ces données pour proposer des informations ou messages plus ciblés, supposés correspondre au profil et aux centres d'intérêts de la personne en fonction de ses habitudes sur Internet (achats, actualités, etc.). Par exemple, lorsque quelqu'un achète une place de concert sur un site, celui-ci peut utiliser les données recueillies pour proposer ensuite d'autres concerts du même type, du moins si la personne concernée a été informée de cette utilisation et si elle ne s'y est pas opposée.

Ces différentes utilisations de données constituent ce qu'on appelle des traitements de données personnelles. Il s'agit de toute opération portant sur des données personnelles dans la vie en ligne comme dans la vie hors ligne. Cela comprend le fait d'enregistrer, de conserver, modifier, rapprocher ces données avec d'autres données, les diffuser, etc.

Les responsables des traitements opérés sur les sites, applications, et réseaux sociaux, sont obligés d'informer les personnes de l'utilisation de leurs données personnelles (pourquoi ils recueillent des données et l'usage qu'ils en font) mais également de leurs droits en matière de traitement de leurs données personnelles.

MONTRES CONNECTÉES[1]

Cet objet connecté est souvent présenté par les fabricants comme un moyen de s'assurer en temps réel que l'enfant ne se trouve pas dans une situation anormale. Les montres connectées présentent généralement les fonctionnalités suivantes :

- Communiquer avec l'enfant (messagerie, téléphone) ;
- Savoir précisément où est situé l'enfant, avec une alerte s'il s'écarte du chemin de l'école ou d'une zone déterminée ;
- Mesurer en temps réel la santé de l'enfant, grâce à des capteurs (rythme cardiaque) ;
- Encourager l'enfant à faire du sport, à se dépenser, grâce à un traceur d'activité (nombre de pas) ;
- Divertir l'enfant avec des fonctions de prise de photo, des jeux et des applications.

Mais l'usage déraisonné d'une montre connectée avec un enfant peut aussi avoir pour conséquence, notamment, de s'introduire excessivement dans son intimité sociale ou corporelle (par exemple en permettant de surveiller la manière dont son enfant interagit dans la cours de récréation, ou comment il se comporte en classe ou lors d'un examen).

La géolocalisation, qui permet, quand elle est activée sur un Smartphone, ou une montre par exemple, de repérer les lieux fréquentés (domicile, établissements scolaires, sportifs, culturels, festifs) par la personne qui porte cet appareil, est très intrusive. Elle donne des informations sur les habitudes et modes de vie de la personne. Elle peut constituer une atteinte aux droits fondamentaux, notamment le droit au respect de la vie privée et à la liberté de circulation. C'est pourquoi il est important de savoir à qui sont transmises ces informations et à quelles fins. Aucun dispositif de géolocalisation ne peut avoir lieu sans avoir recueilli le consentement de la personne qui en fait l'objet ou qui l'utilise. Il faut aussi s'assurer qu'il existe des coordonnées ou une adresse de contact du fabricant pour exercer ses droits concernant ses données personnelles.

Montres connectées à l'école : que dit la loi ?
La loi du 3 août 2018 prévoit que, sauf circonstances particulières, l'utilisation d'un smartphone par un.e élève est interdite à l'intérieur d'une école maternelle ou élémentaire, et d'un collège. Cette interdiction peut également s'appliquer à une montre connectée dès lors qu'elle dispose des mêmes capacités de communication qu'un smartphone (carte SIM, connexion à un réseau WiFi, etc.).

C. Comment exercer ses droits à la protection de ses données personnelles ?

L'article 9 du Code civil (voir la fiche thématique n°1 « Le droit, c'est quoi ? ») dispose que « chacun a droit au respect de sa vie privée ». La vie privée doit être protégée sur Internet comme dans la vie hors ligne. Le **RGPD**, intégré dans la législation française par la loi Informatique et Libertés, renforce les droits des personnes et prévoit de nouveaux droits.

Concrètement, ces textes consacrent les droits suivants :

Le droit à l'information
Un organisme qui collecte des données personnelles doit fournir aux personnes concernées une information claire à propos de l'utilisation de leurs données et de l'exercice de leurs droits.

Avant de collecter ces données, cet organisme doit donc faire preuve de transparence et permettre aux personnes de savoir :

- Pourquoi l'organisme collecte leurs données ?
- A quelles fins les données personnelles pourront-elles être utilisées ?
- Quels sont les droits qui peuvent être exercés ? Par exemple : demander la liste des données détenues à son sujet par un responsable de traitement ; en demander l'effacement ; introduire une réclamation auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL) (voir l'encadré ci-dessous).

Ces informations sur la protection des données des utilisateurs doivent être accessibles depuis la page d'accueil du site de l'organisme sous un intitulé clair (par exemple, « politique de confidentialité », « page vie privée » ou « données personnelles »).

1. Source : https://www.cnil.fr/fr/montres-connectees-pour-enfants-quels-enjeux-pour-leur-vie-privee (2 septembre 2019). Consulté le 31 mars 2020.

Le droit d'accès
Le droit d'accès permet à toute personne de savoir si des données la concernant sont traitées par un organisme (site web, magasin, banque…) et d'en obtenir la communication dans un format compréhensible. Il permet également de contrôler l'exactitude des données et, au besoin, de les faire rectifier ou effacer.

Le droit d'opposition
Ce droit permet à toute personne de s'opposer à ce que ses données personnelles soient utilisées par un organisme pour un objectif précis. Elle doit alors mettre en avant « des raisons tenant à sa situation particulière », sauf en cas de prospection commerciale, où il est possible de s'opposer sans motif (par exemple, une personne souhaite être retirée d'un fichier d'adresses mails de clients d'un site pour ne plus recevoir d'emails publicitaires).

Le droit de rectification
Ce droit permet à toute personne de corriger des données inexactes la concernant (âge ou adresse erronés) ou de compléter des données.

Le responsable du fichier doit également communiquer aux autres destinataires des données, les rectifications apportées – par exemple aux partenaires commerciaux, sauf si une telle communication exigerait des efforts disproportionnés.

Le droit au déréférencement
Toute personne a le droit de demander aux moteurs de recherche de supprimer certains résultats de recherche associés à ses noms et prénoms. Cette suppression ne signifie pas l'effacement de l'information sur le site Internet mais la disparition du lien explicite entre cette information et l'identité de la personne (voir l'exemple ci-dessous).

COMMENT EXERCER SON DROIT AU DÉRÉFÉRENCEMENT ?

Prenons un exemple pour mieux comprendre. Tapez votre prénom et votre nom dans Google, ou un autre moteur de recherche. Vous serez peut-être surpris : des photos de soirée, un clip vidéo réalisé avec des ami·e·s pendant un séjour de vacances, votre nom parmi la liste des responsables de la section jeunesse d'un parti politique. Les résultats de la recherche font un lien entre votre identité et ces contenus. Ce ne sont pas toujours de bons souvenirs ni même des informations que vous avez envie de laisser en libre accès. Vous pouvez exercer votre droit au déréférencement en demandant à Google ou tout autre moteur de recherche, de supprimer les liens qui renvoient à certains contenus (photos, etc.) quand on tape votre nom dans le moteur de recherche. Les contenus ne sont pas supprimés et continueront d'apparaître mais sans lien explicite avec votre identité.

Les principaux moteurs de recherche mettent à disposition un formulaire de demande de suppression de résultats de recherche, dans leurs rubriques ou pages « contact », « service client », ou encore « mentions légales ».
Adressez au moteur de recherche, par le biais de son formulaire en ligne, une demande de « déréférencement d'un contenu vous concernant s'affichant dans la liste de résultats du moteur de recherche ».
Précisez bien l'adresse web (url) du résultat faisant l'objet de votre demande. Pour cela, faire un clic droit sur le lien de résultat et sélectionner « copier l'adresse du lien ».
Motivez votre demande, en indiquant au moteur de recherche pourquoi vous souhaitez que ce lien soit déréférencé : « Le contenu lié à [cette url] me concerne car il est relatif à un article sur un blog montrant ma participation à […] / un annuaire publiant mes coordonnées / etc. Or ce contenu est inexact/obsolète/excessif/publié à mon insu/uniquement lié à ma vie privée/etc. ».
Si vous subissez un impact négatif dans votre vie privée ou professionnelle du fait de ces résultats, précisez-le.
Pensez à conserver une copie de vos démarches si vous souhaitez saisir la CNIL en cas de réponse insatisfaisante ou d'absence de réponse, par exemple en réalisant des captures d'écran de votre demande de suppression et le cas échéant de la notification de refus du moteur de recherche.

Le droit à l'effacement
Si vous souhaitez aller plus loin et supprimer les photos, vidéos, images qui circulent avec votre nom, vous pouvez demander directement aux sites qui les affichent de les supprimer. C'est ce qu'on appelle le droit à l'effacement. Il permet de faire disparaître des données passées de façon définitive.

COMMENT EXERCER SON DROIT À L'EFFACEMENT ?

Vous pouvez exercer votre demande de droit d'effacement par divers moyens : par voie électronique (formulaire, adresse mail, bouton de téléchargement, etc.) ou par courrier, par exemple.

Indiquez quelles sont les données que vous souhaitez effacer. En effet, l'exercice de ce droit n'entraîne pas la suppression simple et définitive de toutes les données vous concernant qui sont détenues par l'organisme. Par exemple, une demande d'effacement de votre photo sur un site n'aboutira pas à la suppression de votre compte.

Le responsable du fichier doit procéder à l'effacement dans les meilleurs délais et au plus tard dans un délai d'un mois, qui peut être porté à trois compte tenu de la complexité de la demande. Dans ce dernier cas, l'organisme doit vous informer des raisons de cette prolongation.
Pour savoir comment exercer concrètement vos droits au déréférencement et à l'effacement, vous pouvez consulter le site de la CNIL, qui vous explique la démarche à suivre et vous donne des conseils pratiques.

D - Des dispositions spécifiques pour les données des mineurs

Le **RGPD** a également introduit pour la première fois dans le droit européen de la protection des données personnelles, des dispositions spécifiques pour les données relatives aux mineurs : ces derniers peuvent être moins conscients des risques et conséquences liées au traitement de leurs données personnelles, ainsi que de leurs droits.

Le texte prévoit, pour les mineurs en dessous d'un certain âge, le recueil du consentement des parents pour les traitements de données effectués dans le cadre de services en ligne destinés à leurs enfants, du moins pour ceux qui nécessitent le recueil du consentement de la personne concernée (par exemple pour du marketing, du profilage, etc.). La France a fixé ce seuil à 15 ans. Cela signifie que le traitement des données d'un enfant de moins de 15 ans, pour ce type de services, nécessite l'accord de ses responsables légaux au même titre que le sien.

À noter que les clauses générales d'utilisation des réseaux sociaux qui autorisent la collecte de données personnelles à partir de 13 ans, sur la base d'une loi américaine, sont sans portée légale en Europe.

Par ailleurs, le RGPD prévoit que l'information destinée à des mineurs quant à l'utilisation de leurs données doit être rédigée dans des termes clairs et facilement compréhensibles.

Le droit de rectification et le droit à l'oubli (qui recouvre les droits au déréférencement et à l'effacement) sont particulièrement importants lorsque le consentement au traitement des informations a été recueilli durant la minorité 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 au moment où les personnes étaient mineures. Les personnes concernées peuvent exercer ce droit à partir du moment où elles étaient mineures au moment de la collecte des données, avec l'aide de leurs parents si celles-ci sont toujours mineures.

Il peut arriver que les responsables légaux publient des photos de leurs enfants sur les réseaux sociaux. Ils s'exposent alors à ce que les enfants fassent valoir leur droit à l'effacement ainsi que leur droit à ne pas faire l'objet d'immixtions dans leur vie privée, consacré dans la Convention internationale des droits de l'enfant (voir la fiche thématique n°6 « Moins de 18 ans, quels droits ? »).

LA COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS

La Commission Nationale de l'Informatique et des Libertés (CNIL) est l'autorité française de protection des données chargée de veiller au respect des droits et libertés des personnes à l'égard des traitements de données personnelles et des usages du numérique et de s'assurer que ces traitements sont conformes au Règlement européen sur la protection des données personnelles (RGPD) et à la loi Informatique et Libertés. A cette fin, la CNIL conseille les professionnels sur leurs obligations en matière de création de fichiers et autres traitements informatiques de données personnelles. Elle aide les particuliers à exercer leurs droits sur leurs données et en cas de difficultés, reçoit et traite leurs plaintes, notamment en ligne.

Pour accomplir ses missions, elle dispose également de pouvoirs de contrôle et de sanction.

La CNIL est particulièrement attentive à la protection des données des enfants en particulier sur Internet et promeut, au plan national et international, une éducation au numérique et aux usages d'un Internet responsable et citoyen, protecteur des données personnelles et de la vie privée. Elle produit de nombreuses ressources pédagogiques (quizz, vidéos, affiches…) et réalise des actions de sensibilisation en direction notamment des publics jeunes et des familles. Elle est à l'origine de la création du collectif EDUCNUM en 2013 (www.educnum.fr). La CNIL peut aussi proposer au Gouvernement toutes mesures législatives ou réglementaires de nature à adapter la protection des libertés et de la vie privée à l'évolution des technologies.

Elle collabore avec ses homologues européens pour assurer le respect des règles de protection des données personnelles et contribuer à l'élaboration de positions communes et participe aux actions de coopération internationale en matière de protection des données. Par ailleurs, la CNIL est investie d'une mission générale de réflexion prospective dans le cadre de laquelle elle se tient informée de l'évolution des technologies et analyse les effets de leur utilisation sur le droit à la protection de la vie privée, l'exercice des libertés et le fonctionnement des institutions.

Des ressources sur la protection des données personnelles sont disponibles sur le site de la CNIL : www.cnil.fr.

SAISIR LE DÉFENSEUR DES DROITS

En cas de traitement discriminatoire des données personnelles (par exemple certains enfants d'un club de foot sont exclus des propositions de sortie du club car désignés sur le fichier des inscrits comme « issus d'une famille en situation de précarité économique », risquant de ne pouvoir contribuer financièrement), ou encore d'atteinte aux droits de l'enfant sur Internet (comme le harcèlement en ligne), il est également possible de saisir le Défenseur des droits, soit en lui écrivant directement ou en contactant ses délégué·e·s réparti·e·s sur toute la France pour leur expliquer la situation et leur demander des conseils. Voir toutes les informations sur **www.defenseurdesdroits.fr**.

2. C'est quoi le cyber-harcèlement ?[2]

On parle de harcèlement quand une personne est la cible de moqueries, d'humiliations, de mises à l'écart, de violences physiques intentionnelles répétées de la part d'autres personnes (bousculades, vols, surnoms méchants, insultes, rejets…). Ces attitudes d'hostilité surviennent à l'égard d'une personne, parce qu'elle est perçue comme différente : son apparence physique, ses origines, ses comportements et habitudes sont alors invoqués pour la signaler comme n'étant « pas comme les autres ». Mais le harcèlement peut aussi être lié à un conflit entre des personnes. Ces agissements entraînent une forte dégradation de l'état de santé physique et mentale de la personne victime ainsi que du climat (école, travail…) dans lequel elle évolue.

On parle de cyber-harcèlement quand ces propos et ces actes se produisent ou se poursuivent sur Internet et les réseaux sociaux. Ce sont des insultes, des commentaires malveillants postés sur un profil, des photos ou des vidéos diffusées parfois à l'insu de la personne concernée. En quelques clics, son intimité peut se trouver dévoilée à un large public, sans possibilité de faire machine arrière. La.le ou les harceleur·euse·s à l'origine du clic et de ceux qui suivent, peuvent agir « à visage découvert » ou se cacher derrière des **pseudonymes** : elles et ils se sentent alors protégé·e·s par l'anonymat. De plus, l'écran entre elles ou eux/elle ou lui et la victime diminue le sentiment de culpabilité. Les auteurs ne sont pas toujours conscients de la portée de leurs actes et n'imaginent pas que leurs actes sont répréhensibles : les sites, applications, réseaux sociaux ont mis du temps à instaurer des règles de modération et de signalement de ces publications. Elles sont encore peu connues des utilisateurs. La loi du 4 août 2014 sur l'égalité réelle entre les femmes et les hommes introduit le cyber-harcèlement comme une circonstance aggravante des harcèlements moral et sexuel dans le Code pénal. Enfin, le cyber-harcèlement en groupe est reconnu depuis l'adoption de la loi renforçant la lutte contre les violences sexuelles et sexistes du 3 août 2018.

A - Repérer

Le cyber-harcèlement, comme le harcèlement, implique plusieurs acteurs : la·le harceleur·euse, la victime et les témoins qui encouragent, restent passifs ou peuvent dénoncer.

Quelques signes avant-coureurs permettent de repérer les cas de cyber-harcèlement.

Le comportement de la victime peut changer. Elle peut développer :
- De l'anxiété, de la crainte, une faible estime de soi ;
- Des troubles du sommeil, de la fatigue ;
- Des retards, des absences ;
- Une baisse de résultats scolaires.

Elle peut se plaindre de manière récurrente, menacer de se faire du mal ou d'en faire aux autres, se replier sur elle-même, s'isoler.

Du côté de l'auteur, on peut constater :
- Une attitude agressive ou provocante ;
- Une faible empathie ;
- La participation à un groupe d'agresseurs ou harceleurs ;
- Une faible conscience de la portée de ses actes.

Le harcèlement sur les réseaux sociaux est souvent permis par des failles dans la protection des données personnelles, qui deviennent les armes des agresseur·euse·s.
Afin d'éviter une diffusion large de ses données personnelles sur Internet et de limiter les risques de harcèlement en ligne, voici quelques conseils :

D'abord, réfléchir avant de publier des informations sur soi car tout le monde peut voir ce que l'on met en ligne ;
- Utiliser un pseudonyme ;
- Ensuite, bien gérer ses paramètres de confidentialité : limiter l'audience en faisant passer son profil de public à privé ;
- Effacer régulièrement ses historiques de navigation et privilégier la navigation privée si on utilise un ordinateur qui n'est pas le sien ;
- Choisir un mot de passe un peu compliqué et ne pas le communiquer ; utiliser un mot de passe différent pour chaque compte.

B - Réagir

Conseils pour réagir au cyber-harcèlement :

Si on est victime :
- Ne pas répondre aux messages postés ;
- Garder des preuves : rassembler des éléments concrets : copie de tout contenu (messages, photos, vidéos) posté et envoyé, recueillir des témoignages ;

2. Voir les sites https://www.e-enfance.org/ et https://www.nonauharcelement.education.gouv.fr/.

- Signaler le contenu :
    - Au site, application, réseau social directement. La plupart sont équipés d'un dispositif de signalement (mail, formulaire, bouton de signalement, etc.) ;
    - Au numéro vert « Net écoute » : 0800 200 000. Gratuit, anonyme, confidentiel et ouvert du lundi au vendredi de 9h à 20h et le samedi de 9h à 18h. Les agents de Net écoute sont joignables également par email, par chat et par Messenger ;
    - Au site spécialisé de la police : via la plateforme de signalement « Pharos » ou le numéro dédié : 0811 02 02 17 ;
    - Au Défenseur des droits, en cas de harcèlement d'un enfant ou de harcèlement discriminatoire : www.defenseurdesdroits.fr.

- Bloquer l'/les auteur(s) des publications malveillantes, par exemple en allant sur son profil et en cliquant sur le bouton «Signaler ou bloquer cette personne» ;
- Se confier à un adulte : parents, professeur·e·s, personnel scolaire, associations ;
- Porter plainte même si l'identité de l'auteur n'est pas établie, auprès de la police, de la gendarmerie ou directement auprès du procureur de la République.

Il ne faut pas :
- S'isoler et penser pouvoir régler le problème seul ou penser que la situation va cesser d'elle-même ;
- Répondre aux attaques et moqueries en ligne ;
- Supprimer les contenus ou messages postés : autant de preuves qui disparaîtront !

Si on est témoin :
- Soutenir la victime ;
- En parler à une personne responsable : parents, professeur·e·s, personnel scolaire, associations, délégué·e·s de classe ;
- Signaler les contenus postés en ligne au site, réseau social.

Il ne faut pas :
- Se moquer de la victime en commentant ou en encourageant les actes de l'agresseur·euse ;
- Participer en faisant circuler les rumeurs, les images compromettantes reçues par des camarades.

Dans le cadre scolaire, lorsque, en tant que victime ou témoin, on identifie cette situation, il faut informer l'équipe éducative (enseignant·e·s, chef·fe·s d'établissement, personnels de la vie scolaire, infirmier·ère·s, etc.) de la situation, à l'appui des témoignages, des copies des contenus, etc.

La.le chef·fe d'établissement peut alors réunir une commission éducative qui rassemble toutes les personnes jugées utiles à l'examen de la situation (délégué·e·s de classe, conseiller principal d'éducation, etc.) et qui comprend au moins un·e enseignant·e et un parent d'élève. Son rôle est d'abord d'étudier la situation, puis de prononcer des mesures éducatives à l'encontre des auteurs des faits. Il doit également prévenir les parents des élèves concerné·e·s, victimes comme auteurs.

L'équipe éducative peut également tenter un dialogue avec les auteurs, leur demander de supprimer le contenu et organiser une rencontre avec la ou les victimes.

En cas d'échec, elle peut engager une procédure disciplinaire et les parents, engager des poursuites pénales.

C - Sanctionner

Le cyber-harcèlement est reconnu comme une circonstance aggravante du délit de harcèlement dans le Code pénal. Des sanctions peuvent donc être prises à l'encontre de l'agresseur, même mineur. Ce dernier voit sa responsabilité pénale engagée quel que soit son âge en fonction de sa faculté de discernement (appréciée au cas par cas par le juge des enfants). Elle ou il peut être sanctionné·e de différentes manières : mesures éducatives, sanctions éducatives, voire peines à partir de 13 ans (travail d'intérêt général, stage de citoyenneté, emprisonnement…) (voir la fiche thématique n°6 « Moins de 18 ans, quels droits ? »).

Le cyber-harcèlement peut être sanctionné d'une peine de deux ans de prison et de 30 000 € d'amende (voir tableau ci-dessous). Les peines sont alourdies à trois ans d'emprisonnement et 45 000 € d'amende lorsque les faits de cyber-harcèlement visent une personne mineure de moins de 15 ans.

Il fait partie de l'arsenal des infractions susceptibles d'être commises dans l'environnement numérique, et peut utilement être remis en perspective par un inventaire des autres outils juridiques permettant de saisir des comportements problématiques qui peuvent y être commis.

INFRACTIONS ET EXEMPLES	SANCTIONS
INJURE	
Définition : L'injure est définie comme « toute expression outrageante, terme de mépris ou invective adressé à une personne ou à un groupe ».	**Sanction civile :** La victime peut mettre en cause la responsabilité civile de l'auteur en lui demandant des dommages et intérêts. La seule constatation de l'injure suffit à lui ouvrir droit à réparation.
Types : L'injure publique est celle qui est entendue ou lue par un public (par exemple, sur un site Internet) L'injure non publique est : - Soit adressée par son auteur à sa victime sans qu'une tierce personne ne soit présente (par exemple, par SMS) ; - Soit prononcée par son auteur devant un cercle restreint de personnes partageant les mêmes intérêts (par exemple, sur un groupe WhatsApp).	**Peine simple :** L'injure non publique est passible d'une contravention de 38 € L'injure publique est passible de 12 000 € d'amende. **Circonstances aggravantes :** L'injure est aggravée si elle revêt un caractère raciste, sexiste, homophobe, transphobe et handiphobe. La peine encourue est alors portée à 1 500 € pour une injure non publique et à un an d'emprisonnement et 45 000 € d'amende pour une injure publique.
Cas particulier : l'injure postée sur un réseau social : - Si elle a été diffusée sur un compte accessible uniquement à un nombre restreint d'ami·e·s sélectionné·e·s par l'auteur des propos, il s'agit d'une injure non publique ; - Le partage sur un réseau social d'une injure peut constituer une injure en elle-même. En effet, peut être punie également la reproduction de l'injure même sous forme dubitative dès lors qu'elle vise une personne qui peut être reconnue.	**Textes applicables :** Loi du 29 juillet 1881 sur la liberté de la presse : article 33 *Peine encourue en cas d'injure publique* Code pénal : article R621-2 *Peine encourue en cas d'injure non publique* Code pénal : articles R625-8-1 *Peine encourue en cas d'injure non publique à caractère discriminatoire*

INFRACTIONS ET EXEMPLES	SANCTIONS
DIFFAMATION	
Définition : Diffamer, c'est faire injure à une personne que l'on connaît ou que l'on ne connaît pas, mais qui est reconnaissable. Peu importe que le fait en question soit vrai ou faux, mais il doit être suffisamment précis pour faire l'objet, sans difficultés, d'une vérification et d'un débat contradictoire. Il doit être possible de répondre par oui ou non à la question : « Untel a-t-il commis le fait » ? Exemple : « Le premier ministre entretient une relation extraconjugale avec telle journaliste ».	**Sanction civile :** La victime peut mettre en cause la responsabilité civile de l'auteur en lui demandant des dommages et intérêts. La seule constatation de la diffamation suffit à lui ouvrir droit à réparation. **Peine simple :** La diffamation non publique est passible d'une contravention de 38 €. La diffamation publique est passible de 12 000 € d'amende. **Circonstances aggravantes :** 1/ La diffamation est aggravée lorsqu'elle revêt un caractère raciste, sexiste, homophobe, transphobe et handiphobe. Les peines encourues sont portées à 1 500 € d'amende pour une diffamation non publique et jusqu'à un an de prison et 45 000 € d'amende pour une diffamation publique. 2/ Seule la diffamation publique est aggravée si elle vise un·e représentant·e de l'autorité publique (élu·e local·e, parlementaire, policier·ère, gendarme, magistrat·e, douanier·ère, inspecteur·rice du travail) en raison de ses fonctions. Elle est alors punissable d'une amende de 45 000 €.
Types : La diffamation est publique lorsque les propos sont susceptibles d'être entendus ou lus par un public. Elle est non publique lorsqu'elle est proférée dans un cadre strictement privé, en l'absence de tiers étrangers.	
Cas particulier : la diffamation sur un réseau social. - Si les propos ont été diffusés sur un compte fermé, accessible uniquement à un nombre restreint d'ami·e·s sélectionné·e·s par leur auteur, il s'agit d'une diffamation non publique. - Le partage sur un réseau social d'une diffamation peut constituer une diffamation en elle-même.	**Textes applicables :** Loi du 29 juillet 1881 sur la liberté de la presse : article 32 *Peines encourues en cas de diffamation publique* Code pénal : article R625-8 *Peines encourues en cas de diffamation non publique* Code pénal : article R625-8 *Peine encourue en cas de diffamation non publique à caractère discriminatoire*

INFRACTIONS ET EXEMPLES	SANCTIONS
ATTEINTE À L'INTIMITÉ DE LA VIE PRIVÉE	
Définition : La vie privée est la sphère d'intimité de la personne, qui a vocation à rester à l'abri des regards d'autrui. Le champ des éléments qui ne peuvent être rendus publics sans le consentement de la personne concernée n'a cessé de s'étendre et englobe aujourd'hui : - Les paroles prononcées dans un cadre privé ; - Les images appartenant à la personne ou la représentant : photos, vidéos ; - La voix ; - Le sexe ; - Les informations sur son domicile ou les lieux qu'elle fréquente ; - Les informations sur son état de santé ; - Ses mails privés ; - Les informations sur sa vie familiale et ses origines familiales ; - Les informations sur ses opinions / convictions politiques, religieuses ou philosophiques ; - La mort.	**Sanction civile :** La victime peut mettre en cause la responsabilité civile de l'auteur en lui demandant des dommages et intérêts. La seule constatation de l'atteinte à l'intimité de sa vie privée suffit à lui ouvrir droit à réparation. **Sanction pénale :** Le droit français sanctionne pénalement l'atteinte à l'intimité de la vie privée lorsqu'elle recouvre : - La captation, l'enregistrement ou la transmission de paroles prononcées à titre privé ou confidentiel, sans le consentement de la personne ; - la fixation (photographie), l'enregistrement ou la transmission de l'image d'une personne se trouvant dans un lieu privé, sans le consentement de celle-ci. La peine encourue s'élève à un an d'emprisonnement et 45 000 € d'amende. **Cas particulier du *revenge porn* :** La loi punit la diffusion de contenus à caractère sexuel sans l'accord de la personne concernée, par deux ans d'emprisonnement et 60 000 € d'amende.
Cas particulier : le *revenge porn* Cette expression désigne les cyber-violences à caractère sexuel. Elles renvoient à une pratique qui consiste à se venger d'une personne en rendant publics des contenus à caractère sexuel dans le but d'humilier cette personne. Ces contenus peuvent être réalisés avec ou sans l'accord de la personne concernée.	**Textes applicables :** Code pénal : article 226-1 *Peines encourues pour atteinte à l'intimité de la vie privée* Code pénal : article 226-2-1 *Peines encourues pour revenge porn*

INFRACTIONS ET EXEMPLES	SANCTIONS

LE *HAPPY SLAPPING*

Définition : Le happy slapping (ou vidéo de lynchage) correspond au fait de filmer une scène de violence subie par une personne, et ce notamment dans le but de diffuser la vidéo de l'agression sur Internet et les réseaux sociaux.

Ces faits ne sont pas incriminés lorsque l'enregistrement ou la diffusion résultent de l'exercice normal d'une profession ayant pour objet d'informer le public, ou sont réalisés afin de servir de preuve en justice.

Deux conséquences pénales s'attachent à la commission de l'infraction d'happy slapping :

- Son auteur est considéré comme **complice** de la personne coupable des atteintes à l'intégrité physique de la victime, et s'expose alors à l'application des mêmes peines que s'il se rendait coupable de ces actes de violence ;
- La diffusion de l'enregistrement est érigée en **infraction autonome**, passible de cinq ans d'emprisonnement et de 75 000 euros d'amende.

Texte applicable :

La loi du 5 mars 2007 relative à la prévention de la délinquance a créé une infraction spécifique et dédiée au *happy slapping* et introduit l'article 222-33-3 dans le Code pénal.

USURPATION D'IDENTITÉ

Définition : L'usurpation d'identité consiste à utiliser, sans l'accord de la personne, des informations permettant de l'identifier. Il peut s'agir, par exemple, de ses nom et prénom, de son adresse électronique, ou encore de photographies. Ces informations peuvent ensuite être utilisées à son insu, notamment pour souscrire sous son identité un abonnement, pour commettre des actes répréhensibles ou nuire à sa réputation.

Peine encourue :

Elle est punie d'un an d'emprisonnement et de 15 000 € d'amende.

Texte applicable :

Code pénal : article 226-4-1

Peines encourues pour usurpation d'identité en ligne ou non.

3. C'est quoi les contenus dangereux ?

A – Les fausses informations[3]

Parmi le flux inépuisable de contenus qui circulent sur Internet, il n'est pas évident de démêler le vrai du faux. Sur Internet, tout le monde peut publier, par exemple, une parodie d'un discours politique, à son cercle d'ami·e·s (voir ci-après, la partie sur les droits d'auteur). Cela se complique dès lors qu'on transmet une information prétendument sérieuse : il faut la vérifier car tout le monde ne respecte pas les codes de déontologie journalistique ou encore ceux de la recherche scientifique. Être informé est en effet un droit inscrit dans la Déclaration Universelle des Droits de l'Homme et la Constitution française. Elles précisent que le public a droit à une information de qualité, indépendante et pluraliste.

A titre d'exemple, lorsqu'il publie une information, la ou le journaliste est tenu par le code de déontologie des journalistes de vérifier tant ses informations que ses sources, et de respecter les droits des personnes. Le code de déontologie des journalistes précise par exemple que la déformation des faits, l'accusation sans preuves, le détournement d'images ou le traitement de l'information avec intention de nuire sont des fautes graves. Si une information contient des erreurs, la ou le journaliste a l'obligation de publier un démenti. En France, la « Charte d'éthique professionnelle des journalistes » a été révisée en 2011 avec l'ajout, notamment, du droit et du devoir de la protection des sources d'information des journalistes.

Les chercheur·e·s sont également tenu·e·s à un certain nombre de devoirs et d'obligations concernant leurs activités de recherche, dont la publication fait partie. Les organismes et les établissements publics d'enseignement et de recherche ont ainsi élaboré en 2015 la « Charte nationale de déontologie des métiers de la recherche » qui rappelle le cadre de l'exercice et de la communication des travaux de recherche : intégrité, honnêteté, secret professionnel, confidentialité, neutralité et transparence des liens d'intérêt, etc.

Mais bien loin de ces considérations, il existe un certain nombre de personnes ou de sites Internet prompts à faire circuler de fausses informations. Ils citeront, par exemple, des chiffres qui n'existent pas ou montreront des images qui ont été retouchées pour en déformer le sens, dans le but de soutenir leur propre discours, d'attirer le plus de lecteurs ou générer le plus de clics possible. Par exemple, on a pu lire lors des dernières élections présidentielles américaine et française que Barack Obama n'était pas réellement né aux États-Unis, que le pape soutenait le candidat Donald Trump ou encore qu'Emmanuel Macron ne souhaitait pas serrer la main des ouvriers.

Ce n'est donc pas parce qu'une information a été relayée des milliers de fois qu'elle est vraie. Avant de la partager à son réseau, il est important d'identifier la source de l'information et d'en vérifier la fiabilité. S'il s'agit d'un site, il est conseillé de vérifier sa vocation et son éditeur, en consultant les pages « A propos de » ou « Qui sommes-nous », ou encore « Contact » ou « Mentions légales » du site. Une rapide recherche sur l'auteur·rice permet également d'éprouver sa fiabilité. Enfin, chercher d'autres articles sur le sujet, émanant de sources différentes, permet de tester la véracité du récit.

A l'ère numérique, la profusion des contenus d'information met en exergue l'importance de l'éducation aux médias et à l'information afin de former, dès l'école, des citoyen·ne·s libres et éclairé·e·s. Cet enseignement transversal est désormais intégré au socle commun de compétences, de connaissances et de culture. Opérateur public de référence, le Centre pour l'éducation aux médias et à l'information (CLEMI) est chargé de la formation des enseignants dans ce domaine, de la diffusion de ressources pédagogiques et de l'organisation d'actions éducatives telles que la Semaine de la presse et des médias dans l'École.

3. Les contenus de cette partie sont, pour la plupart, issus du livret pédagogique « Info ou intox ? Ne tombe pas dans le panneau », réalisé par l'association Génération Numérique : https://asso-generationnumerique.fr/wp-content/uploads/2018/09/Livret-A4-Les-complots-rigolos-BD.pdf et de l'article « Des fake news aux multiples facettes » d'Adrien Sénécat, journaliste au Monde, en ligne sur le site du Centre pour l'éducation aux médias et à l'information (CLEMI) : https://www.clemi.fr/fr/ressources/nos-ressources-pedagogiques/ressources-pedagogiques/des-fake-news-aux-multiples-facettes.html.

B – Les images violentes, sexuelles et haineuses

35 % des 11-18 ans ont déjà été exposés à des images pornographiques sur Internet[4].

Que ce soit par accident ou volontairement, les réseaux sociaux et les Smartphones, incontournables outils de communication et de sociabilité des adolescent·e·s, peuvent les confronter à des images violentes, sexuelles et haineuses, sans qu'elles et ils aient les outils pour les décrypter, les comprendre et s'en protéger[5].

Le risque est double : d'une part, ces contenus peuvent choquer et rester gravés dans les esprits de celle ou celui qui les reçoit, et, d'autre part, ces publications peuvent les concerner et les mettre en danger.

Les images sexuelles sont problématiques quand elles sont vues par des enfants trop jeunes pour les comprendre ou qu'elles sont également violentes. L'impact peut être considérable en pleine construction de la sexualité notamment. Sans autre connaissance ou expérience du sujet, les jeunes pourront penser que la sexualité se pratique comme ces images le montrent, alors qu'il s'agit de contenus fictifs et scénarisés. Des séances obligatoires d'éducation à la sexualité planifiées en début d'année scolaire doivent permettre aux enfants et aux jeunes de mieux identifier les violences sexuelles.

Afin de profiter pleinement d'Internet, il est important de limiter pour les plus jeunes l'exposition à ces images, puis d'échanger avec l'entourage, les parents, les frères et les sœurs, les ami·e·s, sur les contenus qui circulent sur Internet.

JEUX VIDÉO[6]

Le jeu vidéo a la faculté de faire vivre aux joueur·euse·s des moments riches en émotions grâce à la diversité des titres s'adressant à tous les types de public. Les personnes mineures sont évidemment largement concernées puisque, fin 2019, 96 % des 10-17 ans étaient joueur·euse·s[7].

Dans la plupart des situations, le jeu vidéo reste une pratique de divertissement et de loisirs partagée entre ami·e·s ou en famille. Il peut cependant entraîner des pratiques excessives qui font l'objet de nombreuses tensions et préoccupations. C'est pourquoi, il est important de définir pour les joueur·euse·s mineur·e·s combien de temps et à quels moments jouer. Il faut, pour cela, prendre en compte sa consommation globale des écrans (télévision, ordinateur, smartphone, tablette), se demander ce qui attire tant dans un jeu et ne pas se couper de ses autres activités.

Pratique numérique majeure, le jeu vidéo est concerné par les droits et devoirs de chacun·e, notamment en matière de traitement des données personnelles. Quelques conseils :
- Choisir son nom de joueur·euse (pseudonyme) sans référence à son âge, son sexe ou son adresse et ne pas donner ses coordonnées personnelles (nom, prénom, adresse, mail, numéro de téléphone…) ;
- Il vaut mieux ne pas accepter de se rendre seul·e à un rendez-vous avec une personne rencontrée sur une plateforme de jeu ;
- Témoin ou victime du non-respect de la personne ou des règles du jeu, il est possible de signaler ces atteintes à la plateforme du jeu, sans oublier d'en parler à son entourage.

Les contenus de certains jeux associés notamment à la généralisation des pratiques de jeu communautaires peuvent faire émerger des comportements toxiques chez les joueur·euse·s. C'est pourquoi, il est conseillé de :
- Privilégier le jeu coopératif à la compétition qui peut conduire à déchaîner les passions ;
- Ne pas répondre aux insultes qui sont interdites et passibles de sanctions et aux provocations, ne pas participer au dénigrement collectif ;
- Témoin ou victime du non-respect de la personne ou des règles du jeu, utiliser les dispositifs mis en place dans les jeux eux-mêmes (signalement, modération) pour canaliser les comportements toxiques, sans oublier d'en parler à son entourage.

4. Enquête de Génération Numérique menée en ligne auprès de 7 225 répondants de 11 à 18 ans du 4 Novembre 2019 au 26 février 2020.
5. Voir à ce sujet, le rapport de Sophie Jehel : « Les adolescents face aux images violentes, sexuelles et haineuses : stratégies, vulnérabilités, remédiations », janvier 2018.
6. Les contenus de cet encart sont extraits du site www.pedagojeux.fr.
7. Etude SELL/Médiamétrie « Les français et le jeu vidéo », réalisée sur Internet du 2 au 27 septembre 2019, auprès d'un échantillon de 4 049 internautes de 10 ans et plus.

Depuis 2015, la loi impose que tous les jeux vidéo (qu'ils soient vendus sur support physique ou en téléchargement) comportent un logo indiquant la catégorie d'âge à laquelle ils sont destinés avec l'objectif d'éviter l'accès des personnes mineures à des contenus inadaptés. C'est la signalétique PEGI (Pan European Game Information) homologuée par les pouvoirs publics. Elle est constituée de logos correspondant aux âges suivants : 3 ans, 7 ans, 12 ans, 16 ans et 18 ans, qui s'accompagnent d'une échelle de couleur reprenant le principe des couleurs des feux de signalisation). Elle indique l'âge minimum à partir duquel le jeu peut être conseillé. Elle s'accompagne de huit « descripteurs », pictogrammes qui renseignent sur le type de contenus présents dans le jeu et justifiant la classification : violence, langage grossier, drogue, discrimination, peur, horreur, jeux de hasard, sexe et achats intégrés.

Que signifie « achats intégrés » ?
Certains jeux vidéo (appelés « free to play ») disposent d'une version de base disponible en téléchargement gratuit mais certaines portions du jeu, fonctionnalités, objets esthétiques ou de performances, mises à jour ou contenus additionnels, pourront faire l'objet d'achats ultérieurs notamment via des monnaies virtuelles ou via des systèmes de type « loot boxes » (boîtes à butin).

La vigilance quant aux dépenses induites est nécessaire d'autant que, dans certaines boutiques d'objets virtuels, les achats sont automatiquement validés sans demande de confirmation formelle, facilitant les achats non souhaités. Certains sites web illégaux proposent d'acheter ou d'échanger les monnaies et les objets virtuels en dehors du jeu contre de l'argent réel. Il s'agit d'une activité illégale qui constitue une infraction aux conditions d'utilisation des jeux. Le risque est aussi d'être victimes de personnes mal intentionnées. En effet pour procéder à de tels échanges ou achats, les joueur·euse·s doivent souvent fournir des informations relatives à leurs comptes de jeu, tels que leurs mots de passe et autres données personnelles, mais aussi des coordonnées bancaires, ce qui constitue une pratique particulièrement risquée.

LE DARKNET

Le darknet désigne un réseau dans lequel circulent des données qui ne sont pas référencées par les moteurs de recherche classiques. De plus, le partage de données y est anonyme : il est impossible de savoir qui partage quoi. Par conséquent, ce type de réseau est généralement utilisé pour des activités illégales (ce qu'on appelle la « cybercriminalité » qui recouvre les actes malveillants portant préjudice aux internautes). Les mineurs, attirés par l'anonymat de ces réseaux, peuvent ainsi courir le risque d'être exposés à des contenus non adaptés. Sur ces réseaux comme sur le réseau internet classique, il convient de préserver ses données personnelles. En résumé, se rendre sur le darknet n'est pas illégal, mais ce qu'on y fait peut l'être.

4. Le droit d'auteur, c'est quoi ?

Internet permet l'accès rapide à un nombre illimité d'œuvres en tout genre : films, séries, musiques, clips musicaux, photos, etc., que l'on peut facilement partager à son réseau (amis, famille, collègues). Il est aussi un lieu d'expression qui permet de nouvelles formes de création.

Les auteurs et autrices à l'origine de ces créations utilisent eux-mêmes les réseaux sociaux pour diffuser leurs œuvres et se faire connaître. En tant qu'auteurs et autrices, ils sont « propriétaires » de leurs œuvres, sans qu'aucune démarche particulière ne soit nécessaire. On parle alors de **propriété intellectuelle**. Cela signifie que les auteurs et autrices ont des droits sur leurs œuvres leur permettant d'en contrôler l'usage par d'autres personnes. C'est ce que définit le Code de la Propriété Intellectuelle. Par ailleurs, certaines œuvres peuvent être créées par plusieurs personnes, alors désignées comme co-auteurs ou co-autrices. Dans ce cas, l'ensemble des auteurs et autrices pourront faire valoir leurs droits de **propriété intellectuelle**.

L'auteur·rice (ou les auteur·rice·s) a le droit de divulguer son œuvre au public, de voir son nom être apposé en tant qu'auteur ou autrice de l'œuvre, ou encore de veiller à ce que son œuvre soit respectée et non utilisée à des fins qu'elle ou il ne souhaite pas (par exemple, un auteur ou une autrice peut refuser qu'une association ou un parti politique utilise son œuvre car l'auteur ou l'autrice ne partage pas les idées véhiculées par ces derniers).

Elle ou il est aussi en droit de percevoir de l'argent pour l'exploitation de ses œuvres par d'autres personnes (par exemple, la reprise d'une chanson par un chanteur ou une chanteuse), et cela jusqu'à 70 ans après sa mort (les sommes étant alors versées à ses héritiers).

A - L'auteur doit-il toujours donner son autorisation ? Oui...

Il est interdit de reproduire, traduire, adapter, exposer, représenter publiquement, distribuer ou communiquer une œuvre au public sans l'accord de l'auteur ou de l'autrice, que l'on peut contacter directement si ses coordonnées sont publiques, ou bien par l'intermédiaire de son éditeur ou éditrice, du responsable du blog, du site qui présente l'œuvre.

La contrefaçon

La **contrefaçon** est le fait de représenter ou reproduire une œuvre existante sans l'accord de l'auteur ou autrice, ou des personnes à qui les droits d'auteur ont été cédés (héritiers par exemple). Ainsi, copier une œuvre (une chanson, un album de musique, un film, une image ou autre) sur un support physique (un CD ou un DVD) ou la mettre à disposition sur Internet (c'est-à-dire « l'uploader » pour que d'autres internautes puissent y avoir accès) est interdit et puni de 3 ans d'emprisonnement et 300 000 € d'amende, ou de 7 ans d'emprisonnement et 750 000 € d'amende si elle est commise en bande organisée (article L. 335-2 du Code de la propriété intellectuelle). La victime de contrefaçon (l'auteur ou l'autrice) peut également demander réparation du préjudice subi par cette contrefaçon, sous forme de dommages et intérêts.

Dans un jugement du tribunal pour enfants de Béthune d'avril 2017[8], le juge a déclaré coupable de contrefaçon un groupe de mineurs qui avait créé un forum permettant le téléchargement d'œuvres protégées par le droit d'auteur et le partage de liens de téléchargement illicites.

La réponse graduée et la contravention de négligence caractérisée

La Haute autorité pour la diffusion des œuvres et la protection des droits sur Internet (Hadopi) est l'organisme en charge de protéger la reproduction des œuvres sur Internet. À cette fin, elle met en place la procédure de réponse graduée. Ce mécanisme de prévention consiste à rappeler au titulaire d'une connexion à Internet son obligation de veiller à ce que celle-ci ne soit pas utilisée pour mettre à disposition sur les **réseaux « pair à pair »**, des œuvres protégées par le droit d'auteur.

Ainsi, après trois avertissements restés infructueux, l'Hadopi peut décider de saisir le juge. Il s'agit de la « contravention de négligence caractérisée ». La·le titulaire de l'abonnement Internet encourt alors une peine maximale de 1 500 € (ou de 7 500 € pour les personnes morales).

En pratique, avant de partager un contenu sur Internet, l'utilisateur·rice doit vérifier si celui-ci est soumis aux droits de l'auteur ou de l'autrice. Pour cela, des indications peuvent figurer sur le site dans les conditions générales d'utilisation, dans les **mentions légales**, sous la photo ou la vidéo ou encore sous le document à télécharger. Mais attention, ce n'est pas parce que rien n'est précisé que le contenu n'est pas protégé. Il faut alors adresser une demande d'autorisation directement à l'auteur ou autrice, ou à l'éditeur du contenu (site), ou encore à la société qui gère ses droits à la place de l'auteur ou de l'autrice elle-même.

B - ... mais pas tout le temps

Une fois divulguée au public, il est possible, dans certains cas, d'utiliser une œuvre sans avoir à demander l'autorisation préalable à l'auteur ou autrice. On parle alors d'exceptions au droit d'auteur. Par exemple, l'auteur ou l'autrice ne peut interdire une représentation privée (familiale), une citation de l'œuvre à des fins d'information (discours, revues de presse) ou pédagogiques (cours) ou encore une caricature de cette dernière.

Ces règles s'appliquent dans le monde physique comme sur Internet.

8. Voir https://www.legalis.net/jurisprudences/tribunal-pour-enfants-de-bethune-jugement-du-27-avril-2017/

C - Comment regarder un film, lire un livre numérique, écouter une musique ou télécharger une photo légalement ?

Il existe, sur Internet, une multitude d'offres apparaissant respectueuses des droits de propriété intellectuelle, permettant de regarder un film ou une série, d'écouter de la musique ou de télécharger des photos, le tout légalement. Cela signifie que ces offres ont obtenu les autorisations de la part des auteurs ou autrices, ou de leurs **ayants droit** et rémunèrent ces derniers pour la diffusion de leurs œuvres.

Comment l'offre légale rémunère-t-elle les auteurs et les autrices ?

Les plateformes et services légaux redistribuent aux auteurs et autrices, et plus largement à l'industrie culturelle une partie de leurs revenus. Ces revenus proviennent de deux sources :
- pour les offres payantes : de l'abonnement (streaming musique etc.) ou de l'achat à l'unité (film, épisode de série, album…) ;
- pour les offres gratuites : de la publicité.

Où trouver l'offre légale sur Internet ?

Plus de 480 plateformes, sites et services culturels légaux sont actuellement recensés par l'Hadopi, cette liste étant disponible sur le site hadopi.fr. Pour les œuvres audiovisuelles, il existe également le moteur de recherche du Centre national du Cinéma et de l'Image Animée (CNC) qui propose un accès à l'offre légale en vidéo à la demande disponible en France.

Depuis 2012, les bibliothèques proposent le prêt numérique en bibliothèque (PNB) pour accéder légalement à de nombreux livres numériques.

L'Hadopi accompagne aussi les internautes dans les recherches d'œuvres accessibles légalement par le biais du signalement d'œuvres introuvables.

Comment reconnaître la légalité des sites Internet ?

Il est souvent difficile de savoir si un site est légal ou non. Afin de reconnaître un site illicite, il existe plusieurs indices :
- la présence de nombreuses publicités intempestives qui s'ouvrent très régulièrement (pop-up) ;
- la surreprésentation des publicités pour adultes ou de jeux en ligne ;
- la présence de publicités manifestement trompeuses ou frauduleuses (escroquerie) ;
- l'absence de moyens de paiement sécurisés et connus ;
- la présence de films actuellement diffusés en salles de cinéma ;
- l'absence de mentions légales ou la présence de mentions légales ou de conditions d'utilisations farfelues.

D - Les plateformes sont-elles responsables des contenus diffusés ?

Les plateformes (YouTube, Dailymotion, Facebook, etc.) sur lesquelles on diffuse des images, photos, vidéos, de la musique, ne sont pas considérées comme les auteurs des contenus postés par les utilisateurs, et donc non tenues responsables de ces contenus. Néanmoins, elles doivent obtenir une autorisation de la part des titulaires de droits des œuvres que les internautes mettent en ligne. Comme le précise la directive européenne sur le droit d'auteur du 17 avril 2019, les plateformes ont l'obligation de conclure des accords avec les auteurs et autrices pour que les contenus mis en ligne respectent les droits d'auteur et puissent assurer une rémunération aux auteurs et autrices.
Ainsi, les plateformes peuvent bloquer un contenu parce que sa diffusion n'est pas autorisée par le titulaire des droits, ou, dans le cas inverse, lui verser une rémunération.

Monde numérique : quels droits ?

Fiche pédagogique 11

Quelques pistes pour animer une ou plusieurs séances sur le thème : « Monde numérique : quels droits ? »

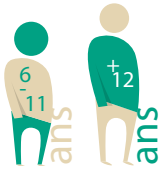
Cette fiche vous donnera quelques idées d'activités à mettre en place avec des enfants ou des jeunes, en classe ou en dehors de la classe. Libre à vous de vous en servir, d'en créer d'autres ou de les adapter à votre environnement. L'important est de rendre les enfants acteurs de la séance et de leur permettre de construire avec vous leur compréhension de leurs droits et devoirs dans un monde numérique.

	• Connaître et exercer ses droits en matière de protection des données personnelles • Appréhender le cyber-harcèlement et connaître les moyens de le prévenir et de le sanctionner • Repérer les contenus dangereux (fausses informations, images violentes, etc.) • Comprendre la notion de droits d'auteur	• Connaître et exercer ses droits en matière de protection des données personnelles • Appréhender le cyber-harcèlement et connaître les moyens de le prévenir et de le sanctionner • Repérer les contenus dangereux (fausses informations, images violentes, etc.) • Comprendre la notion de droits d'auteur
	• Un tableau • Des feuilles • Deux urnes • Des ordinateurs	• Un tableau • Des feuilles • Des plots • Des ordinateurs
	Document à imprimer ou à projeter : • Les mots croisés • L'affiche de la CNIL (annexe 1)	Document à imprimer ou à projeter : • L'affiche de la CNIL (annexe 1) • Les étiquettes des infractions et sanctions • La planche de BD vierge (annexe 4)
	• Débat – discussion • Mots croisés • Création d'affiche • Rédaction	• Débat – discussion • Mise en situation • Rédaction • Création d'un support de sensibilisation

 **Objectifs**  **Matériel** **Préparation**  **Types d'animation**

Pour commencer la séance…

Vous pouvez poser la question aux enfants et aux jeunes « Qu'a-t-on le droit de faire et de ne pas faire sur Internet et sur les Smartphones ? » afin de les interroger sur le champ des possibles et des limites que comporte l'exercice des droits sur les réseaux sociaux, les sites et les applications.



(10')

Vous pouvez recueillir leurs réponses sur un tableau divisé en deux colonnes « Ce que l'on a le droit de faire » et « Ce que l'on n'a pas le droit de faire ».

Vous pouvez, à partir des réponses données par les enfants et les jeunes, identifier des grands ensembles de sujets à aborder, comme le droit à la protection des données personnelles (respect de la vie privée), le harcèlement en ligne, le partage d'œuvres d'auteurs (musique, films, etc.).

Vous pouvez expliquer que…

Internet (sites, applications, réseaux sociaux) n'est pas une zone de non-droit et que les règles de la vie hors ligne s'appliquent aussi dans la vie en ligne.

Exemples :
- *Il est interdit de partager des informations personnelles sur une personne sans son consentement*
- *Il est interdit d'injurier et de relayer une injure visant une personne, que ce soit en privé, en public, sur Internet*
- *Il est interdit de reproduire et partager une œuvre (musique, photo, film) sans l'accord de son auteur ou autrice*

(30')

Vous pouvez demander aux enfants de trouver, par équipes, des exemples de situations de divulgation d'informations personnelles, de harcèlement ou de partage d'œuvres d'auteurs, qui peuvent avoir lieu dans la vie hors ligne comme dans la vie en ligne (sur Internet et les Smartphones). Vous pouvez ensuite leur proposer de jouer, sous forme de saynètes ces situations. Après chaque saynète, les enfants discutent afin de décrire ce qu'ils ont vu et de montrer que des règles s'appliquent dans la vie réelle comme dans la vie virtuelle.

(15')

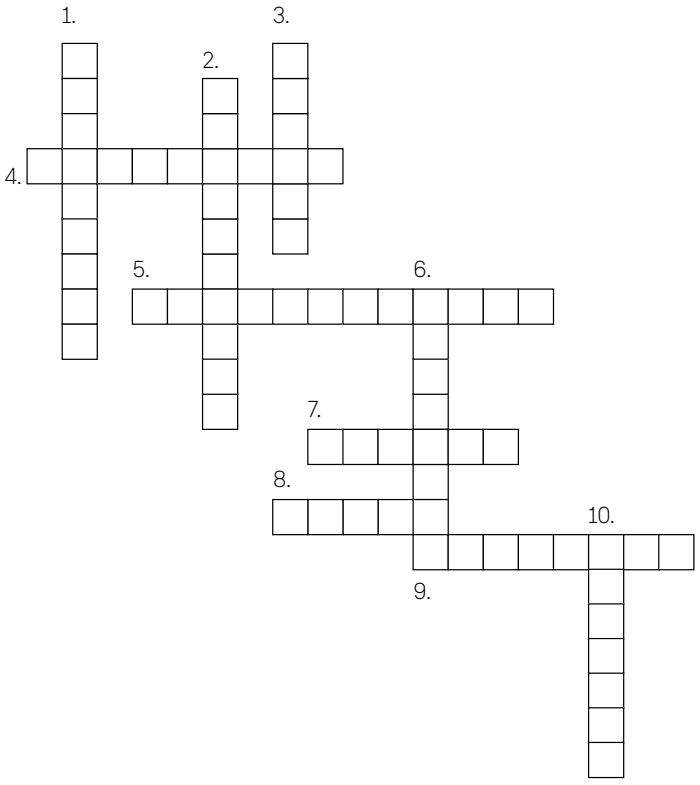
Vous pouvez demander aux jeunes de trouver des exemples de situations de divulgation d'informations personnelles, de harcèlement ou de partage d'œuvres d'auteurs, qui peuvent avoir lieu dans la vie réelle comme dans la vie virtuelle (sur Internet et les Smartphones). Ils peuvent également jouer le scénario sous forme de saynète.

La Commission Nationale de l'Informatique et des Libertés (CNIL) est l'autorité française de protection des données chargée de veiller au respect des droits et libertés des personnes à l'égard des traitements de données personnelles et des usages du numérique. Elle aide les particuliers à exercer leurs droits sur leurs données et en cas de difficultés, reçoit et traite leurs plaintes, notamment en ligne. Pour accomplir ses missions, elle dispose également de pouvoirs de contrôle et de sanction.

6 - 11 ans (30')

Vous pouvez demander aux enfants, répartis en équipes, de compléter la grille de mots croisés ci-dessous. Vous pouvez corriger à l'appui de l'affiche de la CNIL « 10 conseils de la CNIL pour rester net sur le web » (annexe 1 p. 199), en expliquant à chaque fois les conseils et les mots difficiles.

1) Sur Internet, tout le monde peut voir ce que tu mets en ligne : infos, photos, opinions. Tu dois .... avant de publier.
2) Tu es responsable de ce que tu publies en ligne alors modère tes propos sur les réseaux sociaux, forums, etc. Tu dois ... les autres.
3) Donne le minimum d'informations personnelles sur Internet. Ne communique ni tes opinions politiques, ni ta religion, ni ton numéro de téléphone. C'est ton jardin ...
4) Paramètre toujours tes profils sur les réseaux sociaux afin de rester maître des informations que tu souhaites partager. Il en va de ta ...
5) Crée ... adresses mail. Tu peux utiliser une boîte mail pour tes amis et une autre boîte mail pour les jeux et les réseaux sociaux.
6) Ne publie pas de photos gênantes de tes amis ou de toi-même car leur diffusion est incontrôlable. C'est ton ... qui est en jeu.
7) N'utilise pas ton nom et prénom en ligne : recours plutôt à un ... Seuls tes amis et ta famille sauront qu'il s'agit de toi.
8) Attention aux mots de passe. Ne les communique à personne et choisis-les un peu compliqués : ni ta date de naissance ni ton nom ! C'est ...
9) ... régulièrement tes historiques de navigation et pense à utiliser la navigation privée si tu utilises un ordinateur qui n'est pas le tien.
10) Tape régulièrement ton nom dans un moteur de recherche pour découvrir quelles informations te concernant circulent sur internet. Vérifie les ... que tu laisses derrière toi.



Réponses : 1) Réfléchir - 2) Respecter - 3) Secret
4) Sécurité - 5) Plusieurs - 6) Image
7) Pseudonyme - 8) Confidentiel
9) Efface - 10) Traces

+ 12 ans (30')

Vous pouvez répartir les jeunes en équipes. Chaque groupe pioche deux des dix conseils de la CNIL présentés sur l'affiche « 10 conseils de la CNIL pour rester net sur le web » en annexe (annexe 1 p. 199). Chaque équipe doit ensuite faire deviner les conseils en mimant une situation.

Pour naviguer sur Internet sereinement, il faut réfléchir avant de publier.

(30')

Sur une table vous pouvez installer deux urnes : je publie / je ne publie pas. Vous pouvez répartir les enfants en équipe et leur distribuer des cartes avec des exemples d'informations, des images à partager sur les réseauxsociaux et les Smartphones (voir la liste indicative ci-dessous). Vous pouvez les laisser échanger et décider, selon la situation, s'il est possible de publier sereinement ou s'il faut s'abstenir.

Quelques exemples :
- *Une photo du petit frère qui vient de naître*
  Le bébé, même si c'est votre frère, ne peut pas dire s'il est d'accord avec cette image de lui. Il vaut mieux s'en tenir au cercle familial pour diffuser cette photo.
- *Léo a trouvé une photo de son père enfant, qui lui ressemble beaucoup. Il voudrait la mettre dans sa story Snapchat…*
  Il est possible de publier cette photo si Léo a demandé l'accord de son père. Dans le cas contraire, il ne doit pas la publier.
- *Manon est partie au bord de la mer avec deux amies, elles ont pris plusieurs photos d'elles en maillot de bain. Maintenant qu'elles sont rentrées, elles ne savent pas si elles peuvent les mettre sur Instagram*
- *Une image sur laquelle on peut lire un numéro de téléphone*
- *Une capture d'écran qui me géolocalise et montre mon adresse*

Vous pouvez dépouiller les votes avec les élèves et discuter ensemble de leurs choix, à l'appui de l'affiche de la CNIL « 10 conseils de la CNIL pour rester net sur le web » (annexe 1 p. 199).

(30')

Vous pouvez organiser un débat « mouvant » sur le thème : je publie / je ne publie pas. Matérialisez au sol trois espaces avec des plots : je publie / rivière du doute / je ne publie pas.

Quelques exemples :
- *Une photo d'une carte d'identité*
- *Un post sur les réseaux sociaux « t'es gros »*
- *Un tweet « je pars en vacances deux semaines à New York ! »*
- *Une image d'un jeu en ligne avec une conversation d'une personne qui donne son adresse / identifiant à une personne qu'elle ne connaît pas*
- *Un post avec mon numéro de téléphone pour qu'on m'ajoute sur Snapchat*
- *Un dessin personnel*
- *Une photo du voisin de chambre de ma grand-mère à l'hôpital*

A chaque phrase, les jeunes se déplacent dans l'une des trois zones pour exprimer leur désaccord, doute ou accord. Faites-les réagir et échanger des arguments. Vous pouvez conclure à l'appui de l'affiche de la CNIL « 10 conseils de la CNIL pour rester net sur le web » (annexe 1 p. 199).

On parle de harcèlement quand une personne est la cible de moqueries, d'humiliations, de mises à l'écart, de violences physiques intentionnelles répétées de la part d'autres personnes. On parle de cyber-harcèlement quand ces propos et ces actes se produisent ou se poursuivent sur Internet et les réseaux sociaux. Le cyber-harcèlement est un délit puni par la loi.

(20')

Vous pouvez diffuser une vidéo du site nonauharcelement.gouv.fr et discuter avec eux des violences qu'elle met en scène. Vous pouvez les interroger sur ce que ressentent, selon eux, les personnages, sur ce qu'ils auraient fait à leur place, etc. Vous pouvez ensuite demander aux enfants de faire une affiche ou une vidéo (en groupe ou seul) contre le cyber-harcèlement et participer au prix « Non au harcèlement », en envoyant leur réalisation.

(20')

Vous pouvez présenter les situations suivantes aux jeunes :

1. **Clothilde** a 12 ans. Elle adore les jeux vidéo et a rencontré Léo sur une plateforme en ligne. Ils se parlent beaucoup. Un groupe de filles l'apprend et commence à insulter de plus en plus souvent et violemment Clotilde sur sa vie sentimentale, au collège, mais aussi en ligne à l'aide de faux comptes. Clotilde se renferme d'abord sur elle-même, puis, petit à petit, elle se rend compte qu'elle n'a pas à affronter seule le harcèlement. Elle veut que cela cesse. Elle décide d'en parler à sa professeure principale et elles trouvent une solution.

2. **Ilyès** a 14 ans. Un jour, dans les vestiaires de sport, un autre élève a pris, à son insu, une photo de lui en caleçon dans une position gênante et l'a diffusée aux élèves du collège. Ilyès est victime de nombreuses moqueries, insultes et des montages photos, notamment à caractère pornographique, sont faits de lui. Il n'ose pas en parler car il pense que c'est de sa faute. Il a des pensées très sombres et s'isole de plus en plus. Il ne peut plus supporter la situation, et décide de chercher de l'aide sur Internet.

3. **Salomé** a 16 ans. Elle est en couple depuis plusieurs mois. Son copain insiste pour qu'elle lui envoie des photos d'elle dénudée. Salomé ne se sent pas à l'aise avec cette idée mais elle finit par céder et lui envoyer une photo intime. Quelques jours plus tard, elle est visée par des insultes à caractère sexuel. Son copain a partagé la photo avec des amis qui l'ont diffusée aux élèves de leur lycée. Salomé se sent à la fois responsable de la situation et violée dans son intimité. Les insultes sont de plus en plus fréquentes et difficiles à vivre. A cela s'ajoutent des violences physiques, elle est chahutée par des élèves. Elle n'ose plus sortir de chez elle et est angoissée tous les jours à l'idée d'aller au lycée. Elle trouve le courage d'en parler à l'infirmière du collège et trouve une solution.

4. **Mathéo** a 11 ans et il est victime de cyber-harcèlement. Toutes les semaines, des élèves du collège prennent des vidéos de lui où ils le violentent, l'insultent, se moquent de lui en direct sur l'application Périscope, qui permet à l'utilisateur de retransmettre en direct ce qu'il est en train de filmer, ou dans des stories Snapchat. Mathéo ne supporte plus cette situation et il comprend que rien ne justifie qu'il subisse ce harcèlement sur les Smartphones et les réseaux sociaux. Il décide d'en parler à ses parents qui vont voir le proviseur du collège. Ce dernier convoque les harceleurs et Mathéo, pour discuter, mais le harcèlement continue malgré ce rendez-vous. Les harceleurs ne sont pas sanctionnés pour leur comportement dangereux et violent car le proviseur estime qu'il s'agit de chamailleries entre enfants. Les parents de Mathéo sont désemparés. Ils décident de saisir le Défenseur des Droits qui trouve une solution.

Vous pouvez répartir les jeunes en quatre groupes. Chaque groupe propose une ou plusieurs solutions à la situation qui lui a été attribuée.

Le cyber-harcèlement est une infraction punie par la loi et ses conséquences peuvent être très graves. Le fait que l'auteur du cyber-harcèlement soit mineur ne le dispense pas de sanctions.

Il n'est pas nécessaire d'aborder plus en détail le contenu des sanctions avec les enfants.

(30')

Vous pouvez répartir les jeunes en groupes et leur distribuer les étiquettes avec les types d'infractions, les exemples et les sanctions, afin qu'ils les fassent correspondre.
Vous trouverez les étiquettes des infractions, exemples et sanctions en annexe 2 p. 200.

Ce n'est pas parce qu'une information a été relayée des milliers de fois qu'elle est vraie. Avant de la partager à son réseau, il est important d'identifier la source de l'information et d'en vérifier la fiabilité.

(20')

Vous pouvez demander aux enfants de rédiger un court article dans le journal de leur établissement scolaire à partir de mêmes informations. Vous pouvez choisir des titres issus de l'actualité. Vous pouvez conclure en montrant que l'on peut transmettre des messages différents à partir d'une même information.

Quelques exemples :
- Chien – chasseur – champignons toxiques
- Footballeuse – accident de ski – fracture
- Panne de manège – enfants – pompiers

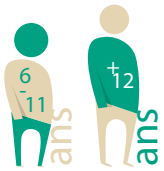
(30')

Vous pouvez demander aux jeunes de s'exercer à la fabrique de l'information en produisant leur propre média, seuls, à plusieurs, en milieu scolaire ou extra-scolaire, avec les objectifs suivants[1] :
- Comprendre comment une actualité est traitée par les médias.
- Démêler le vrai du faux : apprendre à croiser les sources et à vérifier la fiabilité d'une information.
- Aborder les règles de déontologie inhérentes à la publication d'un média.

Le site du CLEMI (www.clemi.fr) propose des conseils et des ressources pour lancer son média. Vous pourrez conclure qu'il est très simple de manipuler des informations, notamment sur internet, et de rappeler les astuces pour repérer la fiabilité d'un document :
- *Regarder le site, l'adresse, la source des images.*
- *Isoler le ou les suffixes du nom de domaine (.fr, .com, .net, etc.).*
- *Émettre des hypothèses sur la nature des documents, sur la nature de l'émetteur (entreprise, association, gouvernement…), sur ses intentions (vendre, communiquer, informer, aider, militer…), sur le pays d'implantation du site.*
- *Vérifier avec le service «whois» le propriétaire du nom de domaine. Y a-t-il dans les documents rencontrés des éléments qui permettent de connaître la qualité des auteurs (journaliste, chercheur, témoin…) ?*

1. Consulter la rubrique « médias scolaires » sur le site du CLEMI https://www.clemi.fr/fr/medias-scolaires.html ou encore le site de l'association «Jets d'Encre» qui soutient, fédère et défend la presse d'initiative jeune http://www.jetsdencre.asso.fr/.

Attention, il est interdit de reproduire, traduire, adapter, exposer, représenter publiquement, distribuer ou communiquer une œuvre au public sans l'accord de l'auteur ou autrice.



(15')

Vous pouvez demander aux enfants de repérer les différences entre les captures d'écran de sites licites et de sites illicites (voir en annexe p. 201 les exemples extraits des ressources pédagogiques de l'Hadopi)[2]. Vous pouvez corriger en indiquant l'ensemble des indices sur un tableau permettant de savoir si un site est légal ou non :

· La présence de nombreuses publicités intempestives qui s'ouvrent très régulièrement (pop-up) ;
· La surreprésentation des publicités pour adulte ou de jeux en ligne ;
· La présence de publicités manifestement trompeuses ou frauduleuses (escroquerie) ;
· L'absence de moyens de paiement sécurisés et connus ;
· La présence de films actuellement diffusés en salles de cinéma ;
· L'absence de mentions légales ou la présence de mentions légales ou de conditions d'utilisations farfelues.

L'auteur·rice (ou les auteur·rice·s) d'une œuvre a le droit de divulguer son œuvre au public, de voir son nom être apposé en tant qu'auteur ou autrice de l'œuvre, ou encore de veiller à ce que son œuvre soit respectée et non utilisée à des fins qu'elle ou il ne souhaite pas. Cependant, les droits des auteurs et autrices ne sont pas toujours respectés.

(20')

Vous pouvez demander aux enfants de réaliser une œuvre de leur choix (image, BD, musique, vidéo, etc.) et les attribuer à un autre enfant ensuite, puis détourner l'utilisation de leur œuvre (par exemple, la chanson écrite par des enfants sera utilisée dans un journal pour illustrer un article qui relaie de fausses informations). Vous pouvez recueillir les réactions des enfants/auteurs et échanger avec eux sur la notion d'auteur et d'utilisation de leurs œuvres.

(30')

Vous pouvez demander aux jeunes d'inventer un support de sensibilisation aux droits d'auteurs sous forme de bande dessinée (voir la planche vierge en annexe p. 202). Une fois leur support créé, vous pouvez les inviter à débattre sur le régime de protection qu'ils souhaitent choisir pour leur œuvre.

2. Cette activité est extraite des modules pédagogiques de l'Hadopi : https://www.hadopi.fr/ressources/modules-pedagogiques-enseignant

Il existe, sur Internet, une multitude d'offres apparaissant respectueuses des droits de propriété intellectuelle, permettant de regarder un film ou une série, d'écouter de la musique ou de télécharger des photos, le tout légalement.

Il n'est pas nécessaire d'aborder ces notions avec les enfants.

(20')

Vous pouvez exposer aux jeunes cette situation :

Léa, en classe de 6e, est fan des Frérots de la Plancha[3]. Et ce matin, au collège, tout le monde parle de leur nouvelle chanson. Lucas, son meilleur ami, lui dit qu'avec son téléphone, elle peut tout écouter en ligne. De retour à la maison, elle va voir sa grande-sœur, Maëlle, et son grand frère, Yanis, pour leur demander conseil.

Choix 1 : Léa suit le conseil de sa sœur Maëlle et obtient le fichier de musique illégalement. Pour cela, elle cherche d'abord la musique sur un site de téléchargement de musique. La recherche est longue : de nombreux liens sont inactifs et des fenêtres publicitaires s'ouvrent en permanence. Elle récupère le fichier en téléchargeant la musique illégalement sur son smartphone.

Choix 2 : Léa suit le conseil de son frère Yanis, et demande à ses parents de bénéficier de l'abonnement familial compris dans leur forfait téléphonique.

Vous pouvez demander aux jeunes de dresser les inconvénients du choix 1 en répondant aux questions suivantes à l'aide du site Hadopi.fr :

- Qui met les vidéos sur les plateformes de partage de vidéos (par exemple Youtube, Dailymotion) ?
- Les vidéos sur les sites de partage sont-elles toujours mises en ligne de manière légale ?
- Comment reconnaît-on un site légal d'un site illégal ?
- Est-ce que je risque quelque chose en allant sur les sites illégaux ? Mon smartphone risque-t-il quelque chose si je vais sur un site illégal ?

Vous pouvez ensuite demander aux jeunes de dresser les avantages du choix 2 en répondant aux questions suivantes à l'aide du site Hadopi.fr :

- Comment savoir si un site est légal ?
- Comment les artistes sont-ils rémunérés sur Internet ?
- Existe-il des sites référençant les offres légales ?
- Toutes les offres légales musicales sont-elles forcément payantes ?

3. Cette activité est extraite des modules pédagogiques de l'Hadopi : https://www.hadopi.fr/ressources/modules-pedagogiques-enseignant

Quizz « Monde numérique : quels droits ? »[4]

6/11 ans

1. Comment appelle-t-on le mot personnel qui permet d'accéder à sa boîte mail ?

A. Un mot doux
B. Un mot de passe
C. Un mot des parents

2. Comment appelle-t-on le harcèlement en ligne ?

A. Le hyper-harcèlement
B. Le cyber-harcèlement
C. Le super-harcèlement

3.Comment réagir à quelqu'un qui t'embête sur Internet ?

A. Ne rien faire
B. Le menacer
C. Le bloquer
D. Le signaler

4. Vrai ou faux : tu peux télécharger gratuitement un film ou un livre sur Internet si tes parents t'y autorisent ?

A. Vrai
B. Faux

Réponses : 1. B — **2.** B — **3.** C et D — **4.** B (si ce n'est pas sur un site officiel et payant, c'est illégal et puni par la loi).

12 ans et plus

1. Quel droit te permet de changer des informations sur toi diffusées sur Internet et qui sont inexactes ?

A. Le droit à l'erreur
B. Le droit de rectification
C. Le droit à l'oubli

2. A qui s'adresser si un site ne répond pas après une demande d'effacement de données personnelles (par exemple, une photo de toi) ?

A. Hadopi
B. Défenseur des droits
C. CNIL

3. Vrai ou faux : cliquer sur « J'aime » sur une publication se moquant d'une personne participe au cyber-harcèlement ?

A. Vrai
B. Faux

4. Sur un réseau social, quels paramètres te servent à choisir qui peut voir tes photos ? (Inco e-Enfance)

A. Les paramètres de confiance
B. Les paramètres de concurrence
C. Les paramètres de confidentialité

5. Comment s'appelle l'action de reproduire une œuvre sans l'autorisation de son/ses auteur(s) ?

A. La concurrence déloyale
B. Le piratage
C. La contrefaçon

Réponses : 1. B — **2.** C — **3.** A — **4.** C — **5.** C

4. Questions extraites de l'éventail Les Incollables® « Ta vie privée, c'est un secret », réalisé par Éditions spéciales Play Bac, en collaboration avec la Commission Nationale de l'Informatique et des Libertés (CNIL), et l'éventail Les Incollables® « Deviens un super-héros du Net » réalisé par Éditions spéciales Play Bac, en collaboration avec Association e-Enfance, protection de l'enfance sur internet. Avec l'aimable autorisation d'Élisabeth Gildé.

Cartooning for Peace : « Monde numérique : quels droits ? »

Thématiques : Droits de l'enfant, Droit et internet
Point clés : 11
Format : Exposition
Public : Elèves du secondaire
Description : À travers des caricatures sur des kakémonos, un dossier pédagogique pour les intervenants et un dossier ludique pour les élèves du secondaire, l'association Cartooning for Peace, en partenariat avec le Défenseur des droits, propose d'aborder la question « Monde numérique : quels droits ? ».
Lien pour consulter : https://educadroit.fr/sites/default/files/Livret_11_2020.pdf
Date : 2020
Auteur : L'association Cartooning for Peace, en partenariat avec le Défenseur des droits

Affiche « 10 conseils de la CNIL pour rester net sur le Web »

Thématiques : Droits de l'enfant, Droit et internet
Point clés : 6 et 11
Format : Affiche
Public : Elèves du primaire et du secondaire
Description : Cette affiche présente 10 conseils pour sensibiliser les jeunes aux problèmes de sécurité internet.
Lien pour consulter : https://www.cnil.fr/fr/10-conseils-pour-rester-net-sur-le-web
Date : 2016
Auteur : CNIL

15 minutes pour comprendre le cyber-harcèlement

Thématiques : Droits de l'enfant, Droit et internet
Point clés : 6 et 11
Format : Diaporama
Public : Elèves du primaire et du secondaire
Description : Cette fiche thématique permet de mieux comprendre le phénomène du cyber-harcèlement, ce qu'en pensent les enfants, et le vocabulaire utile pour le repérer, le prévenir et s'en protéger en… 15 minutes.
Lien pour consulter : https://www.unicef.fr/sites/default/files/fiche_thematique-myunicef-le_cyberharcelement.pdf
Date : 2019
Auteur : UNICEF France

10 conseils de la CNIL pour rester Net sur le web

1 Réfléchis avant de publier !

Sur internet, tout le monde peut voir ce que tu mets en ligne : infos, photos, opinions.

2 Respecte les autres !

Tu es responsable de ce que tu publies en ligne alors modère tes propos sur les réseaux sociaux, forums... Ne fais pas aux autres ce que tu n'aimerais pas que l'on te fasse.

3 Ne dis pas tout !

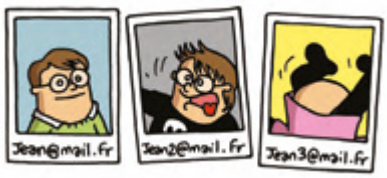
Donne le minimum d'informations personnelles sur internet. Ne communique ni tes opinions politiques, ni ta religion, ni ton numéro de téléphone...

4 Sécurise tes comptes !

Paramètre toujours tes profils sur les réseaux sociaux afin de rester maître des informations que tu souhaites partager.

5 Crée-toi plusieurs adresses e-mail !

Tu peux utiliser une boîte e-mail pour tes amis et une autre boîte e-mail pour les jeux et les réseaux sociaux.



6 Attention aux photos et aux vidéos !

Ne publie pas de photos gênantes de tes amis ou de toi-même car leur diffusion est incontrôlable.

7 Utilise un pseudonyme !

Seuls tes amis et ta famille sauront qu'il s'agit de toi.

8 Attention aux mots de passe !

Ne les communique à personne et choisis-les un peu compliqués : ni ta date ni ton surnom !

9 Fais le ménage dans tes historiques !

Efface régulièrement tes historiques de navigation et pense à utiliser la navigation privée si tu utilises un ordinateur qui n'est pas le tien.

10 Vérifie tes traces !

Tape régulièrement ton nom dans un moteur de recherche pour découvrir quelles informations te concernant circulent sur internet.

CNIL.
Commission Nationale de l'Informatique et des Libertés

Retrouvez d'autres conseils et astuces sur www.cnil.fr et sur www.educnum.fr ! #EducNum

Annexe 2 : Tableau des sanctions du cyber-harcèlement

TYPE D'INFRACTION	PEINES ENCOURUES	EXEMPLES
L'injure / l'injure publique : L'injure est définie comme « toute expression outrageante, terme de mépris ou invective adressé à une personne ou à un groupe ». - L'injure publique est celle qui est entendue ou lue par un public (ex : sur un site Internet). - Le partage sur un réseau social d'une injure peut constituer une injure en elle-même.	Si l'infraction est non publique, elle est passible d'une contravention de 38 €. Si l'infraction est publique, elle est passible de 12 000 € d'amende.	Khadija a insulté une camarade de classe sur WhatsApp.
Atteinte à l'intimité de la vie privée : - La vie privée est la sphère d'intimité de la personne, qui a vocation à rester à l'abri du regard d'autrui.	La peine encourue peut s'élever à un an d'emprisonnement et 45 000 € d'amende.	Kilian a publié un post sur un réseau social de deux professeurs en train de s'embrasser.
Le happy slapping : - Le happy slapping (ou vidéo de lynchage) correspond au fait de filmer une scène de violence subie par une personne, et ce notamment dans le but de diffuser la vidéo de l'agression sur Internet et les réseaux sociaux.	L'auteur de l'infraction est considéré comme complice de la personne coupable des atteintes à l'intégrité physique de la victime et s'expose aux mêmes peines. La diffusion de l'enregistrement est, passible de cinq ans d'emprisonnement et de 75 000 € d'amende.	Manon est bousculée et tapée par des camarades dans la cours de récréation. Jules filme la scène et la poste sur Snapchat.
Usurpation d'identité : - L'usurpation d'identité consiste à utiliser, sans l'accord de la personne, des informations permettant de l'identifier.	L'infraction est punie d'un an d'emprisonnement et de 15 000 € d'amende.	Théo crée un profil sur un réseau social au nom de son professeur de français dans le but de se faire passer pour lui.
Le revenge porn : - Cette expression désigne les cyber-violences à caractère sexuel. Elles renvoient à une pratique qui consiste à se venger d'une personne en rendant public des contenus à caractère sexuel dans le but d'humilier cette personne. Ces contenus peuvent être réalisés avec ou sans l'accord de la personne concernée.	L'infraction est punie de deux ans d'emprisonnement et 60 000 € d'amende.	Etienne a partagé une photo à caractère sexuel de Fatou à ses camarades parce qu'elle a décidé de rompre avec lui.
La diffamation : - Une diffamation consiste à dire quelque chose qui porte atteinte à l'honneur ou à la dignité d'une personne ou d'un groupe. Peu importe que le fait en question soit vrai ou faux, mais il doit être très précis. Il doit être possible de répondre par oui / non à la question : « Untel a-t-il commis le fait » ? - Le partage sur un réseau social d'une diffamation peut constituer une diffamation en elle-même.	Si l'infraction est non publique, elle est passible d'une contravention de 38 €. Si l'infraction est publique, elle est passible de 12 000 € d'amende.	Eliott a partagé sur un réseau social l'information selon laquelle la professeure de mathématiques trompe son mari avec le professeur d'anglais alors que c'est faux.

Annexe 3 : Pages d'accueil de sites licites et illicites

Hadopi

Dispositif technologique utilisé

Téléchargement direct

Points d'attention

- **Accès peu sécurisé** (présence d'un *https* mais présence aussi d'un cadenas gris avec un triangle d'avertissement jaune)
- **Films récemment sortis au cinéma**
- **Mentions étranges** (derniers films ajoutés, derniers « Blu-rays »), avec des **fautes d'orthographe** (pas d'accent)
- Choix de contenus culturels trop large ? Offre pléthorique : musique, film, jeux, dessins animés etc. - trop de choix ?
- Pas de mentions légales
- Pas de conditions générales d'utilisation ou de vente (CGU ou CGV)

Conclusion

Ce site de téléchargement est **illicite**.

En 2016, la justice a considéré que le site *zone-telechargement.com* permettait la diffusion des œuvres protégées par le droit d'auteur sans l'autorisation des titulaires de droits, et qu'il portait ainsi atteinte aux droits d'auteur. Il a été fermé.

Hadopi

Dispositif technologique utilisé

Mention du procédé torrent (réseau pair à pair)

Points d'attention

- **Nom du site douteux**
- **Choix de contenus culturels trop large ?** Offre pléthorique concernant les biens culturels disponibles : musique, audiovisuel, jeux vidéo mais aussi **contenu inadapté pour les enfants (*porn*) et case étrange « autre ».**
- **Présence de liens douteux** ou peu compréhensibles en bas de la page
- Pas de mentions légales
- Pas de conditions générales d'utilisation ou de vente (CGU ou CGV)

Conclusion

Ce site de téléchargement via réseau pair à pair est **illicite**.

Le site *the pirate bay* a été condamné par la justice suédoise en novembre 2010 pour des atteintes au *copyright* et a été fermé.

Hadopi

Dispositif technologique utilisé

Téléchargement direct ou streaming

Points d'attention

- **Accès sécurisé** (présence de *https* et d'un cadenas fermé vert)
- **Présence de mentions légales, de protection de la confidentialité et de gestion des cookies** (attention la seule mention de ces éléments n'est pas suffisante, il est important de lire les mentions légales)
- Possibilité de bénéficier d'une offre gratuite ou payante
- Possibilité d'écouter de la musique sur plusieurs supports (avantage présent sur certaines offres légales)
- Liens de la page Facebook et Twitter du site

Conclusion

Au vu des indices présents, ce site proposant de la musique peut être considéré comme licite.

Ce site n'existe pas mais a été crée pour la formation.

En cas de doute sur un site, vous pouvez consulter la page Hadopi.fr qui référence les sites et services considérés comme légaux.

Annexe 4 : Planche BD vierge