Comprendre et gérer la protection de ses données personnelles

Repères

conseil supérieur de l'éducation aux médias
CSEM
FÉDÉRATION WALLONIE-BRUXELLES

Le CSEM et l'éducation aux médias en bref

conseil supérieur de l'éducation aux médias
CSEM

Le Conseil supérieur de l'éducation aux médias (CSEM) a pour missions principales de promouvoir l'éducation aux médias et de favoriser l'échange d'informations et la coopération entre tous les acteurs et organismes concernés par l'éducation aux médias en Fédération Wallonie-Bruxelles ; notamment les secteurs des différents médias, l'enseignement obligatoire et l'éducation permanente. Le CSEM assure une large diffusion de toutes ces initiatives via le site internet www.csem.be

« Données personnelles » en bref

Une donnée personnelle est toute information permettant d'identifier directement ou indirectement une personne physique. Exemples : prénom, nom, adresse postale ou mail, date de naissance, photos, empreintes digitales, adresse IP, mot de passe, données de géolocalisation ou de santé…

L'éducation aux médias (EAM) est l'ensemble des pratiques visant le développement des connaissances, des compétences et des pratiques médiatiques de leurs bénéficiaires (désignées par l'expression « littératie médiatique ») dans le but de rendre ceux-ci actifs, autonomes, critiques, réflexifs et créatifs dans leurs usages des médias.

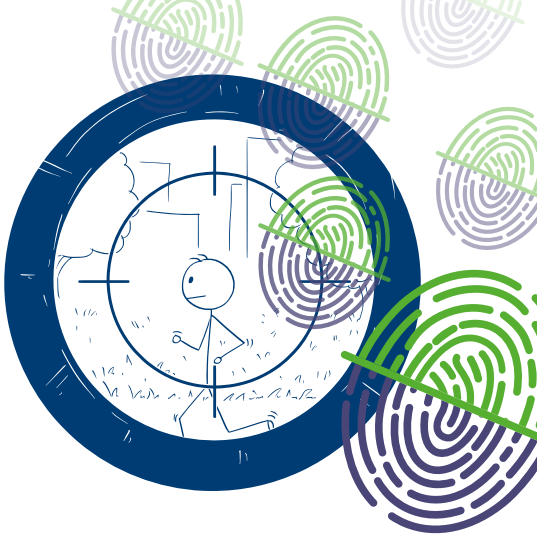
https://www.csem.be/csem/le-conseil

https://www.csem.be/csem/textes-et-avis/textes-de-positionnement-de-leducation-aux-medias

Le CSEM et les données personnelles

Le CSEM propose des pistes concrètes pour sensibiliser et accompagner les jeunes dans la gestion et la protection de leurs données personnelles. Ce carnet de la collection Repères s'adresse aussi bien aux parents qu'aux professionnels de l'éducation et de l'animation.

Pourquoi accompagner les jeunes dans la gestion de la protection de leurs données personnelles ?



Le concept de données personnelles renvoie aux notions de vie privée et de vie publique. La frontière entre ces notions est floue et mouvante.

La vie privée renvoie à la sphère intime, à ce que nous voulons garder pour nous ou nos proches, à l'abri des regards d'autrui. Elle s'oppose à la vie publique, à ce que nous décidons de partager avec le plus grand nombre. Le concept de données personnelles nous fait balancer entre vie privée et vie publique. Entre les deux, la frontière est floue : elle peut varier d'une personne à l'autre et évolue aussi au fil du temps. Prenons l'exemple de nos photos. Voici une vingtaine d'années encore, les photos restaient dans un album de famille ou sur une cheminée, donc dans la sphère privée, sans que l'on doive les protéger comme si elles étaient des données personnelles. Aujourd'hui, à l'ère d'internet et des réseaux sociaux, les photos numériques voyagent et se dupliquent beaucoup plus facilement qu'avant et peuvent vite devenir des données publiques.

L'univers du numérique nous montre une nouvelle fois son double visage avec ce sujet : il offre à la fois de formidables possibilités et perspectives tout en générant son lot de risques et de questions. Dans ce cadre, n'est-il pas nécessaire d'épauler les jeunes afin qu'ils utilisent ces outils numériques en toute connaissance de cause ? Un accompagnement d'autant plus important qu'à la suite de la pandémie liée à la Covid-19, le smartphone, la tablette et l'ordinateur se sont imposés comme des objets incontournables, plus seulement pour nos loisirs, mais aussi pour nos actes quotidiens (payement, déplacement, réservation, authentification, cours en ligne, etc.)

5h28 : c'est le temps moyen que passe quotidiennement un Belge (âgé de 16 à 64 ans) connecté à Internet.

Source : Rapport digital 2021 de l'agence We Are Social et Hootsuite.

Évolution de la protection des données

Depuis 1992, une loi belge protège les citoyens contre le traitement de leurs données personnelles. Cette loi « vie privée » a laissé sa place, en mai 2018, à une loi européenne : le Règlement Général sur la Protection des Données (RGPD).

Pour mieux protéger la vie privée de ses citoyens, l'Union européenne a adopté le RGPD. Cette base légale permet, par exemple, à un internaute de demander aux entreprises de lui communiquer les données qui le concernent. Elle lui donne aussi le droit d'en obtenir la modification voire la suppression.

L'ensemble des droits décrits par le RGPD et les démarches à suivre pour les appliquer sont à découvrir sur : *https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens_fr*

Avec l'arrivée du RGPD est née l'**Autorité de protection des données**, l'organe de contrôle indépendant chargé de veiller au respect de la protection des données en Belgique. Il est notamment chargé de donner des avis et des recommandations à propos de la protection des données, d'informer les citoyens sur le sujet, de récolter les plaintes, etc. : *https://www.autoriteprotectiondonnees.be/citoyen*

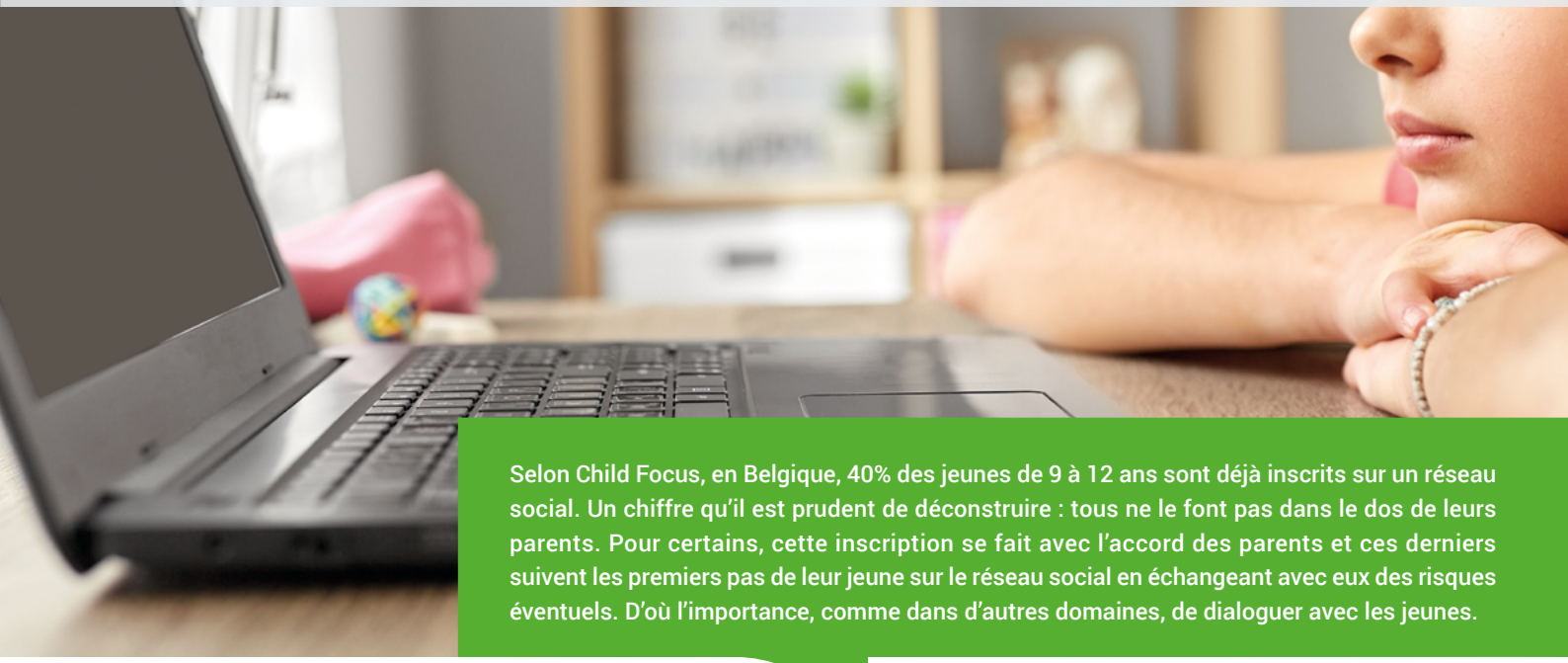
LES DONNÉES SENSIBLES

Certaines données personnelles sont dites « sensibles » : elles concernent la santé, l'origine ethnique, les opinions politiques, les convictions religieuses ou encore l'orientation sexuelle. Elles sont soumises à un traitement particulier : selon le RGPD, ces données sensibles ne peuvent, sauf exception – dont la sauvegarde de la vie humaine –, être collectées.

13 ans, la majorité numérique ?

13 ans, c'est l'âge officiellement requis pour s'inscrire sur un réseau social.

La raison ? Aux États-Unis (pays d'origine de la majorité des réseaux sociaux), la collecte de données relatives à un enfant de moins de 13 ans est interdite. 13 ans, c'est aussi l'âge à partir duquel, en Belgique, un enfant est propriétaire de ses données personnelles et de son image. À cet âge, on estime qu'il est capable de donner son propre consentement dans ce domaine : l'autorisation de ses parents - les deux, pour être précis - n'est donc plus requise. À la suite de l'arrivée du RGPD, la Belgique a fixé cette limite à 13 ans, ce qui n'est pas le cas chez nos voisins : elle est de 15 ans en France et de 16 ans au Luxembourg. Cette étape importante où le jeune devient propriétaire de ses données personnelles ne lui donne en rien la « majorité numérique », comme on l'entend souvent, à tort : jusqu'à 18 ans, ses parents sont toujours responsables, juridiquement parlant, par exemple s'il fait un achat démesuré sur Internet ou s'il expose, sans leur consentement, la photo de ses copains ou de ses professeurs sur un réseau social.



Selon Child Focus, en Belgique, 40% des jeunes de 9 à 12 ans sont déjà inscrits sur un réseau social. Un chiffre qu'il est prudent de déconstruire : tous ne le font pas dans le dos de leurs parents. Pour certains, cette inscription se fait avec l'accord des parents et ces derniers suivent les premiers pas de leur jeune sur le réseau social en échangeant avec eux des risques éventuels. D'où l'importance, comme dans d'autres domaines, de dialoguer avec les jeunes.

Les données personnelles d'un jeune en 24 heures chrono

Imaginons une journée type d'un jeune de 15 ans – on l'appellera Sacha – et des actions où il laisse des traces de ses données personnelles.

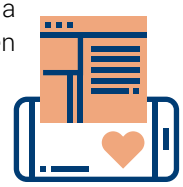
07 h 00 : Le réveil connecté de Sacha sonne. Comme tous les matins, son premier coup d'œil est pour son smartphone et ses messages arrivés durant la nuit.

07 h 23 : Sacha souhaite « bonne journée » à sa petite sœur, encore endormie, en lui enregistrant un message rigolo via son panda connecté.

07 h 29 : Le smartphone géolocalisé de Sacha lui signale, en temps réel, que son bus sera à l'arrêt, au bout de sa rue, dans 14 minutes.

07 h 32 : Sacha quitte la maison avec la musique de sa playlist dans les oreilles.

07 h 43 : En montant dans le bus, Sacha valide sa carte à puce MOBIB personnelle.



08 h 22 : Avant les cours, Sacha immortalise l'anniversaire de Charlie et en fait une story Instagram en taguant ses potes.

10 h 10 : Au cours de géographie, Sacha effectue, à la demande de son enseignant, des recherches sur son smartphone à propos des lieux qu'il a visités en Europe.

12 h 50 : Sacha paye son sandwich, sans contact, avec son smartphone, qui se déverrouille avec ses empreintes digitales.

13 h 10 : Discussion entre potes autour d'une nouvelle paire de sneakers et recherche de son meilleur prix, sur Internet. Au passage, Sacha donne son adresse électronique pour obtenir un bon de réduction.

14 h 45 : La montre connectée de Sacha lui signale ses 7812 pas déjà faits aujourd'hui. Bravo ! C'est mieux que sa moyenne hebdomadaire, à la même heure.

17 h 10 : Avant l'entraînement de volley, Sacha pose pour la photo de son équipe qui viendra alimenter le site du club.

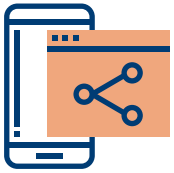
18 h 55 : Petite discussion, dans la cuisine, autour du robot ménager connecté, entre Sacha, son père et l'assistant Google, à propos de la recette de la sauce béchamel.

19 h 05 : Sacha se connecte à la plate-forme de l'école, envoie un devoir et consulte son horaire du lendemain.

20 h 25 : Sacha allume la Smart TV familiale et se connecte avec son mot de passe afin de pouvoir reprendre, au bon endroit, sa série favorite.

21 h 25 : Après une partie de jeu vidéo sur sa console, Sacha se plonge dans un manga, sur son smartphone, loué sur une plateforme en ligne.

22 h 45 : Comme tous les soirs avant d'aller dormir, le dernier coup d'œil de Sacha est pour son smart-phone.



En 24 heures,

notre jeune – que nous avons appelé Sacha –, a, via les écrans et autres objets connectés, laissé derrière lui une série de données personnelles. On sait notamment qu'il aime le volley, les sneakers, les mangas, les séries télévisées et… la sauce béchamel. Mais aussi le trajet qu'il emprunte le matin, l'école qu'il fréquente, les pays qu'il a visités ou encore le snack où il achète son sandwich le midi. Autant de données qui, comme on va le découvrir plus loin dans ce carnet, vont permettre aux réseaux sociaux et aux sites internet de lui fournir du contenu spécifique et des publicités ciblées.

« Vie privée / vie publique » : la vision des jeunes diffère de celle des adultes

Contrairement à leurs aînés, les jeunes d'aujourd'hui sont nés alors que le numérique était bien installé dans notre quotidien. Une caractéristique qui les pousse à avoir une approche différente des outils numériques mais aussi des notions de vie privée et vie publique. Petit éclairage à travers trois cas fictifs.

Mina (9 ans)

Mina regarde des vidéos sur YouTube et joue en ligne. Elle est déjà très à l'aise sur Internet. Lorsqu'elle doit donner son nom, son prénom et même son âge ou son adresse sur Internet, elle le fait sans hésiter. « Que peut-il lui arriver ? », pense-t-elle. Après tout, elle est derrière un écran…

Comment le sensibiliser davantage ?

Posez la question suivante à un jeune qui aurait le même réflexe que Mina : accepterait-il de donner son nom, son prénom, son âge et son adresse à une personne inconnue qu'il croiserait en rue ? Il est fort probable que sa réponse soit « non ». Cette réflexion devrait l'aider à se rendre compte des risques qu'il court à faire de même lorsqu'il est face à son écran.

Ahmed (13 ans)

Ahmed aime le skateboard : lorsqu'il n'est pas sur sa planche, il consulte des vidéos en ligne et des sites spécialisés dans ce type de matériel. Alors, oui, il reçoit de la publicité ciblée sur son smartphone à propos de son skate. Il en est conscient ! Mais, il préfère se voir proposer de la publicité liée à sa passion que pour des produits qui ne l'intéressent pas, comme c'est le cas à la télévision.

Comment le sensibiliser davantage ?

Avec un jeune qui aurait la même réflexion qu'Ahmed, évoquez les « bulles de filtre » qui, grâce aux algorithmes et sur les réseaux sociaux notamment, vous proposent des informations qui correspondent toujours à ce qui vous intéresse et surtout à ce que vous pensez, tout en occultant les autres avis et informations car l'objectif des réseaux sociaux est qu'on y reste le plus longtemps possible. Vous pouvez aussi le sensibiliser au phénomène de la publicité ciblée et aux sommes d'argent qui sont brassées avec la collecte de nos données personnelles (voir page 14).

Alan (16 ans)

Lorsqu'il n'est pas au cours, Alan passe une bonne partie de son temps sur les réseaux sociaux pour poster des photos et réagir à celles de ses potes. Des photos qu'il ne choisit jamais au hasard. Quitte à recommencer plusieurs fois le même cliché et à jouer avec les filtres de son application, il ne montrera jamais un portrait de lui dont il n'est pas fier : son image, il la soigne et il y tient plus que tout ! Et c'est pareil pour les photos de ses amis qu'il partage.

Comment le sensibiliser davantage ?

Avec un jeune qui aurait la même démarche qu'Alan, évoquez la question suivante : ces images postées et retravaillées avec des filtres ne montrent-elles pas un monde « lisse » qui ne correspond pas nécessairement à la réalité ?

Au-delà de ces trois situations qui permettent d'engager, avec les jeunes, le débat sur la protection des données personnelles, gardez à l'esprit qu'un jeune n'est pas l'autre. Et que le rapport qu'il entretient avec le numérique dépend d'une multitude de facteurs : son âge, son expérience avec les outils numériques, le milieu familial dans lequel il grandit, l'école qu'il fréquente et les sensibilisations à l'éducation aux médias qu'il a eues ou pas ; etc.

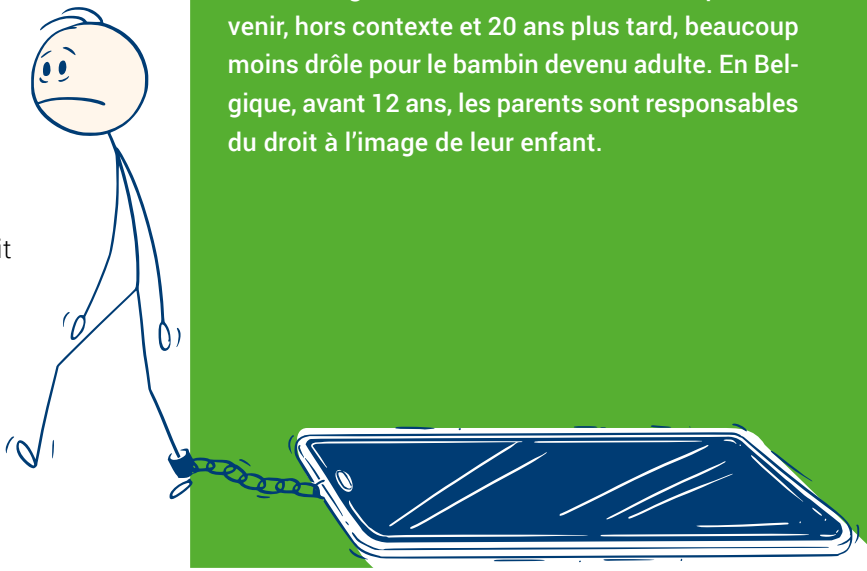
54 % des 19-24 ans s'inquiètent quant à l'accès qu'ont les organisations à leurs données personnelles, malgré le RGPD.

Source : Mike Cooray & Rikke Duus

Rien ne disparaît d'Internet pour toujours

Nos photos font aussi partie de nos données personnelles. L'usage que nous faisons des réseaux sociaux – Snapchat en tête, pour les plus jeunes – laisse souvent penser que les photos qui y sont postées sont éphémères. Erreur : tout ce qui apparaît sur Internet y reste souvent… pour toujours !

Pour illustrer le fait qu'une photo partagée « pour s'amuser » sur un réseau social peut, par effet boule de neige, avoir des conséquences à long terme, prenons l'exemple de Lucas (16 ans) qui s'endort dans un canapé. Un de ses potes le prend en photo : sur le cliché, on aperçoit une canette de bière. Lucas était-il juste fatigué ou éméché ? La photo ne le dit évidemment pas. Dans la soirée, la bande d'amis de Lucas partagent, taguent et commentent la photo qui devient virale. La photo est aussi vue par sa sœur, ses parents et certains de ses professeurs. Mais aussi par son entraîneur et les parents des enfants dont Lucas s'occupe au club d'athlétisme. Endormi, Lucas n'avait évidemment pas donné son consentement pour la prise de la photo et sa diffusion : son droit à l'image (voir ci-contre) n'a pas été respecté. Les jours qui suivent la diffusion de la photo, Lucas doit s'expliquer, devant ses parents notamment. Ce n'est pas tout : cette image où il n'est pas à son avantage pourrait lui coller à la peau plus longtemps encore. Que pensera un éventuel futur employeur lorsqu'il tombera sur cette photo en effectuant, sur Internet, des recherches sur Lucas avant de l'engager ?



SHARENTING

Le fait de partager, en tant que parents, des photos de ses enfants sur les réseaux sociaux porte un nom : c'est le sharenting ! Derrière ce geste, il y a de la fierté surtout, mais aussi une envie de partager ses joies et ses difficultés de parents. Gardons à l'esprit que poster de tels clichés, c'est quelque part en perdre le contrôle, pour toujours. La photo drôle et mignonne d'un bambin de 2 ans… peut devenir, hors contexte et 20 ans plus tard, beaucoup moins drôle pour le bambin devenu adulte. En Belgique, avant 12 ans, les parents sont responsables du droit à l'image de leur enfant.

LE DROIT À L'IMAGE

Personne ne peut être filmé ou pris en photo sans son autorisation. Le droit à l'image stipule qu'il faut le consentement d'une personne pour la prendre en photo : prendre la pause signifie que l'on donne automatiquement son consentement. Pour que cette photo soit diffusée (sur les réseaux sociaux, sur un site internet, dans une publication, etc.), la personne photographiée doit, une nouvelle fois, donner son consentement. En donnant son consentement pour être pris en photo, on ne donne donc pas automatiquement son consentement pour que cette dernière soit rendue publique. Tout le monde dispose de ce droit à l'image, peu importe son âge. Avant 12 ans (soit l'âge du discernement), ce sont les parents (obligatoirement, les deux parents) qui donnent leur consentement pour leur enfant. Entre 12 et 18 ans, le consentement doit être donné par le jeune et par ses parents.

Les jouets et objets connectés

Un objet connecté est un matériel électronique qui peut communiquer avec un ordinateur, une tablette, un smartphone, etc. Cet objet peut, grâce à une liaison sans fil (WIFI ou Bluetooth), envoyer et recevoir des informations. Zoom sur trois objets connectés particulièrement prisés des jeunes et qui récoltent des données personnelles.

Les jouets connectés :

Ils ont la forme de poupées, de robots, d'ours en peluche ou encore de boîtes à histoire, etc. À la différence des jouets classiques, ces jouets électroniques qui interagissent avec les enfants sont connectés, via le WIFI ou le Bluetooth, à votre ordinateur et offrent notamment la possibilité d'enregistrer des messages et de les écouter. Pour cela, ils sont pourvus d'un micro et parfois même d'une caméra et fonctionnent avec une application à télécharger.

Les montres connectées :

Dans sa formule la plus simple, la montre connectée est un mini-ordinateur portable – permettant de recevoir et de passer des appels, voire de se connecter à Internet –, qui peut servir à géolocaliser votre enfant. Certaines de ces montres sont également des « bracelets d'activités », utilisés notamment par les sportifs, qui récoltent des données personnelles relatives à leur santé (pouls, calories brûlées, nombre de pas, heures de sommeil, etc.) et qui peuvent être envoyées, via une application, sur un ordinateur.

Les consoles de jeux :

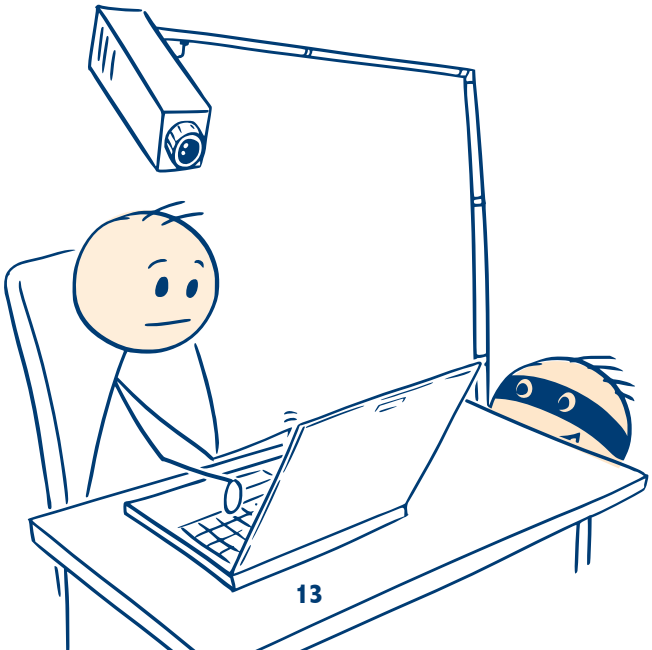
Ces consoles permettent de jouer mais aussi de dialoguer, à distance, avec des joueurs que l'on connaît, dans la vie réelle, ou pas. Les joueurs utilisent généralement un pseudo et un avatar et non leur véritable identité et photo.

Les risques :

- Même si les fabricants sont obligés de sécuriser les infos personnelles collectées, celles-ci risquent d'être utilisées à des fins publicitaires ou d'être mises, frauduleusement, à disposition de tous. Exemple : un assureur ou un employeur pourrait, après avoir eu accès à certaines de vos données personnelles, vous refuser un contrat ou un emploi ;
- Des failles de sécurité peuvent permettre à des hackers d'avoir accès à des informations sensibles (adresse, âge de l'enfant ou du jeune, etc.) et même, d'entrer en contact avec eux, parfois de manière malveillante, notamment via les consoles de jeux, en se cachant derrière un pseudo.

Les conseils :

- Lors de leur mise en marche, ne donnez qu'un minimum d'informations : utilisez un pseudo plutôt que le prénom et le nom de l'enfant (ou un avatar, pour les jeux en ligne);
- Créez une adresse mail servant spécifiquement à ce genre d'usage ;
- Modifiez le code d'accès ou le mot de passe fourni avec l'objet ;
- Faites régulièrement les mises à jour de sécurité ;
- Éteignez l'objet lorsqu'il n'est pas utilisé et effacez les données en ligne lorsque vous cessez de vous en servir.

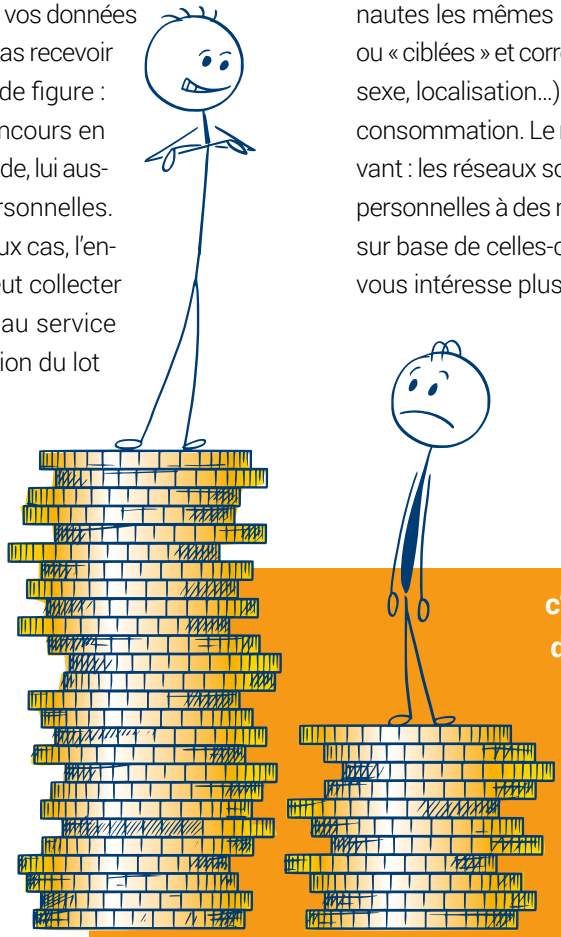


Internet : nos données valent de l'or

Sur Internet, vous renseignez sans cesse des données personnelles vous concernant. Une collecte qui ne se fait pas toujours de manière consciente de votre part.

Évoquons d'abord le cas des sites de vente en ligne qui vous demandent des données personnelles (nom, prénom, adresse postale, adresse mail, etc.), indispensables pour vous faire parvenir l'objet ou encore le billet que vous souhaitez acheter. Dans ce cas, vous n'avez pas d'autres choix que de renseigner correctement vos données personnelles sous peine de ne pas recevoir votre objet ou billet. Autre cas de figure : lors de la participation à un concours en ligne, l'organisateur vous demande, lui aussi, une série d'informations personnelles. Important à savoir : dans les deux cas, l'entreprise ou l'organisateur ne peut collecter que les données nécessaires au service qu'il vous rend ou à la distribution du lot qu'il vous propose de gagner. L'utilisation de vos données personnelles à des fins publicitaires ne peut se faire qu'avec votre consentement et pour une durée maximale de 3 ans après la dernière activation de votre profil.

Lors d'une vente en ligne ou d'un concours, vous donnez vos informations personnelles de manière consciente. Sur Internet, vous laissez, cette fois sans vous en rendre vraiment compte, des données personnelles. La faute aux fameux cookies qui sont des fichiers insérés sur votre ordinateur (ou votre smartphone) par le site web que vous visitez ou l'application que vous utilisez. Grâce à eux, les sites web ne proposent pas à tous les internautes les mêmes publicités : elles sont « personnalisées » ou « ciblées » et correspondent à votre profil d'internaute (âge, sexe, localisation…) mais aussi à vos habitudes de vie et de consommation. Le modèle économique d'Internet est le suivant : les réseaux sociaux et les sites revendent les données personnelles à des marques pour qu'ensuite vous parvienne, sur base de celles-ci, de la publicité ciblée qui vous parle ou vous intéresse plus spécifiquement. C'est la raison pour laquelle tout est fait pour vous forcer à rester le plus longtemps possible sur un réseau social ou sur un site.



17,89 €,

c'est la valeur moyenne des données personnelles dans le monde. Les prix vont de 2,66 € (sexe et nom) à 69,55 € (identifiant et mot de passe).

Source : Ponemon Institute

Depuis 2018 et l'arrivée du RGPD, l'installation des cookies doit se faire avec le consentement de l'internaute : c'est la raison pour laquelle lorsque vous visitez un site pour la première fois (ou passé un délai de 13 mois), une fenêtre apparaît, vous invitant à accepter ou à gérer le fonctionnement de ces cookies. Alors que vous ne pouvez pas refuser les cookies nécessaires au bon fonctionnement du site, vous pouvez refuser les cookies fonctionnels (dont le but est de collecter les données personnelles que vous avez déjà fournies), les cookies de performances (qui améliorent la fonctionnalité d'un site) et les cookies marketing. Ce sont ces derniers qui vous proposent de la publicité « ciblée », sur base de vos habitudes de navigation.

Le business des data brokers

Les data brokers ou courtiers en données sont des sociétés spécialisées dans la collecte et la revente de données personnelles. Elles sont au centre d'un business brassant des milliards d'euros : après avoir acquis des données brutes, les data brokers les croisent avec d'autres fichiers de données afin d'en augmenter la valeur marchande. Le but étant de disposer des listes de profils très ciblés d'internautes – exemple : les jeunes qui entrent à l'université – afin de les vendre à des fins marketing. Le travail des data brokers se fait dans l'ombre.

Monnayer ses données ?

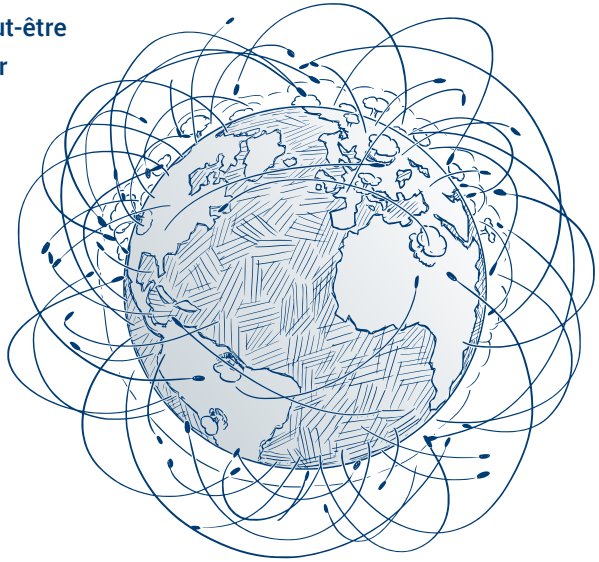
L'application française Tadata permet aux jeunes de 15 à 35 ans de revendre leurs données personnelles ou plutôt le droit d'utilisation de ces dernières. Concrètement, après l'inscription (qui n'est valable qu'avec sa carte d'identité), les jeunes renseignent des données personnelles qui seront revendues à des marques à des fins marketing. Cette initiative fait débat.

Certains estiment que nos données, qui sont des extensions de nous-mêmes, ne devraient pas être l'objet d'un commerce. Tandis que d'autres mettent en avant le fait que nos informations personnelles profitent à tout le monde sauf à nous-mêmes, qui avons généré ces données. Voilà une belle question à débattre avec les jeunes.

En 2018, les agissements de l'entreprise britannique Cambridge Analytica avaient fait scandale : après avoir récupéré les données personnelles de 90 millions de profils Facebook, cette entreprise avait, à la veille des élections américaines, bombardé les électeurs indécis de messages favorables à Trump. Suite à l'arrivée du RGPD, les data brokers doivent, en Europe, obtenir le consentement pour récupérer des données personnelles.

Données personnelles : un univers en évolution perpétuelle

Ce que l'on pense aujourd'hui impossible ou improbable sera peut-être une réalité demain. Avec autant de conséquences nouvelles pour la protection de nos données personnelles.



Notre voix : bientôt une donnée personnelle ?

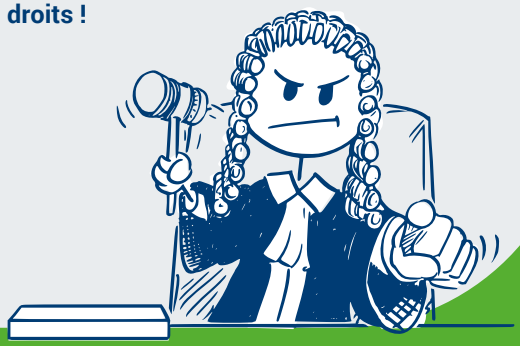
La plateforme de streaming musical Spotify a déposé un brevet qui permet d'affiner votre playlist en fonction de votre humeur : une innovation qui permet de vous proposer des musiques différentes selon que vous soyez, par exemple, triste ou stressé ! Pour que ces choix se fassent de manière fluide, la plateforme de streaming écoute et analyse le timbre de votre voix, mais aussi les bruits et l'ambiance qui vous entourent. Dans le futur, notre voix pourrait donc, elle aussi, faire partie de nos données personnelles.

Au-delà des évolutions technologiques, le débat autour des données personnelles évolue également au gré des événements et des faits d'actualité que nous rencontrons. L'apparition, en Belgique, en octobre 2021, du Covid Safe Ticket (CST) pour lutter contre la pandémie de COVID-19 en est une belle illustration : dès sa mise en place, il a suscité des débats et des questionnements à propos du respect de notre vie privée.

Données personnelles : quels sont mes droits ?

Les entreprises et organisations auxquelles vous avez donné votre consentement pour l'utilisation de vos données personnelles, notamment via l'autorisation des cookies, sur le web, ne peuvent pas faire n'importe quoi de ces dernières. Vous avez des droits !

- **Le droit d'accéder à vos données personnelles :**
  Vous voulez savoir quelles sont les données qu'une entreprise ou une organisation possède sur vous ? Si vous leur posez la question, elles sont dans l'obligation de vous répondre.
- **Le droit de rectifier vos données personnelles :**
  Une entreprise ou une organisation a collecté des données qui ne sont pas ou plus correctes ? Si vous la contactez, elle doit rectifier les données inexactes ou qui ne sont plus à jour.
- **Le droit de transférer vos données personnelles :**
  Vous voulez quitter une application, une plateforme de streaming ou un réseau social pour un autre ? Vous avez le droit de demander que vos données personnelles (photos, messages, etc.) vous suivent et soient transférées vers l'application, la plateforme ou le réseau social que vous utilisez désormais.
- **Le droit de retirer votre consentement :**
  Vous changez d'avis et vous ne désirez plus donner votre consentement pour le partage d'une donnée personnelle ? L'entreprise ou l'organisation concernée doit prendre en compte cette nouvelle situation.
- **Le droit de faire effacer vos données personnelles :**
  Une donnée personnelle n'est plus correcte ou vous dérange, par exemple dans le cas d'une photo qui a été postée lorsque vous aviez moins de 12 ans ? Vous avez le droit de demander que cette donnée soit effacée.



PORTER PLAINTE ?

En Belgique, c'est l'Autorité de protection des données qui veille à ce que le RGPD soit respecté et que vos données personnelles soient collectées par les entreprises et organisations dans le respect de la loi. En cas d'utilisation abusive de vos données, si votre demande auprès de la firme concernée a échoué, une plainte peut être déposée auprès de l'Autorité de protection des données via ce lien : https://www.autoriteprotectiondonnees.be/citoyen/agir/introduire-une-plainte

Données personnelles : comment accompagner les jeunes à la maison ?

Voici quelques conseils pour accompagner, en fonction de son âge, votre jeune dans la gestion et la protection de ses données personnelles.

Avant 12 ans

- Sur le même modèle que la journée type de Sacha (voir page 6), faites, avec lui, le tour de sa journée type. À quel moment utilise-t-il un outil numérique ? À quel moment laisse-t-il derrière lui des données personnelles ?

- Sensibilisez votre enfant à l'importance des pseudonymes lors de l'utilisation des objets numériques, jouets connectés ou jeux en ligne. Amusez-vous à trouver ensemble un pseudo. Discutez des situations où il convient d'utiliser un pseudo et des situations où il est nécessaire de donner sa véritable identité.

- Vous avez l'habitude de poster des photos de vos enfants sur les réseaux sociaux ? Discutez-en avec eux : qu'en pensent-ils ? Quelles peuvent être les conséquences aujourd'hui et plus tard ?

Après 12 ans

- Sur le même modèle que la journée type de Sacha (voir page 6), faites le tour d'une journée type de votre jeune. À quel moment utilise-t-il un outil numérique ? À quel moment laisse-t-il derrière lui des données personnelles ?

- En tapant le prénom et le nom de votre jeune (ou le vôtre) dans un moteur de recherche, vérifiez quelles sont les informations qui apparaissent. Qu'en pensez-vous ? Incitez votre jeune à effectuer régulièrement cette recherche.

- Aidez votre jeune à choisir un mot de passe qui soit suffisamment sécurisé (avec des lettres, des chiffres et des caractères spéciaux). Retrouvez des conseils et un test pour vérifier le degré de sécurité d'un mot de passe via le site : http://bonmotdepasse.be.

- Créez avec votre jeune plusieurs adresses mails, pour chaque type d'activité : une pour les amis et les proches ; une pour les réseaux sociaux ; une pour les jeux ; une pour les démarches administratives, etc

- Faites régulièrement les mises à jour de sécurité des écrans et appareils connectés de la maison et incitez votre jeune à faire de même avec son smartphone et ses propres objets connectés.

- Si votre jeune est amené à faire des achats en ligne et à communiquer ses coordonnées bancaires, informez-le de l'importance de le faire uniquement sur des sites sécurisés : l'adresse du site doit commencer par https (un petit cadenas apparaît avant l'url).

Comment accompagner les jeunes à l'école et dans les structures d'éducation et d'animation ?

Conseils aux professionnels de l'éducation

Avant 12 ans

- Lancez la discussion sur la protection des données à partir de la séquence animée **C'est quoi, la protection des données personnelles ?** à découvrir via le site www.1jour1actu.com. Dans la foulée, voyez ensemble à quels moments, à leur âge, ils laissent derrière eux des données personnelles.
- Discutez de la place des écrans et du numérique dans leur quotidien. Comment était-ce avant ? Demandez-leur d'imaginer à quoi ressembleront les outils numériques et les réseaux sociaux dans 10 ans.

Après 12 ans

- Lancez la discussion sur la protection des données à partir de la séquence animée **La nouvelle loi vie privée de A à Z** à découvrir via le site www.jedecide.be. Incitez les élèves à consulter ce site, fait pour eux, pour apprendre à protéger leur vie privée.
- Discutez de la place des réseaux sociaux dans leur vie quotidienne. Pourraient-ils s'en passer ? Comment était-ce avant ? Demandez-leur d'imaginer le réseau social de leur rêve.
- Lancez le débat autour de l'ampleur que peut prendre un selfie partagé sur les réseaux sociaux en visionnant la série documentaire d'Arte **L'effet domino**. À découvrir via ce lien : https://www.arte.tv/fr/videos/087579-001-A/l-effet-domino.
- Installez, sur un ordinateur de l'école, le logiciel **Cookieviz**, développé en France par la CNIL (Commission Nationale de l'Informatique et des Libertés) : cet outil de visualisation permet d'analyser, en temps réel, l'impact des cookies lors de votre navigation. À télécharger via : https://linc.cnil.fr.
- Proposez-leur de jouer à **Datak**, un « serious game » sur la protection des données personnelles, développé par la Radio Télévision Suisse. À découvrir via www.datak.ch.

Tous les âges

- Consultez le site jedecide.be et ses nombreux supports pédagogiques pour vous aider à mener des discussions et des débats en classe.
- Faites appel à des associations spécialisées ou à des centres de ressources en éducation aux médias pour réaliser des ateliers en classe.

Le dico des données personnelles

Algorithmes : instructions et opérations réalisées avec des données et dans un ordre précis afin de produire un résultat ou de résoudre un problème.

Big Data : volume gigantesque de données (textes, photos, vidéos, etc.) diffusées, partagées et stockées sur Internet.

Bulle de filtre : système qui permet, grâce aux algorithmes, de vous proposer des informations qui correspondent à vos intérêts et vos opinions tout en occultant toutes les autres informations.

Cookies : petits fichiers stockés sur votre ordinateur ou votre smartphone et qui peuvent notamment mémoriser certaines de vos données ou tracer les sites consultés.

Consentement : dans le cadre du RGPD, il s'agit d'accepter de manière explicite, que nos données à caractère personnel fassent l'objet d'un traitement.

Data broker : société spécialisée dans la collecte, l'agrégation et la revente de données personnelles.

Données personnelles : toute information permettant d'identifier directement ou indirectement une personne physique.

Droit à l'image : droit de toute personne physique à disposer de son image et à s'opposer à la diffusion de sa photo sans son consentement.

Géolocalisation : technique permettant, le plus souvent à l'aide d'un GPS, de localiser avec précision une personne ou un objet.

Hacker : personne qui s'introduit de manière frauduleuse dans un réseau ou un système informatique.

Métadonnées : données qui délivrent des informations ou décrivent d'autres données.

Publicité ciblée (ou personnalisée) : technique qui identifie les internautes et leur propose des publicités qui leur sont spécialement destinées en fonction de leur profil et de leur comportement sur Internet.

Réseau social : site ou application qui permet de se regrouper, de dialoguer et d'échanger des informations.

Retargeting (ou reciblage) : technique qui permet, sur base des informations collectées sur l'internaute, de lui proposer des publicités pour un produit ou un service pour lequel il a marqué un intérêt.

Reconnaissance faciale : technique qui permet d'authentifier une personne à partir des traits de son visage.

RGPD : Règlement Général sur la Protection des Données qui encadre le traitement des données personnelles dans l'Union européenne.

Sharenting : le fait de partager, en tant que parents, des photos de ses enfants sur les réseaux sociaux.

Vie privée : renvoie à la sphère intime, à ce que nous voulons garder pour nous.

Vie publique : par opposition à la vie privée, elle rassemble tout ce que nous décidons de partager avec le plus grand nombre.


SCANNING
SEARCH
COMPLET
ANALYSIS

Les dossiers de la collection « Repères » ont pour objectifs d'informer et d'outiller, de façon succincte et concrète, les parents et les professionnels de l'éducation.

Ce carnet a été élaboré dans le cadre du GT usages médiatiques.
Rédaction: Anouck Thibaut

Parmi les thèmes traités :

- le cyberharcèlement
- la liberté d'expression
- la désinformation
- les jeux vidéo
- La protection de ses données personnelles
- l'identité numérique
- le flux d'informations
- le big data
- les influenceurs
- Réseaux sociaux et démocratie

Juin 2022 – Les ressources proposées dans cet ouvrage sont correctes à la date de parution

Retrouvez tous nos dossiers sur
http://www.csem.be/collectionreperes

conseil supérieur de l'éducation aux médias
CSEM

Une initiative du Conseil supérieur de l'éducation aux médias

CSEM
Boulevard Léopold II, 44-6E630
1080 Bruxelles
www.csem.be – csem@cfwb.be

FÉDÉRATION WALLONIE-BRUXELLES

Éditeur responsable: Paul de Theux - CSEM - Boulevard Léopold II, 44 - 6E630 - 1080 Bruxelles - Design: www.acg-bxl.be