INTERNET ET MOI

PROTECTION, LIMITES, OPPORTUNITÉS.

Fondation Roi Baudouin
Agir ensemble pour une société meilleure

NOTAIRE.BE

INTERNET ET MOI

PROTECTION, LIMITES, OPPORTUNITÉS.

Fondation Roi Baudouin

Agir ensemble pour une société meilleure

NOTAIRE.BE

AVANT-PROPOS

Les nouvelles technologies de communication et d'information ont considérablement facilité notre quotidien. Quelques clics suffisent désormais pour payer des factures ou réserver des vacances. Aujourd'hui, Il y a peu de risque de se perdre en chemin, où que nous soyons. Et nous pouvons rester en contact permanent avec les gens que nous aimons.

Mais la facilité avec laquelle nous surfons sur le Web présente également un revers. A travers tous les actes que nous faisons en ligne, nous partageons des données personnelles, parfois même sans y penser. Des données qui valent leur pesant d'or pour les réseaux publicitaires et les entreprises ; pour les 'escrocs' aussi, qui n'apprécient que trop ces nouveaux canaux pour contourner ou enfreindre la loi.

Tout cela ne doit cependant pas être une raison pour se méfier de ce nouveau monde ou pour lui tourner le dos. Les utilisateurs ont beaucoup plus de possibilités de se protéger en ligne qu'ils ne le pensent. Avec ce guide pratique, le but de la Fondation Roi Baudouin et de la Fédération du Notariat est de fournir une information de première ligne pour apprendre à utiliser intelligemment les nouvelles technologies numériques.

Comment veiller en ligne au respect de sa vie privée ? Comment faire ses achats en toute sécurité ? Comment protéger son enfant contre le cyber-harcèlement ? Peut-on critiquer son employeur sur Facebook ? Que faire si on est victime d'hameçonnage, que quelqu'un tente d'extorquer nos données personnelles? Peut-on transmettre sa collection de musique localisée dans un cloud à ses héritiers ? Le présent guide répond à ces questions, et à bien d'autres.

1. VIE PRIVÉE & CYBERSÉCURITÉ

Données personnelles et traces en ligne

Dans tout ce que nous faisons en ligne, nous partageons des **données personnelles** telles que notre nom, des photos, des numéros de téléphone et de comptes en banque, des adresses e-mails, un réseau,… Il n'est pas toujours évident de savoir qui détient nos données et si quelqu'un en fait éventuellement un usage détourné.

Outre les données partagées consciemment, par exemple lorsque nous complétons un formulaire sur Internet, il y a les **traces** que nous laissons en ligne (souvent de manière inconsciente), comme les fichiers journaux, les cookies ou les applis.

FICHIERS JOURNAUX

Tout ce que nous faisons en ligne est conservé dans des fichiers journaux *(logfiles)*. Ces fichiers consignent, notamment avec quel fournisseur d'accès nous surfons, les fichiers sur lesquels nous cliquons. Ils enregistrent les moments auxquels nous surfons et la durée de nos visites virtuelles. Ils ne conservent pas nos données personnelles mais bien celles de notre ordinateur, et celles-ci sont ensuite utilisées par les gestionnaires des sites Web pour améliorer la navigation.

COOKIES

Les sites Web utilisent des cookies, des petits 'fichiers texte' qui s'installent sur le disque dur de notre ordinateur, smartphone ou tablette lorsque nous visitons un site Web. Certains sont utiles et permettent de nous identifier rapidement lors d'une prochaine visite au même site, sans devoir à nouveau redémarrer toute une procédure de connection ou indiquer nos préférences, comme celle de langue par exemple.

Les sociétés d'e-marketing, les boutiques en ligne et les réseaux sociaux utilisent également des cookies. Ils analysent les sites que nous visitons, les produits pour lesquels nous montrons de l'intérêt et relient ces informations à nos données personnelles (par exemple celles complétées en ligne). Ils peuvent ainsi nous adresser des publicités plus ciblées, ou transmettre ces données à d'autres entreprises.

APPLIS

Vous voulez apprendre une langue rapidement ? Il existe des dizaines d'applis qui affirment pouvoir le faire. Mieux dormir ? Une 'appli du sommeil' vous guide pour rejoindre les bras de Morphée. Vous voulez perdre du poids, méditer, planifier votre journée ? Il existe de nombreuses applis qui vous proposent de faciliter votre vie quotidienne, mais qui fournissent lors de chaque utilisation des informations utiles aux annonceurs. Chaque fois que vous regardez une vidéo sur YouTube par exemple, cette catégorie est ajoutée dans votre compte Google à la liste des sujets que vous trouvez intéressants.
Plus nous laissons de traces derrière nous, plus nous intéressons les annonceurs.

PLATEFORMES DES MÉDIAS SOCIAUX

Vous avez certainement déjà vécu cela : vous avez regardé des chaussures sur le site Web d'un vendeur et voilà que cette paire vous poursuit en ligne. Les entreprises de médias sociaux comme Facebook utilisent votre comportement de recherche ou de surf pour aider les annonceurs à vous proposer des publicités ciblées.

Comment se protéger ?

Rien de ce que l'on fait en ligne n'est donc véritablement privé ? Est-il illusoire de croire au respect de la vie privée ? Et bien non. La législation sur le respect de la vie privée impose en effet des restrictions aux entreprises et organisations qui veulent collecter et utiliser les données vous concernant. Vous pouvez aussi prendre vous-même des mesures de précaution pour protéger vos données et vos appareils, et effacer vos traces en ligne.

PROTÉGER SA VIE PRIVÉE

Attention, chien de garde
La loi européenne sur la protection de la vie privée est entrée en vigueur le 25 mai 2018, sous le nom de **Règlement Général sur la Protection des Données**, ou **RGPD** (*General Data Protection Regulation*, ou GDPR). Cette réglementation de la vie privée protège vos données encore mieux que ne le faisait la législation belge en la matière.

Le RGPD définit les règles que doivent suivre les entreprises, les organisations et les autorités quand elles collectent, transmettent, adaptent, relient ou copient des données personnelles, ainsi que les droits dont vous jouissez pour protéger vos données.

Les entreprises, organisations et autorités qui veulent utiliser vos données personnelles ont des **obligations** :

- Elles doivent disposer d'un motif de traitement légitime pour traiter vos données ;
- elles doivent clairement indiquer dans leur **politique de respect de la vie privée** pourquoi elles collectent vos données personnelles, ce qu'elles comptent en faire, qui peut les consulter et combien de temps elles conservent ces données ;
- elles peuvent utiliser les données uniquement dans le but annoncé et **ne peuvent pas collecter ni conserver plus de données que nécessaire ;**
- elles doivent systématiquement préciser où vous pouvez adresser vos **questions ou réclamations**.

Si une appli ou un site Web propose plusieurs options de confidentialité, c'est l'option la plus respectueuse de la vie privée qui doit être activée de façon standard *(privacy by default)*.

De quels droits jouissez-vous pour protéger vos données personnelles ?

DROIT À L'INFORMATION : vous avez le droit de savoir qui utilise vos données.

DROIT DE POSER DES QUESTIONS : vous pouvez toujours demander si une organisation ou une entreprise conserve des données vous concernant.

DROIT À L'ACCÈS DIRECT : vous pouvez obtenir une copie de toutes les données et demander où le sous-traitant a obtenu ces données. L'Autorité de protection des données (APD) propose des lettres types pour ce genre de demandes.

DROIT À L'ACCÈS INDIRECT : les données médicales peuvent être demandées par un intermédiaire comme votre médecin traitant ; les données relatives à la sécurité ou visant à prévenir ou punir un acte illégal peuvent être consultées via l'Organe de contrôle de l'information policière (COC).

DROIT À LA RECTIFICATION : vous pouvez faire corriger des données incorrectes ; vous pouvez faire effacer des données incomplètes, non pertinentes ou interdites.

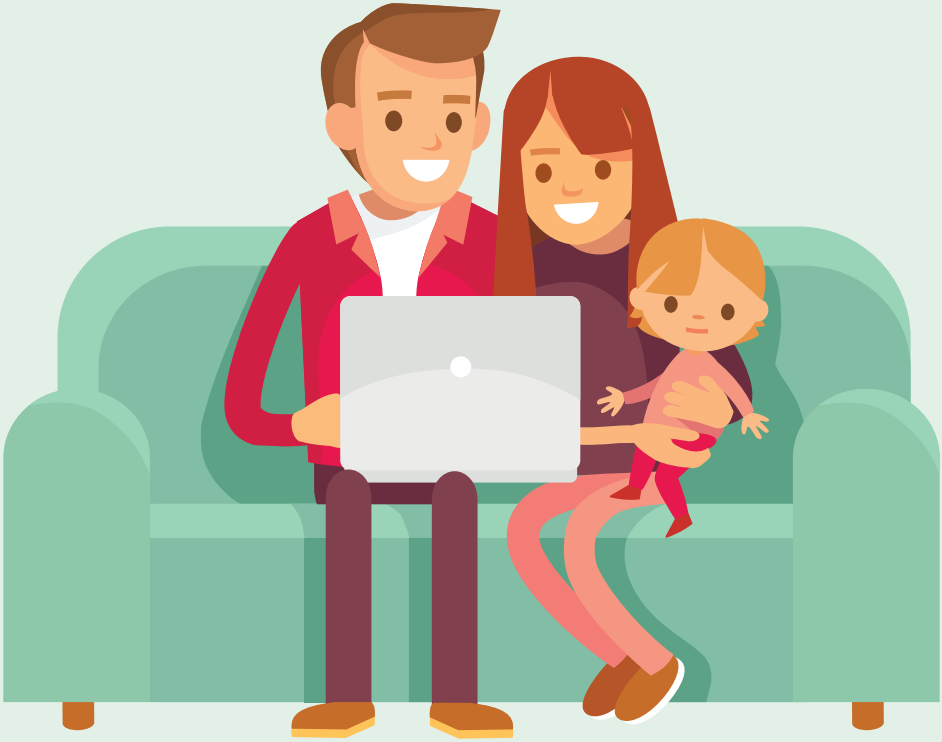
DROIT À L'OPPOSITION : vous pouvez vous opposer au traitement de vos données, sauf si les données sont nécessaires à la conclusion ou à l'exécution d'un contrat, ou quand leur traitement est imposé par la loi.

DROIT DE NE PAS ÊTRE SOUMIS À UNE DÉCISION AUTOMATISÉE : les entreprises ou les organisations peuvent analyser vos données pour établir un profil ; elles ne peuvent pas utiliser ce profil pour prendre des décisions importantes qui peuvent vous nuire comme, par exemple, l'augmentation des primes d'assurance.

Pour toute information sur le respect de la vie privée : **www.jedecide.be** ou **www.autoriteprotectiondonnees.be**. Ces sites Web proposent des dossiers thématiques, des informations de fond et des conseils. Vous y trouverez également toutes sortes de recommandations.

CONSERVER LES COOKIES UTILES, REJETER LES COOKIES PUBLICITAIRES

Vous ne souhaitez pas que des entreprises ou d'autres organisations suivent votre comportement de surf ? Vous pouvez paramétrer votre navigateur (Internet Explorer, Chrome, Firefox, Edge, Safari) de telle sorte qu'il **refuse ou efface les cookies (de façon sélective)**. Vous pouvez modifier ces réglages à tout moment.



CHECK-LIST
Gestion des cookies

- Effacer manuellement : cela peut se faire dans chaque navigateur via les 'paramètres' (effacer les données de navigation).
- Effacer après utilisation : vous pouvez faire effacer les cookies par le navigateur une fois la session fermée.
- Refuser tous les cookies : possible, mais pas recommandé si vous voulez surfer avec fluidité.
- Refuser les cookies tiers (publicité, médias sociaux).
- Adapter le paramétrage des cookies : c'est possible pour chaque site Web que vous visitez.
- Bloqueurs de pubs *(adblockers)* : ils bloquent les publicités et donc les cookies de réseaux publicitaires. N'oubliez cependant pas que les sociétés de médias, par exemple, sont dépendantes des revenus publicitaires.

GOOGLE : DÉBRANCHER L'ŒIL QUI VOIT TOUT

Google sait quelles applis vous utilisez et quand vous les utilisez, quelles recherches vous avez effectuées, quelles vidéos vous avez regardées, quels e-mails vous avez envoyés. Vous pouvez demander un téléchargement de toutes les données que Google a collectées sur vous à partir de toutes les applis Google possibles (y compris des données que vous avez explicitement effacées).

Via les 'paramètres publicitaires', vous pouvez voir les données que Google possède sur vous et **limiter cette information ou la rendre non disponible**. Si vous ne souhaitez pas que Google vous suive partout en temps réel via l'appli Google Maps, vous pouvez désactiver la fonction 'Partage de position'.

Il existe également des moteurs de recherche qui ne retiennent pas les comportements antérieurs. Revers de la médaille, les informations obtenues sont souvent moins précises.

APPLIS : SACHEZ CE QUE VOUS ACHETEZ

Les applis veulent en 'savoir' le plus possible sur vous. Elles demandent l'accès à vos contacts, vos photos, votre caméra ou micro, votre position. Et vous avez vite fait de cliquer sur 'OK' quand l'appli vous demande une autorisation. Parfois c'est sans conséquence, mais beaucoup d'applis ratissent plus de données personnelles qu'elles n'en ont besoin, pour les transmettre ensuite à d'autres entreprises.

C'est pour cela qu'il est toujours préférable de bien lire les conditions d'utilisation, pour savoir quelles données sont collectées par l'appli, pourquoi cette appli en a besoin et à qui elle transmet les données. Si vous estimez que c'est exagéré ou trop vague, vous pouvez décider de ne pas installer l'appli, ou contacter le développeur et lui demander pourquoi il a besoin de ces informations.

Les applis doivent indiquer clairement ce qu'elles font avec vos données. Elles doivent demander un consentement explicite et actif, et donc pas par une simple case à cocher au préalable. Elles doivent demander ce consentement de façon progressive : par exemple ne demander l'accès à la caméra que lorsque l'appli a besoin de la caméra, et pas directement lors du téléchargement.

CARTOGRAPHIE MOBILE

Google Street View permet de voir en ligne toutes les rues de Belgique. Quand on filme la voie publique, on filme inévitablement des maisons, des véhicules, des terrains et des personnes. Pour se conformer à la loi sur la protection de la vie privée, Google doit rendre les visages ou les plaques minéralogiques non identifiables. Si vous considérez que c'est insuffisant, vous pouvez demander de renforcer ce **'floutage'** ou rendre également le véhicule ou la maison non identifiables. Il suffit pour cela de cliquer sur 'Signaler un problème' chez Google. Si cela ne fonctionne pas, vous pouvez toujours faire intervenir l'Autorité de protection des données (APD).

CHECK-LIST APPLIS

- Lisez les conditions d'utilisation, la politique de confidentialité et les autorisations, afin de savoir quelles sont les informations collectées par l'appli, ce que cette appli en fait et qui a accès à ces données.
- Adaptez les paramètres de façon à limiter ou refuser l'accès aux données personnelles.
- Connectez-vous avec un mot de passe plutôt que via Facebook.
- Fiez-vous à votre bon sens : si vous estimez que l'appli vous demande trop d'informations, ne l'installez pas ou prenez contact avec le développeur.

PLATEFORMES DES MÉDIAS SOCIAUX : LIMITER LES PUBLICITÉS

Il est quasi impossible d'échapper aux publicités sur les médias sociaux. Vous pouvez néanmoins faire en sorte que ces publicités ne soient pas basées sur votre comportement en ligne si vous ne le souhaitez pas (voir ci-dessous). Vous avez aussi à tout moment le droit de vous opposer sans frais à l'utilisation de vos données à des fins de marketing direct.

CHECK-LIST MARKETING DIRECT

- Utilisez les *likes* avec prudence. Vous éviterez de la sorte que les réseaux publicitaires n'en apprennent trop sur vos préférences.
- Revérifiez les informations que vous avez données pour votre profil. Est-il vraiment nécessaire que le réseau social sache tout cela ?
- Téléchargez votre archive Facebook via les 'Paramètres généraux du compte'. Vous aurez ainsi une vue sur les thèmes publicitaires liés à votre profil et sur les annonceurs qui possèdent (officiellement) des informations à votre sujet.
- Adaptez les paramètres relatifs à la confidentialité et aux publicités pour l'ordinateur ou le smartphone.
- Désactivez les fonctions de localisation (avec lesquels les médias sociaux, via les données GPS savent où vous êtes).
- Associez éventuellement les cartes de fidélité à une adresse e-mail que vous n'utilisez pas. Les exploitants des données associent souvent les données des cartes de fidélité aux données en ligne des réseaux sociaux.

Les sites des réseaux sociaux ne sont jamais vraiment 'privés'. Vous n'avez en effet aucun contrôle sur les paramètres de confidentialité de vos contacts ni sur leur comportement en ligne. **Un partage est par définition public**, mais vous pouvez limiter les risques. Les sites des réseaux sociaux vous donnent la possibilité d'affiner vos paramètres de confidentialité. Vous pouvez ainsi choisir qui peut visualiser vos posts, vos photos ou vos vidéos : uniquement vous, vos 'amis', les contacts de vos amis, ou tout le monde.

Si vous n'y faites pas attention, vos données sont exposées à tous. Le fisc lui-même pourrait par exemple contrôler sur votre profil de médias sociaux si vous utilisez pour partir en vacances en Italie un véhicule que vous déclarez à 100% dans votre société. Les renseignements obtenus via des réseaux sociaux ne constituent certes pas une preuve en soi, mais peuvent servir à justifier une enquête plus approfondie.

Pour toute question ou réclamation :

- l'Autorité de protection des données (APD) en ce qui concerne le traitement des données personnelles à des fins de marketing direct : **www.autoriteprotectiondonnees.be.**
- le Point de contact du SPF Économie (Direction générale Contrôle et Médiation) si aucun consentement n'a été demandé pour de la publicité par e-mail : **https://pointdecontact.belgique.be.**

Qu'est-ce que l'Autorité de protection des données peut faire pour vous ?

UNE QUESTION ?

Vous pouvez alors recourir à leur service d'aide de première ligne, accessible par téléphone ou par e-mail. Vous trouverez sur le site Web de plus amples informations sur l'accessibilité de ce service.

UNE RÉCLAMATION ?

Vous pouvez envoyer un courrier explicatif daté et signé, avec suffisamment d'informations à propos du problème que vous rencontrez. L'APD agit en tant que médiatrice entre les parties. Elle possède un pouvoir d'investigation, peut effectuer des contrôles et imposer des sanctions. L'intervention de l'APD est gratuite.
www.autoriteprotectiondonnees.be

LE DROIT À L'OUBLI : FAIRE EFFACER DES DONNÉES GÊNANTES VOUS CONCERNANT

Imaginez que vous ayez commis une erreur de jeunesse qui a fait la une des médias. Depuis, vous avez mis de l'ordre dans votre vie, mais en effectuant une recherche Google sur votre nom, le moteur de recherche vous rappelle ce passé. À vous, mais potentiellement aussi à votre employeur, à vos contacts professionnels, ou à votre nouvelle compagne.

Vous avez le droit de demander l'effacement de vos données. Ce sont les entreprises qui doivent expliquer pourquoi elles ne voudraient ou ne pourraient pas le faire. Ce droit ne se limite pas aux moteurs de recherche ou aux archives en ligne. Il s'applique à n'importe quel enregistrement numérique de vos données par n'importe quel prestataire de services.

Ce 'droit à l'oubli' n'est pas absolu. Vous ne pouvez par exemple pas faire effacer un diagnostic noté par un médecin dans votre dossier en ligne. Il y a en outre le droit à une information correcte pour les autres utilisateurs.

CHECK-LIST
EFFACEMENT DES RÉSULTATS DE RECHERCHE

- Prenez contact avec le Webmaster de la page qui contient l'information. Si vous ne le faites pas, l'information pourrait disparaître des résultats du moteur de recherche mais le lien continuerait d'exister.
- Si cela ne fonctionne pas, allez sur la page 'Supprimer du contenu' du moteur de recherche et suivez les étapes indiquées. Vous devrez notamment fournir la preuve de votre identité et expliquer pour chaque lien ou url la raison pour laquelle vous voulez le supprimer.
- Vous pouvez aussi, simultanément ou si le moteur de recherche n'accède pas à votre demande, adresser un envoi recommandé contenant la même demande.
- Si aucune suite n'est donnée à votre demande, vous pouvez introduire une réclamation auprès de l'Autorité de protection des données ou du tribunal civil.

CYBERSÉCURITÉ

Vous pouvez sécuriser vos appareils, et donc vos données, contre les hackers en prenant quelques précautions.

MALWARE : LUTTER CONTRE LES SALES PETITES BÊTES

Le mot 'malware' est le nom générique pour désigner les logiciels indésirables ou malveillants tels que les virus, les logiciels espions (spyware) ou les logiciels rançonneurs (ransomware). Vous pouvez par exemple vous faire infecter par un malware quand vous installez un logiciel gratuit. Sans que vous vous en rendiez compte, ce genre de logiciel malveillant peut vous diriger vers un site frauduleux, par exemple un site imitant celui de votre banque, ou faire apparaître de faux pop-ups lors de vos achats sur Internet.

Un **spyware** est un logiciel qui espionne votre comportement de surf et collecte des données à votre insu. Ce genre de logiciel est utilisé par des annonceurs publicitaires ou par des hackers.

Dans le cas d'un **ransomware**, un virus prend votre appareil et/ou vos fichiers en otage. Les responsables exigent ensuite une rançon pour les libérer. Il ne faut pas accéder à leur demande car vous n'avez aucune certitude que vos fichiers vont effectivement être débloqués. Face à un tel virus, vous devez désactiver immédiatement le WiFi, faire 'nettoyer' votre appareil et réinstaller vos programmes. Si vous effectuez des back-ups réguliers, vous pourrez également (faire) réinstaller vos données. Vous pouvez également surfer avec un autre appareil sur le site **www.nomoreramsom.org**, issu de la collaboration entre agences de police et sociétés spécialisées en sécurité informatique. Celui-ci vous permettra éventuellement de trouver la clé pour déverrouiller vos fichiers.

Vous trouverez de plus amples informations dans la brochure Ransomware de la Cert.be, que vous pouvez télécharger via **https://www.cert.be/fr.html** ou **https://www.safeonweb.be/fr**.

CHECK-LIST
PROTECTION DES SMARTPHONES ET DES LAPTOPS

- Effectuez régulièrement des mises à jour de vos logiciels et de votre sécurité.
- Effectuez des back-ups.
- Apprenez à identifier les e-mails frauduleux.
- Utilisez une bonne protection antivirus.
- Utilisez des mots de passe forts.

www.safeonweb.be/fr/surfez-en-toute-securite

QUE FAIRE SI QUELQU'UN SE FAIT PASSER EN LIGNE POUR VOUS ?

La plupart des platesformes de médias sociaux ont un bouton pour signaler quand quelqu'un s'y fait passer pour vous. Si vous ne possédez pas de compte sur la plateforme en question, vous pouvez compléter un formulaire dans le *Help Centre* de cette plateforme. Si la personne a commis des méfaits sous votre nom, vous pouvez porter plainte à la police pour usurpation d'identité.

VOTRE WEBCAM PEUT-ELLE ÊTRE HACKÉE ?

Bien sûr. Si votre webcam a été hackée, d'autres personnes peuvent observer ce qui se passe via votre webcam sans que vous ne l'ayez activée. Vous pouvez limiter les risques avec un bon antivirus et un mot de passe (fort) pour votre webcam. Il existe aussi dans le commerce des caches *(webcam-cover)* à apposer sur la webcam de votre laptop.

Adressez-vous au Point de contact du SPF Économie (Direction générale Contrôle et Médiation) en cas d'hameçonnage *(voir p. 32-34)*, de spam (courrier électronique indésirable) ou de ransomware : **https://pointdecontact.belgique.be.**

2. ARGENT

ACHETER

Acheter en ligne fait désormais partie intégrante de notre vie. Vous pouvez vous offrir un pull-over ou un livre sans bouger de chez vous ou même signer numériquement un contrat d'achat que vous auriez par le passé dû envoyer par courrier recommandé en trois exemplaires. Difficile de faire plus facile. Quelques mesures de précaution s'imposent néanmoins si vous ne voulez pas vous faire flouer.

COMMENT SAVOIR SI UN WEBSHOP EST FIABLE ?

Les webshops fiables indiquent toujours l'identité explicite du vendeur, un prix clair pour les produits proposés, des informations sur l'endroit où on peut renvoyer les articles et qui contacter en cas de problème. Pour les webshops belges, vérifiez la présence du label BeCommerce.

BECOMMERCE : MÉDIATEUR POUR LES CONFLITS AVEC DES BOUTIQUES EN LIGNE

BeCommerce est une association belge d'entreprises soucieuses de garantir la qualité de l'e-commerce. Ses membres respectent les règles belges et européennes en matière de sécurité, de respect de la vie privée et de commerce équitable. Ils se conforment en outre aux règles de comportement du label de qualité BeCommerce. Les boutiques en ligne qui portent ce label sont certifiées par un bureau d'audit indépendant. Les consommateurs qui ont des problèmes avec une boutique en ligne et qui ne trouvent pas écho auprès de la boutique en question, peuvent faire intervenir la Commission des Litiges de BeCommerce. BeCommerce propose sa médiation pour les plaintes concernant tant ses membres que des non-membres actifs sur le marché belge.

Le site Web de BeCommerce **(www.becommerce.be/fr)** propose un formulaire de signalement de plainte.

Vérifiez si vous pouvez régler vos achats via une zone de paiement sécurisée, que vous reconnaîtrez à une adresse (url) commençant par 'https://' ou au petit cadenas précédant l'url. Votre paiement sera alors codé par les serveurs d'une entreprise de sécurisation spécialisée et traité en toute sécurité. Vous pouvez vérifier la fiabilité des services de paiement via BeCommerce (voir encadré).

Les sites Web fiables renvoient directement un accusé de réception reprenant l'aperçu de la commande et des données de paiement.

CHECK-LIST
ACHETER EN LIGNE EN TOUTE SÉCURITÉ

- Ne faites jamais d'achats en surfant via un réseau WiFi public (non sécurisé).
- Si vous voulez acheter en ligne, optez pour des sites Web connus. Si vous ne les connaissez pas, faites une recherche préalable.
- Contrôlez l'url du webshop.
- Vérifiez si vous pouvez régler vos achats via une zone de paiement sécurisée.
- Si vous ne recevez pas d'accusé de paiement, n'hésitez pas à prendre contact avec le gestionnaire du site Web.
- Contrôlez régulièrement vos extraits de compte.

QUE FAIRE SI UN ACHAT EN LIGNE SE PASSE MAL ?

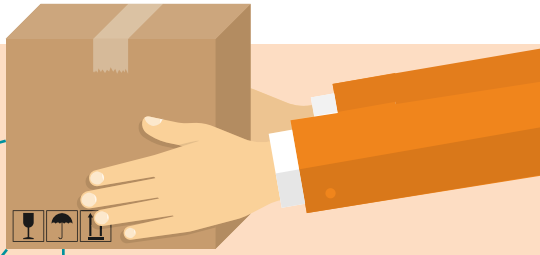
Malgré toutes les mesures de précaution, un achat en ligne peut toujours mal se passer : montant débité de votre carte de crédit plus élevé que prévu, colis non livré ou faillite du vendeur.

Commencez toujours par contacter le webshop et conservez tous les e-mails échangés en guise de preuve. La responsabilité du vendeur est engagée jusqu'à ce que la commande soit dans vos mains. Si le vendeur ne réagit pas, vous pouvez déposer plainte auprès du service de médiation de la Poste **(www.omps.be)** qui agira en tant que médiateur. Si cela non plus ne fonctionne pas ou si vous êtes victime d'une escroquerie, vous pouvez vous adresser au SPF Économie, via son point de contact. Vous pouvez également introduire une plainte à test-achats.be ou au CEC, plateforme européenne pour les droits des consommateurs **(https://www.cecbelgique.be)**.

Les sociétés de cartes de crédit proposent une assurance contre les fraudes par Internet et les commandes non livrées ainsi que pour les livraisons endommagées ou ne correspondant pas à ce qui avait été commandé. Si vous pouvez prouver que vous avez essayé de récupérer le montant en question et qu'il n'est pas question de malveillance de votre part, le montant vous sera remboursé. Vous devez néanmoins effectuer la déclaration dans les trois mois qui suivent la commande.

Si vous suspectez une fraude avec votre carte de crédit, prenez contact avec votre banque pour faire bloquer votre carte ainsi que votre application de banque en ligne. N'enregistrez jamais les données de votre carte de crédit sur votre ordinateur ou votre laptop, pour éviter que les hackers ne puissent les trouver.

QUE FAIRE SI VOTRE COLIS A ÉTÉ PERDU?



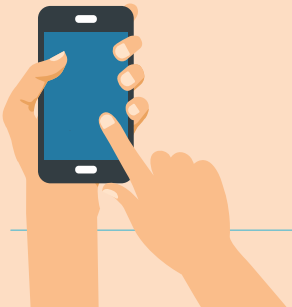
1.
Prenez contact avec le département clientèle du service de livraison.

3.
Déposez plainte auprès du service de médiation de la Poste.

2.
Prenez contact avec le vendeur.

Pour les envois nationaux : plainte auprès du Point de contact du SPF Économie **https://pointdecontact.belgique.be.**

Pour les envois internationaux : plainte auprès du Centre européen du Consommateur (CEC) **www.cecbelgique.be.**



QU'EN EST-IL POUR DES ACHATS EFFECTUÉS EN DEHORS DE L'UE ?

Lorsque l'on commande des articles dans des webshops situés aux États-Unis ou dans d'autres pays en dehors de l'Union européenne, il peut y avoir de mauvaises surprises à la livraison du colis. Vous pouvez en effet avoir à payer des suppléments comme des droits d'importation, de la TVA et des accises. Soyez particulièrement vigilent.

A l'arrivée du colis, en cas de mauvaise surprise, il vous reste deux options : payer le supplément ou refuser le colis, auquel cas il n'est pas toujours facile de se faire rembourser.

Vous trouverez une liste des tarifs pour les droits d'importation sur le site Web de bPost : **www.bpost.be**.

POUVEZ-VOUS CONFIRMER PAR E-MAIL L'ACHAT D'UNE MAISON ?

Dans le secteur de l'immobilier, il est devenu possible de négocier et confirmer une vente par e-mail. Étant donné les agendas chargés de tout le monde, il peut sembler beaucoup plus facile de faire tout cela par voie électronique. Jusqu'il y a peu, la valeur de preuve d'un e-mail pour la vente d'une maison n'était pas encore établie.

Il est actuellement possible de conclure valablement un compromis de vente par e-mail, sms, WhatsApp et d'autres canaux digitaux. Pas besoin, dans ce cas, de signature numérique. L'acheteur et le vendeur sont néanmoins encore toujours tenus de signer ensuite l'acte authentique de vente devant notaire.

En cas de litige, le juge ne peut plus ignorer un e-mail ou un autre message électronique comme mode de preuve. Si, en tant que vendeur ou acheteur d'une maison, vous souhaitez malgré tout avoir plus de sécurité par rapport à une offre, Test-Achats a établi une lettre type que l'on peut télécharger sur son site Web et qui confirme l'offre de vente par écrit, dans un délai à définir par l'acheteur et le vendeur, en attendant la signature du compromis de vente.

BIDDIT.BE: ACHETER OU LOUER UN BIEN EN LIGNE, DE MANIÈRE SIMPLE ET EN TOUTE SÉCURITÉ

Biddit.be est une initiative de la Fédération du Notariat (Fednot). Dorénavant les vendeurs peuvent offrir leur bien immobilier en ligne d'une manière simple, transparente et sécurisée. Acheter un appartement ou une maison se révèle facile via www.biddit.be. Vous savez immédiatement dans quelle catégorie de prix se trouve un bien immobilier car il y a un prix de départ pour chaque offre. Vous pouvez faire une offre avec votre ordinateur en utilisant votre carte d'identité électronique ou via votre smartphone avec l'application Itsme. Les enchères peuvent être faites manuellement ou automatiquement, jusqu'à un montant maximum que vous avez prédéterminé et que vous seul connaissez. Chaque offre est visible par tous les visiteurs de Biddit.be. Lorsque la période d'offre de 8 jours est passée, vous savez immédiatement si votre offre était la plus haute. Dans ce cas, le notaire vous contacte, pour finaliser la vente. Beaucoup plus rapidement que pour une vente classique. Par la vente en ligne, le notaire a eu la possibilité de faire toutes les démarches et vérifications à l'avance, de façon à ce que l'acheteur et le vendeur sachent immédiatement où ils en sont. Attention, chaque offre vous engage.

Plus d'informations sur **www.biddit.be** ou via votre notaire.

SIGNATURE NUMÉRIQUE

Depuis 2016, la signature numérique a autant de valeur qu'une signature papier et les documents numériques ont donc, eux aussi, autant de valeur que les documents papier. Vous pouvez conclure des contrats par e-mail, mais il y a bien sûr un dispositif de sécurité. Les documents numériques doivent en effet contenir une signature certifiée offrant des garanties supplémentaires. Vous pouvez utiliser votre carte e-ID pour apposer une signature numérique. Vous aurez besoin à cet effet d'un lecteur de cartes ainsi que des codes fournis avec votre e-ID, et vous devrez également télécharger le logiciel. Pour de plus amples informations à ce sujet : **www.eid.belgium.be.**

PARTAGER

Il y a de plus en plus de gens qui ne souhaitent plus acheter eux-mêmes des objets aussi différents qu'une foreuse, une machine pour faire des pâtes ou une voiture mais décident d'en partager l'utilisation. L'**économie collaborative** tire parti des possibilités offertes par Internet et par la technologie mobile pour s'organiser. Même si une (petite) compensation est parfois demandée, le but n'est pas de faire des bénéfices, mais d'échanger ou de partager des objets et des services.

Il y a aussi l'**économie de plateforme**. Il s'agit souvent d'activités commerciales qui utilisent les nouvelles technologies pour mettre en contact les consommateurs et les producteurs privés de biens ou de services. Dans ce contexte, une compensation est toujours demandée. ListMinut est un exemple de ce type de plateforme.

La loi laisse pas mal d'espace aux initiatives *peer-to-peer* pour se développer mais cela ne veut pas dire pour autant qu'il n'y ait pas de règles ni de conditions à respecter.

PARTAGE ET ASSURANCES

Lorsque vous êtes actifs dans l'économie collaborative ou l'économie de plateforme, vérifiez que vous avez souscrit de bonnes assurances (familiale, incendie ou voiture). De plus en plus d'assureurs tiennent compte de ces nouveaux modes de partage et d'utilisation.

Pour plus d'informations sur le partage et les assurances: **www.abcassurance.be**

QUE FAIRE SI VOUS AVEZ PRÊTÉ UN OBJET SUR UNE PLATEFORME COLLABORATIVE ET QUE CET OBJET VOUS REVIENT ENDOMMAGÉ ?

Si vous partagez des objets sur une plateforme en ligne, il est recommandé de contrôler avec l'utilisateur l'état dans lequel se trouvent les objets quand il vient les enlever et quand il vient les restituer. Sur certaines plateformes collaboratives, vous pouvez consigner votre **accord** sous la forme d'une déclaration juridiquement contraignante. Si vous ne récupérez pas vos objets ou qu'ils vous reviennent endommagés, l'utilisateur devra les (faire) réparer ou remplacer.

QUE FAIRE SI UN BRICOLEUR DE LA PLATEFORME COLLABORATIVE SE BLESSE ?

Vérifiez avec votre assureur que votre assurance familiale couvre ce genre de cas. Si vous faites appel à des professionnels pour des travaux, vous devez avoir une assurance pour les employés de maison.

QUE FAIRE SI VOUS PARTAGEZ VOTRE PROPRE VÉHICULE AVEC D'AUTRES PERSONNES ?

Si vous partagez votre voiture avec vos voisins ou que vous la proposez **sur une plateforme *peer-to-peer*** (Cozycar, Sharynx, Dégage, Tapazz, Drivy, Caramigo), il y a des règles sur la façon de déclarer d'éventuels dégâts, la façon d'assurer le véhicule, ce qu'il faut faire en cas d'amende ou en cas de conflit avec l'utilisateur de votre véhicule.

QUE FAIRE SI VOUS PROPOSEZ UNE CHAMBRE EN LOCATION VIA AIRBNB ET QUE LE LOCATAIRE OCCASIONNE DES DÉGÂTS ?

Même quand vous proposez une chambre ou un studio en location sur la plateforme AirBnB, vous devez respecter le règlement de votre région régissant la location de chambres et de résidences à des fins de tourisme.

Si un locataire occasionne des dégâts à la chambre ou au studio que vous proposez en location, vous pouvez faire appel aux services d'AirBnB.

Si vous proposez un bien en location via AirBnb ou une autre plateforme, prenez contact avec votre assureur pour savoir si votre assurance incendie et votre assurance familiale (assurance responsabilité civile) doivent être adaptées.

INFORMATIONS SUR LA RÉGLEMENTATION :

Région flamande :
www.toerismevlaanderen.be/logiesdecreet/aanmelden
Région Bruxelles-Capitale :
www.werk-economie-emploi.brussels/fr_FR/hebergement-touristique
Région wallonne :
www.wallonie.be/fr/formulaire/detail/37415

CHECK-LIST
ACHATS DE SECONDE MAIN EN LIGNE

- Examinez le profil du vendeur et vérifiez sa réputation sur la plateforme et/ou via Google.
- Posez des questions à propos de l'article, demandez ses caractéristiques exactes. Conservez les messages échangés, l'annonce initiale et la copie du virement bancaire.
- Demandez des données personnelles, comme une adresse ou un numéro de téléphone.
- Essayez d'aller enlever personnellement les articles, certainement s'ils sont chers, pour pouvoir les vérifier avant de les emporter.
- Soyez prudent si le vendeur est situé à l'étranger. N'utilisez à aucun prix des canaux de paiement tels que Western Union ou Moneygram, et n'utilisez pas de chèques.
- Si l'achat n'arrive pas ou qu'il est endommagé, prenez d'abord contact avec le vendeur. S'il n'y a pas de réaction, vous pouvez introduire une plainte à la police.

Il est indispensable de souscrire de bonnes assurances incendie et familiale. Si vous proposez régulièrement un logement à la location, ce qui s'apparenterait plus à une activité professionnelle, vous allez devoir souscrire une police 'responsabilité civile exploitation'.

Si vous louez un bien avec AirBnb, pour éviter toute fraude, réalisez toutes les transactions via leur site officiel. N'acceptez pas de conclure la réservation par e-mail par exemple. De même, pour le paiement, faites-le sur le site avec une carte de crédit de manière sécurisée.

LES PLATEFORMES COLLABORATIVES ET LE FISC

Les revenus issus de l'économie collaborative vont bénéficier d'un régime fiscal de faveur. Jusqu'à 6.000€ par an, ils seront exonérés de taxes. Vous devez déclarer ces revenus dans votre déclaration fiscale. La plateforme par le biais de laquelle vous avez obtenu ces revenus doit être agréée par le ministère des Finances.

Pour connaître les plateformes agréées et en savoir plus sur les conditions :
https://finances.belgium.be/fr/particuliers/avantages_fiscaux/economie-collaborative.

BANQUE

Personne ne veut avoir la surprise désagréable de voir que son compte bancaire a été pillé ou sa carte de crédit utilisée frauduleusement. Les banques font tout ce qu'elles peuvent pour sécuriser de façon stricte leurs applications mobiles et en ligne mais tous ces protocoles de sécurité perdent leur utilité si les clients communiquent leurs données bancaires par le premier e-mail venu. Les utilisateurs peuvent s'éviter pas mal de désagréments en prenant quelques mesures de précaution élémentaires.

COMMENT RECONNAÎTRE UN E-MAIL D'HAMEÇONNAGE (PHISHING) ? QUE FAIRE QUAND ON S'Y EST FAIT PRENDRE ?

L'hameçonnage est la tentative par une personne d'extorquer vos données personnelles, numéros de comptes et codes PIN, en se faisant passer pour votre banque (ou pour la société émettrice de votre carte de crédit, ou pour la police, ou toute autre instance). L'hameçonnage représente de loin la plus grande part des tentatives d'escroquerie relevées par les banques.

Vous recevez un e-mail ressemblant à celui que vous enverrait votre banque (ou une entreprise, ou une autre instance) qui vous demande de vous connecter en utilisant le lien inclus dans le message. L'expéditeur ajoute avec insistance que si vous ne le faites pas, votre carte sera par exemple bloquée. Le lien en question vous dirige vers un site Web, frauduleux mais crédible, sur lequel il vous est demandé d'introduire en guise de contrôle votre code PIN ou le code généré par votre lecteur de carte. Si vous faites cela, des personnes pourront piller votre compte.

Les escrocs adaptent en permanence leur modus operandi, leurs e-mails d'hameçonnage ont une apparence de plus en plus professionnelle. Ils recherchent de nouveaux canaux et adaptent leur message. Outre les e-mails, ils recourent de plus en plus souvent à des médias sociaux comme Facebook ou WhatsApp pour piéger les gens. Ils vont aussi plus souvent subtiliser de plus petites sommes, en plusieurs tentatives, afin de pouvoir rester plus longtemps sous le radar.

COMMENT PRÉVENIR L'HAMEÇONNAGE ?

Il y a moyen de prévenir l'hameçonnage avec quelques mesures de précaution. La plus importante : **ne communiquez jamais en ligne vos données ou codes personnels**. Une banque ne demandera jamais vos codes personnels par e-mail. Si vous recevez ce genre de demande, cela doit déclencher une sonnette d'alarme.

Même si les e-mails d'hameçonnage deviennent de plus en plus professionnels, il est souvent possible de les reconnaître : par l'adresse e-mail de l'**expéditeur**, qui diffère de façon un peu étrange de l'adresse e-mail officielle de la banque (par exemple avec une extension qui n'est pas .be ou .com), par la **façon de s'adresser** (non nominative) et par le **ton contraignant** ('votre carte va être bloquée si vous ne réagissez pas'). De plus, les transactions bancaires en ligne se font systématiquement via un **site Web sécurisé**, affichant un petit cadenas dans la ligne d'adresse et commençant par http**s**://. Pour effectuer des opérations en ligne, il est recommandé de vous rendre directement sur le **site Web de la banque**, plutôt que d'utiliser un lien indirect.

Vous pouvez empêcher de nombreuses tentatives d'hameçonnage avec un **bon antivirus, un solide pare-feu et un filtre anti-spams**. Et si l'expéditeur vous est inconnu, ne cliquez jamais sur un lien inclus dans son message.

Si vous recevez un e-mail suspect, transmettez-le à **votre banque**, à phishing@(nom de la banque).com ou .be. La banque peut alors bloquer le lien suspect et prendre les précautions qui s'imposent afin que d'autres clients ne soient pas touchés par la tentative d'escroquerie. Vous pouvez également signaler le message auprès du **Point de contact du SPF Économie** (https://pointdecontact.belgique.be) ou le transmettre à suspect@safeonweb.be au **Centre pour la Cybersécurité Belgique** (CCB). Au CCB, le message est scanné et si nécessaire analysé plus en détail. Le CCB signale les messages frauduleux aux principaux éditeurs de logiciels antivirus ainsi qu'aux fournisseurs de navigateurs Internet, pour qu'ils puissent bloquer ces liens frauduleux.

CHECK-LIST
OPÉRATIONS BANCAIRES EN TOUTE SÉCURITÉ

- Faites attention aux e-mails d'expéditeurs inconnus.
- Ne cliquez jamais sur un lien suspect dans un e-mail.
- Installez une bonne protection antivirus.
- Utilisez la version la plus récente pour les applis, les logiciels, les systèmes d'exploitation.
- Mettez les logiciels et les systèmes d'exploitation à jour. Les mises à jour contiennent souvent des patches de sécurité.
- Tenez votre compte bancaire à l'œil afin de détecter rapidement une éventuelle transaction suspecte.
- Si vous effectuez des opérations bancaires avec votre smartphone, fermez toujours les sessions quand vous avez terminé.
- Si votre smartphone a été volé, faites immédiatement bloquer votre carte bancaire. Vous bloquerez ainsi l'accès à l'application bancaire.
- N'utilisez pas de réseaux WiFi publics pour vos opérations bancaires en ligne.
- **Ne communiquez jamais vos codes personnels.**

AVEZ-VOUS ÉTÉ VICTIME D'HAMEÇONNAGE ?

Contactez immédiatement votre banque ou Cardstop pour **bloquer votre carte/vos cartes**. Si de l'argent a déjà été prélevé de votre compte, vous devez **déposer plainte à la police**. Vous pouvez ensuite utiliser cette plainte pour demander à la banque de **récupérer la somme concernée**. La banque étudie chaque cas de manière individuelle, vérifie si vous êtes de bonne foi et/ou si vous n'avez pas fait preuve de négligence. Dans la plupart des cas, les banques remboursent les sommes perdues. Mais vous serez passé par de nombreuses tracasseries administratives.

APPLIS DE PAIEMENT MOBILE

Pour payer dans un magasin, vous scannez le code QR et introduisez votre code PIN, ou sélectionnez le commerce dans une liste se trouvant sur votre smartphone.

Ces applis de paiement sont reliées dans votre smartphone à votre compte à vue (après installation unique via votre carte) ainsi qu'à votre numéro de téléphone ou votre adresse e-mail. Cela vous permet par exemple de transférer directement de l'argent à un membre de votre famille ou un(e) ami(e) lorsque vous faites une activité ensemble. Vous retrouverez ces personnes dans votre liste de contacts via leur numéro de téléphone ou leur adresse e-mail. Si elles ont installé la même appli (également après une première connexion à leur compte à vue), vous pourrez leur transférer de l'argent immédiatement. Vous trouverez de plus amples informations sur le site Web de votre banque. Il est également conseillé d'examiner les conditions d'utilisation et de confidentialité afin de savoir ce qui se passera avec vos données.

NOUVELLES RÈGLES POUR LES PAIEMENTS EN LIGNE

À partir de l'automne 2018, votre banque peut donner à des parties tierces, comme d'autres banques ou des webshops, l'accès à vos données dans la mesure où vous avez donné votre consentement explicite à cet effet. Il sera alors par exemple possible d'intégrer dans l'appli de votre banque la liste des comptes à vue dont vous disposez dans d'autres banques, de façon à ce que vous puissiez effectuer tous vos paiements à partir d'une seule appli. Ou effectuer des paiements via des webshops, sans carte de banque ni carte de crédit. Ou utiliser des applis pour demander des comparaisons de prix entre différents fournisseurs, sur la base de vos dépenses de télécommunications ou d'énergie. Les parties tierces sont contrôlées par la Banque nationale et doivent respecter des prescriptions de sécurité strictes.

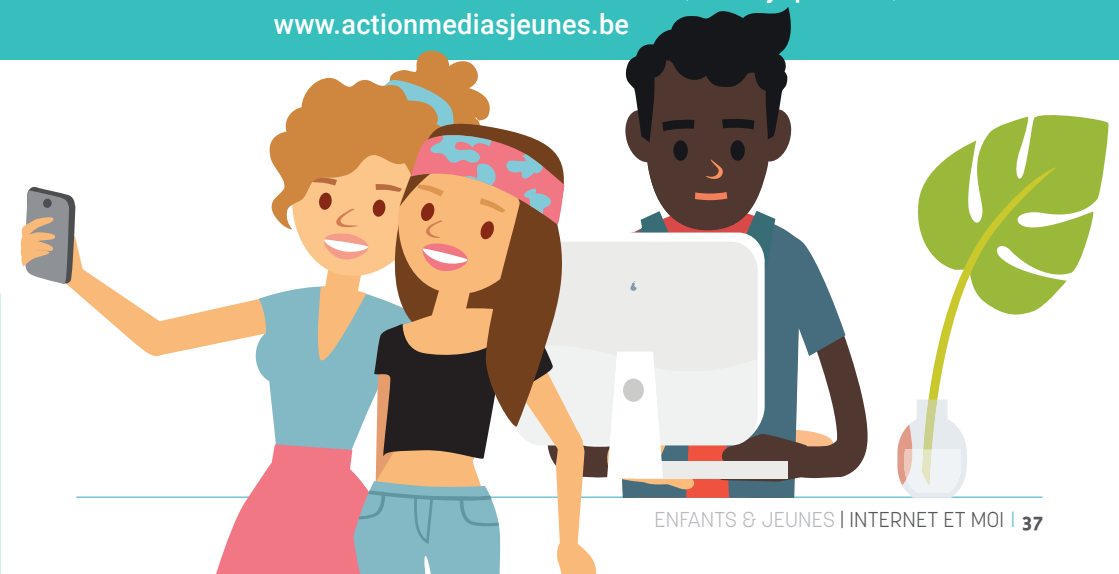
Vous trouverez de plus amples informations à propos des opérations bancaires en ligne sur le site Web de Febelfin : **www.safeinternetbanking.be/fr**. Ce site vous informe également sur les différentes formes de fraude en ligne. Vous trouverez aussi des informations à ce sujet sur le site Web du SPF Économie et sur celui de Cyber Security Belgique (**www.safeonweb.be/fr**).

3. ENFANTS & JEUNES

Le piège principal serait de penser que les digital natives n'ont plus rien à apprendre. Certes, ils maîtrisent la technologie, mais il leur manque encore souvent les compétences émotionnelles ou l'expérience dont ils ont besoin pour se défendre en ligne.

Les parents et les enseignants ont donc un réel rôle à jouer : accompagner les jeunes en ligne, les aider à évaluer les risques, à traiter les informations trouvées, à réagir face aux cyberpersécuteurs et aux *fake news*. Ou encore : leur apprendre la notion de vie privée et de son respect, vis-à-vis d'eux-mêmes mais aussi des autres.

Pour des informations générales et des trucs & astuces sur l'accompagnement en ligne des enfants et des jeunes ainsi que des informations générales sur Internet et les médias sociaux : **www.webetic.be**, **www.yapaka.be**, **www.actionmediasjeunes.be**



JEUNES ENFANTS

POUVEZ-VOUS EXCLURE LES CONTENUS INAPPROPRIÉS SUR INTERNET POUR LES ENFANTS ?

Il n'existe pas de solution sans faille. Il est donc important que les parents s'impliquent dans les activités en ligne de leur enfant et **discutent de ce qu'ils y trouvent, y voient**. Les moyens techniques ne peuvent à eux seuls remplacer ce dialogue permanent entre parents et enfants.

Ceci dit, de nombreux navigateurs et applis vous permettent de limiter en partie ou totalement l'accès aux enfants. Google propose ainsi une option **'safe search'** qui exclut certains contenus des résultats de recherche, comme la pornographie. Sur la plupart des navigateurs, vous pouvez créer des profils personnels pour chaque membre de la famille et limiter ainsi les options de recherche en fonction de l'âge.

YouTube, le rendez-vous en ligne incontournable des enfants et des jeunes, dispose d'un **'restricted mode'** : celui-ci masque certains contenus et les commentaires, parfois pire que les vidéos. Vos enfants souhaitent poster eux-mêmes des vidéos, mais vous voudriez éviter que tout le monde puisse les voir ou les commenter ? Dans ce cas, vous pouvez régler les paramètres de confidentialité du canal sur 'privé'.

Quant aux applications pour iOs ou Android, vous pouvez vérifier la catégorie d'âge à laquelle elles conviennent au moyen des **scores PEGI**. Vous pouvez paramétrer la fonction de recherche d'un compte dans les magasins d'applis de façon à ce que les enfants en quête d'une application n'accèdent qu'aux résultats basés sur un certain score PEGI **(https://pegi.info/fr)**.

LES ENFANTS PEUVENT-ILS ÊTRE ACTIFS SUR LES RÉSEAUX SOCIAUX ?

La plupart des réseaux sociaux fixent la limite d'âge pour se créer un profil à 13 ans. C'est également l'âge minimum établi par la législation belge concernant l'accès pour les mineurs : les jeunes peuvent alors donner eux-mêmes leur consentement pour le traitement de leurs données personnelles. Les plus jeunes enfants peuvent également utiliser des services en ligne comme les médias sociaux, à condition d'avoir la permission de leurs parents et si cela est en conformité avec les conditions d'utilisation de la plateforme.

CHECK-LIST
TEMPS À L'ÉCRAN

- Etablissez le plus possible un dialogue avec votre enfant lorsqu'il joue en ligne. Adaptez les règles à chaque âge.
- Réalisez éventuellement ensemble un plan pour décider où et quand votre enfant peut utiliser une tablette, un ordinateur ou un smartphone.
- Ne vous focalisez pas uniquement sur la durée, vérifiez les conséquences pour votre enfant et l'équilibre par rapport à d'autres activités.
- Donnez le bon exemple : si votre enfant n'est pas autorisé à utiliser son smartphone à table, mettez aussi le vôtre de côté.
- Si vous souhaitez limiter la durée : il existe des applications qui bloquent l'accès à l'ordinateur, la tablette, le smartphone, la console ou la smart-TV après une certaine heure ou un certain laps de temps.

Dans la pratique, les enfants de moins de 13 ans sont massivement actifs sur Facebook, Instagram, Snapchat, WhatsApp ou YouTube – parfois à l'insu de leurs parents. Si un enfant de moins de 13 ans souhaite se créer un profil et obtient l'autorisation de ses parents malgré les conditions d'utilisation, alors mieux vaut le faire ensemble. Il est ainsi possible de régler les paramètres de confidentialité et de se mettre d'accord sur certains points, comme l'ajout de contacts.

POUVEZ-VOUS PARTAGER DES PHOTOS DE VOTRE ENFANT SUR LES RÉSEAUX SOCIAUX ?

Faites très attention lorsque vous partagez des photos et des vidéos de vos enfants. Dans la mesure du possible, veillez à discuter avec eux de ce qu'ils apprécient ou non. Vous pouvez aussi leur demander

systématiquement s'ils sont d'accord avant de poster une photo en ligne. Optez de préférence pour une photo sur laquelle ils ne sont pas directement reconnaissables, comme une photo de dos ou avec un filtre, et veillez aux paramètres de confidentialité de votre profil.

DROIT À L'IMAGE

Personne ne peut télécharger une photo de vous ou de vos enfants en ligne et l'utiliser sans votre autorisation. Même si la personne a pris elle-même la photo en question, elle ne peut la diffuser sans votre permission. Il est permis cependant de prendre l'espace public en photo, même si, par hasard, vous vous y trouvez.
Si vous constatez qu'un tiers utilise une photo de vous sans votre permission, vous pouvez demander à cette personne de supprimer la photo. Si cette personne a posté votre photo sur les médias sociaux et ne réagit pas à votre demande de retrait, vous pouvez demander à l'entreprise de média social de le faire.
Plus d'informations sur le droit à l'image sur :
www.sofam.be, **www.educationauxmedias.eu et https://economie.fgov.be/fr/themes/propriete-intellectuelle/droit-dauteur/droit-limage**

POUVEZ-VOUS CONSULTER LE PROFIL PRIVÉ DE VOTRE ENFANT ? LIRE SES E-MAILS ? CONTRÔLER SON COMPORTEMENT DE NAVIGATION ?

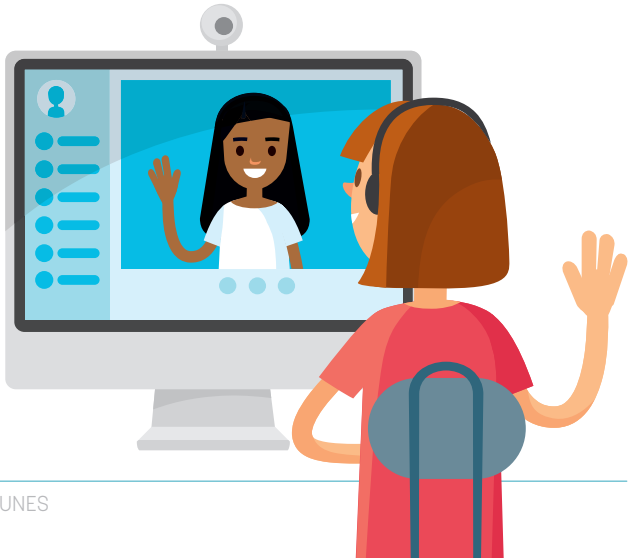
Même en ligne, les enfants ont le droit à la vie privée. Les parents ne devraient donc pas aller trop loin dans le contrôle de l'utilisation d'Internet de leur enfant. L'objectif : trouver un **équilibre entre protection et contrôle** d'une part, et **droit à la vie privée de l'enfant** d'autre part.
Certains parents tentent d'exercer un contrôle en demandant à leur enfant de les accepter comme 'amis' sur leurs réseaux sociaux. Ceux-ci ne voient pas toujours cette requête d'un très bon œil, surtout quand ils sont ados. S'ils acceptent malgré tout (ou y sont forcés), ils adaptent souvent leurs paramètres de confidentialité pour masquer une partie du contenu ou migrent vers d'autres médias sociaux.

Sur le marché, il existe des applications qui permettent un contrôle parental poussé, comme la surveillance à distance des activités de l'enfant sur les médias sociaux ou le suivi de sa localisation. Il est conseillé d'éviter ce genre de pratique, dans la mesure du possible. Il est important que les enfants apprennent, petit à petit, quitte à faire quelques erreurs, à se défendre en ligne.

LES ENTREPRISES PEUVENT-ELLES BOMBARDER LES ENFANTS DE MESSAGES PUBLICITAIRES EN LIGNE ?

Les enfants et les jeunes ont le droit de s'épanouir librement. Lorsque des entreprises suivent leur comportement de navigation pour adapter ensuite leurs messages de marketing direct, ils sont catégorisés, très tôt déjà. De plus, les jeunes ne savent pas évaluer les conséquences de l'appropriation de leurs données par des entreprises (de médias sociaux). Ils ne voient pas le lien entre leur historique de recherche ou leur profil Facebook et les publicités qui leur sont proposées.

L'Union européenne déconseille la publicité sur base du comportement de navigation des jeunes. Mais ce n'est pas une interdiction formelle. Pour les enfants en dessous de 13 ans, les parents doivent donner leur autorisation pour que les données personnelles de l'enfant soient accessibles.



CHECK-LIST
ENTRE CONTRÔLE ET LIBERTÉ

- Le fait de laisser l'ordinateur ou la tablette dans le salon ou une autre pièce commune, permet de garder un œil discret sur les activités en ligne.
- Intéressez-vous aux activités en ligne de votre enfant. Vous augmentez ainsi la probabilité qu'il se tourne vers vous en cas de problème.
- Passez des accords avec lui sur ce qui est autorisé ou non, par exemple : ne pas envoyer de photos ou vidéos sans permission.
- Examinez avec lui comment il gère ses paramètres de confidentialité et l'attitude à adopter face à une difficulté.
- Si à un moment ou un autre vous devez contrôler vos enfants, faites le de la manière la plus ouverte possible. Fouiller ses mails ou consulter son profil Facebook derrière son dos risque de rompre la confiance qu'il a en vous.
- Lorsqu'un enfant fait une 'bêtise' en ligne, essayer de lui expliquer au mieux les implications, les conséquences de son acte.

Les annonceurs ne sont pas censés faire du marketing direct destiné aux enfants en dessous de 12 ans. Dans la pratique, c'est très difficile à contrôler dans la mesure où les enfants peuvent facilement mentir sur leur âge lorsqu'ils sont en ligne.

QUE FAIRE SI UN ENFANT EFFECTUE DES ACHATS NON PERMIS VIA UNE APPLI ?

Mieux vaut prévenir que guérir ou, dans ce cas, tenter de récupérer la somme à postériori. Les parents ont donc tout intérêt à bien expliquer ce que sont les achats intégrés (les achats qui sont proposés dans l'appli elle-même), comment les reconnaître et de se mettre d'accord sur ce qui est permis ou non. Ils peuvent également choisir de ne pas associer leur carte de crédit à l'appli du magasin ou de sécuriser les achats via ce dernier au moyen d'un mot de passe. Autre option : utiliser une carte prépayée.

Ils peuvent être avertis par message lors d'un achat, au cas où l'enfant aurait tout de même trouvé une façon de contourner la consigne, et peuvent ainsi éviter le pire.

QUE FAIRE SI DES INCONNUS PRENNENT CONTACT AVEC UN ENFANT OU UN ADO EN LIGNE ?

Il est important d'apprendre aux enfants à se montrer **prudents envers les demandes d'ajout à une liste d'amis** de la part d'inconnus sur les médias sociaux ou les contacts sur des 'chatrooms', à ne pas accepter les demandes de personnes qu'ils ne connaissent pas 'offline', à ne **jamais transmettre de données personnelles**, et à **s'adresser à l'un de ses parents** ou un autre adulte de confiance si quelque chose leur paraît louche.

Lorsqu'un enfant signale une communication inappropriée, il peut récolter des **preuves matérielles** lui-même ou avec votre aide au moyen de captures d'écran (sessions de chat avec mention de la date et de l'heure, SMS, photos). Vous pouvez ensuite prendre contact avec **l'entreprise de médias sociaux et avec Child Focus**. Le grooming en ligne, stratégie par laquelle l'agresseur vise à gagner peu à peu la confiance de l'enfant pour lui fixer un rendez-vous, est punissable. Il est parfois nécessaire de faire appel à la police pour éviter le pire, à votre enfant et à tous les autres.

QUE FAIRE LORSQUE L'UN DES PARENTS DONNE SA PERMISSION ET L'AUTRE NON ?

L'autorité parentale est exercée par les deux parents. À l'instar des autres questions d'éducation, il est possible que les parents ne soient pas sur la même longueur d'onde concernant la vie en ligne de leur enfant. L'idéal est de parvenir à un accord, même en cas de séparation. Lors de divorce ou de rupture difficile, l'utilisation des médias sociaux peut être une pomme de discorde. L'un des parents peut ainsi autoriser sa fille de 11 ans à avoir un profil Facebook, tandis que l'autre s'y oppose. Dans ce cas, ce dernier peut demander à Facebook de fermer le compte, et l'entreprise

s'exécutera, car ses conditions interdisent la création d'un compte pour un enfant de moins 13 ans sans permission. Il est toutefois préférable de résoudre ce conflit en dialoguant avec l'autre parent et l'enfant. En dernier recours, on se tournera vers le tribunal.

ADOS

QUE FAIRE SI VOTRE ADO EST HARCELÉ EN LIGNE ?

Souvent, le cyberharcèlement est un prolongement du harcèlement dans la vie réelle. Toutefois, sur les médias sociaux, les messages de harcèlement se diffusent comme une trainée de poudre et atteignent rapidement un public bien plus large. Quand un enfant est harcelé en ligne, mieux vaut donc intervenir rapidement.

Parfois, les parents désireux de protéger leurs enfants du cyberharcèlement optent pour une solution radicale : limiter voire bannir l'utilisation des médias sociaux. Cependant, la vie en ligne et hors ligne des enfants et des jeunes est intimement liée. L'enfant harcelé pourra donc percevoir cette décision comme une punition injuste et celle-ci pourrait se révéler inefficace.

L'essentiel est d'apprendre, petit à petit, **à l'enfant à se défendre en ligne**, y compris contre les harceleurs. Le plus important sera de conserver une relation de confiance. Si l'enfant trouve auprès de ses parents du réconfort et du soutien, la famille pourra plus facilement élaborer une stratégie pour lutter contre ce type de persécutions.

Même sans être un as de la technologie, certaines fonctionnalités peuvent se révéler très utiles: il est possible de **renforcer les paramètres de confidentialité** afin d'empêcher les harceleurs de poster un message sans approbation ; bloquer le harceleur ; signaler les messages de harcèlement au média social via le bouton d'alerte. Grâce à des captures d'écran, vous pourrez **prouver** le harcèlement. Toutefois, par honte, les enfants suppriment souvent ce type de messages.

Il faut savoir que les entreprises de médias sociaux n'accèdent pas toujours aux **demandes de suppression de messages ou de pages**. Elles ne le font qu'en cas d'infraction à leur code de conduite. Pour savoir comment réagir au mieux dans votre situation, vous pouvez contacter le portail Click Safe pour un usage sûr et responsable d'Internet, de Child Focus **(www.clicksafe.be)** ou vous adresser au Délégué général aux droits de l'enfant **(www.dgde.cfwb.be)**.

Pour lutter contre le cyberharcèlement et le harcèlement dans la vie réelle, les armes sont identiques. Dans la plupart des cas, les cyberharceleurs sont scolarisés dans le même établissement que l'enfant. L'école peut donc être un allié de taille.

Les parents doivent être extrêmement prudents lorsqu'ils sont tentés de prendre eux-mêmes les choses en main en postant, par exemple, des vidéos en ligne. Ils pourraient se mettre en tort en partageant les données personnelles de mineurs, sans autorisation. De plus ils risqueraient d'entrer dans une escalade qui pourrait se retourner contre les intérêts de la famille.

Quand ils l'estiment nécessaire, dans les cas graves, comme lorsqu'il y a des menaces de violence physique, les parents peuvent entreprendre des démarches juridiques. Lorsqu'un enfant est l'auteur de harcèlement (grave) et qu'une plainte est déposée, les règles habituelles de responsabilité parentale du fait d'enfants mineurs sont d'application. Dans certains cas, la responsabilité du jeune peut également être engagée.

Sur **www.childfocus.be** ou **www.stopcyberhate.be**, enfants & ados, parents et professionnels trouveront des conseils et des plans par étape pour lutter contre le cyberharcèlement.

CHECK-LIST CYBERHARCÈLEMENT

- Ensemble, renforcez les paramètres de confidentialité et bloquez le(s) harceleur(s).
- Via le bouton d'alerte, signalez le harceleur au réseau social.
- Prenez des captures d'écran en guise de preuves matérielles.
- Impliquez l'école.
- Éventuellement, lorsque vous estimez que le harcèlement est grave, déposez une plainte.
- Ne postez pas vous-même des vidéos des harceleurs en ligne.

COMMENT SUPPRIMER DES IMAGES OU DES MESSAGES NUISIBLES OU OFFENSANTS ?

Face à une photo offensante, trop révélatrice, ou à une vidéo malveillante, le premier réflexe est : « il faut supprimer cela tout de suite ». Vous pouvez **demander aux entreprises de médias sociaux de supprimer le contenu offensant via le bouton d'alerte**. Dans les cas graves, celles-ci accèdent généralement à la demande, mais peuvent tarder à répondre.

Le plus rapide est de **demander à l'auteur des faits de supprimer les messages ou images, et/ou de contacter ses parents**. Si cela ne fonctionne pas et en l'absence de réaction de la part des réseaux sociaux, les parents ou les jeunes eux-mêmes peuvent se tourner vers **Child Focus**. L'école peut également jouer un rôle de médiation.

Ils peuvent également déposer plainte auprès de l'Autorité de la protection des données ou de la police. Mais si l'objectif est de supprimer le contenu offensant, cela sera plus rapide via Child Focus, qui dispose d'une ligne directe avec les réseaux sociaux.
Il est judicieux de déposer une plainte lorsque les autres parties font la sourde oreille, que la personne incriminée refuse de supprimer le contenu ou lorsqu'il existe un danger pour l'enfant, notamment en cas d'images très explicites. Child Focus vérifiera alors avec les parents et éventuellement avec la police si les images se sont propagées et si l'enfant a besoin d'un accompagnement.

SEXTING :
UNE EXPÉRIENCE INNOCENTE OU UN TERRAIN MINÉ ?

Les jeunes **expérimentent**. Ils explorent leur corps et se montrent curieux envers celui des autres. À l'époque numérique, ils se tournent aussi vers la technologie pour assouvir cette curiosité. Un jeune sur dix indique être adepte du sexting – soit l'envoi de messages ou de photos de soi-même, à connotation sexuelle, pour flirter, attirer l'attention, ou 'prouver son amour'. Dans plus de trois quarts des cas, le destinataire est un partenaire ou un(e) ami(e).

Céder à la panique ne sert à rien. Lorsqu'il s'avère qu'un jeune pratique le sexting, mieux vaut **discuter avec lui des limites et des risques. Il est essentiel qu'il ne se livre à cette pratique qu'avec quelqu'un en qui il a totalement confiance.**

Lorsqu'un jeune partage des images intimes avec son petit ami / sa petite amie avec consentement mutuel et pour leur utilisation personnelle, cela n'est pas punissable. Ce n'est pas non plus considéré comme de la pornographie infantile. Par contre, l'envoi d'une photo, par un jeune, sans la permission de la personne y figurant, peut être punissable.

Soyez attentif et repérez les signaux indiquant que l'enfant a pu être forcé à faire ou à partager ces photos. **Pour plus de sécurité, le mieux est de masquer le visage.**

Il faut être attentif à ne pas céder à la tentation de désigner un coupable trop rapidement. Il y a faute lorsque quelqu'un rompt la confiance et envoie une photo compromettante. En effet, quand la photo est envoyée, celui-ci n'a plus aucun contrôle sur son utilisation.

LE VISIONNAGE D'IMAGES PORNOGRAPHIQUES EN LIGNE PAR DES JEUNES EST-IL PUNISSABLE ?

Officiellement, il faut avoir au moins 18 ans pour regarder du porno. Toutefois, ces images sont tellement accessibles que cette limite d'âge reste théorique. Dans la pratique, le visionnage de contenu pornographique par des jeunes n'est pas punissable. Par contre, l'envoi de telles images, à des amis par exemple, est bel et bien sanctionnable.

Il est important que les parents parlent de la pornographie en ligne avec leurs enfants. De telles images peuvent entraîner la confusion chez les jeunes et la vue de corps 'irréalistes' peut miner leur confiance en eux. Les parents doivent être attentifs aux signaux d'alarme trahissant une consultation trop fréquente de ces sites. Si le jeune montre des signes d'utilisation abusive ou d'un début d'addiction, vous pouvez vous adresser à un psychologue ou à un sexologue.

Plus d'informations pour les jeunes sur la pornographie en ligne : www.yapaka.be ou www.webetic.be. Vous pouvez signaler des images illégales à Child Focus : **www.childfocus.be**.

VLOGS

Après l'école, les enfants et les ados se ruent massivement sur Internet pour y « binge-watcher » les vlogs (blogs vidéo) de leurs héros YouTube. De nombreux ados s'essayent à leur propre canal vlog. Les parents qui souhaitent sécuriser l'environnement de leur jeune vlogueur peuvent désactiver l'option commentaires ou filtrer les réactions négatives. Ils peuvent demander que l'enfant leur montre systématiquement son vlog avant de le publier en ligne.

CHECK-LIST JEUX EN LIGNE

- Le jeune doit être attentif à ne pas utiliser son vrai nom, ne pas communiquer son adresse ou sa localité via le chat. Il doit rester prudent lorsqu'il envoie des photos.
- Est-ce qu'il s'agit d'un chat sur un jeu en ligne? Veillez à ce que la conversation se cantonne au jeu et dans le jeu.
- Faites attention au score PEGI afin de choisir des jeux adaptés à chaque âge ou regardez des vidéos 'trucs et astuces' sur YouTube pour vous faire une idée du contenu.
- Un jeune joue trop ? Incitez-le à avoir encore d'autres hobbys, à voir des amis et à ne pas négliger ses obligations, comme par exemple les devoirs scolaires.
- Si l'impossibilité de jouer est source de colère, d'angoisse ou de mauvaise humeur, alors il faut réagir et se tourner éventuellement vers des professionnels.
- Prenez éventuellement conseil auprès de spécialistes. De plus en plus d'unités psychiatriques prennent en compte également ce type d'addiction avec une approche ciblée.

SNAPCHAT: CAPTURES D'ÉCRAN ET GÉOLOCALISATION

Snapchat, une application permettant d'envoyer des messages, des photos et des récits vidéo à un réseau d'amis connaît une popularité fulgurante chez les ados. Ces messages restent disponibles pendant 24 heures pour les destinataires et se suppriment automatiquement, à moins d'être sauvegardés. Les posts sont effacés du serveur de Snapchat après 30 jours maximum. Snapchat présente toutefois des dangers pour les personnes convaincues de la totale disparition des messages. Le destinataire peut, par exemple, prendre une capture d'écran de votre post et éventuellement la diffuser. Snapchat vous signale lorsque quelqu'un prend une capture d'écran, mais cette fonction peut être contournée. Il est également conseillé aux parents d'avertir leurs ados quant à la fonction de géolocalisation, via laquelle tous leurs contacts peuvent savoir où ils se trouvent. Les utilisateurs peuvent se rendre invisibles, ou visibles uniquement par leurs plus proches contacts.

ÉCOLE

L'ÉCOLE PEUT-ELLE POSTER DES PHOTOS DE VOTRE ENFANT EN LIGNE ?

Au début de l'année scolaire, les parents doivent indiquer s'ils consentent à la diffusion de photos et vidéos de leur enfant sur le site Internet ou la page Facebook de l'école. Idéalement, les parents devraient pouvoir donner leur autorisation pour chaque utilisation. Par exemple, non pour Facebook, mais oui pour la page photo (fermée) de l'école. Dans les faits, de nombreuses écoles ne demandent qu'une seule et unique permission.

Parfois, les écoles se montrent encore négligentes en matière de droit à l'image. Certaines d'entre elles disposent ainsi d'une page Facebook par classe et la rendent 'publique' – soit accessible à tous, même aux personnes non inscrites sur le réseau social. Ils entendent ainsi permettre à tous les parents de la consulter, mais l'ouvrent alors à tout le monde par la même occasion. D'autres écoles tiennent des blogs de classe sur le site de l'école et omettent de les sécuriser au moyen d'un mot de passe. Les parents opposés à la diffusion d'images de leur enfant ont donc plutôt intérêt à refuser cette permission.

Les différents réseaux de l'enseignement ont leurs propres directives pour les écoles. Par ailleurs, l'Autorité de protection des données a mis au point un plan par étapes pour aider les écoles à mieux protéger les données. Cette brochure peut être téléchargée sur le site Web de l'APD : **www.autoriteprotectiondonnees.be**.

UN ENFANT PEUT-IL UTILISER SON SMARTPHONE À L'ÉCOLE ?

La politique relative à l'utilisation du smartphone figure dans le règlement de l'école. Certaines écoles interdisent ces appareils et obligent les élèves à les ranger discrètement toute la journée au sein

de l'établissement. D'autres par contre, tolèrent le pianotage durant les pauses. Pendant les cours, le téléphone peut alors être placé dans un bac, par exemple.
Les écoles ont le droit de confisquer des affaires personnelles si les élèves s'en servent pour perturber le cours ou troubler l'ordre. Et cela vaut pour le smartphone. Elles ne peuvent toutefois le conserver plus que nécessaire. La plupart du temps, cette durée est spécifiée dans le règlement de l'école. Elles ne sont pas non plus autorisées à en consulter le contenu sans l'autorisation du jeune et de ses parents.

Dans les hautes écoles et les universités, il est plus difficile de restreindre l'utilisation des smartphones et des ordinateurs portables. Les récits de tricherie via smartphone ou smartwatch sont légion. Chaque établissement scolaire fixe ses règles contre la fraude numérique dans son règlement d'examen. Beaucoup interdisent les smartphones et smartwatchs pendant les examens, mais cela ne suffit pas toujours.

Par conséquent, ils cherchent d'autres façons de lutter contre la fraude comme l'utilisation d'un scanner portable capable de détecter un smartphone allumé dans un rayon de vingt mètres, ou l'installation obligatoire d'un logiciel sur l'ordinateur portable permettant aux professeurs de suivre l'écran au cours de l'examen.

Plus d'informations pour les enfants et les jeunes:
www.jeminforme.be
www.jedecide.be
www.clicksafe.be

Plus d'informations pour les adultes :
www.childfocus.be
www.yapaka.be
www.webetic.be
www.jedecide.be
www.clicksafe.be

4. TRAVAIL

La technologie mobile a ébranlé la notion de travail de bureau. Le travail n'est plus systématiquement synonyme de poste fixe, de bureau en îlot. Avec Internet, il n'a plus de limites. Les professionnels pianotent sur leurs smartphone, tablette, ou ordinateur portable dans le train, à la maison, à l'aéroport, au café, dans le parc ou en déplacement chez des clients. Le lieu de travail est partout.

De nombreuses personnes utilisent leur ordinateur portable ou smartphone professionnel à l'extérieur du lieu de travail ou en dehors des heures de bureau. D'autres ont recours à l'ordinateur au travail afin de réserver un restaurant pour le soir ou jeter un coup d'œil à leur fil d'actualités Facebook, pendant la pause-café, le lunch, ou quand ils ont un instant de libre.

Que peut-on faire ? Que ne peut-on pas faire ? Pour les employeurs et les salariés, la question manque encore de clarté. Le lieu de travail n'est pas un salon privé. Lorsque vous signez un contrat d'embauche, vous acceptez que vos droits soient limités dans le cadre professionnel. Cela n'implique toutefois pas la suppression de votre droit à la vie privée ou de votre liberté d'expression.

Nous passons beaucoup de temps au travail. Selon la Cour européenne des droits de l'homme, il est dès lors parfaitement normal d'avoir le droit d'y envoyer un message privé, par exemple, ou de chercher une bonne adresse en ligne. De plus, avec le télétravail, la frontière entre vie professionnelle et privée s'estompe.

LA TRANSPARENCE, SOURCE DE SOLUTIONS

De nombreux conflits peuvent être évités grâce à des règles claires sur l'utilisation d'Internet dans le règlement de travail, ou une **politique Internet** du bureau spécifiant où, quand, et comment les sala-

riés sont autorisés à utiliser Internet, leur e-mail et les médias sociaux sur le lieu de travail. Les employeurs doivent alors communiquer explicitement ces directives.

Avec des accords clairs, sans utilisation abusive, et tant que le travail est accompli, de nombreux employeurs sont disposés à faire preuve d'une relative souplesse quant à l'utilisation d'Internet sur le lieu de travail, même si certaines entreprises préfèrent en bloquer l'accès.

Afin de garantir le bon fonctionnement de l'entreprise, un employeur peut **exercer un contrôle**. Et grâce à l'évolution rapide de la technologie, il dispose pour ce faire de nombreux outils de contrôle. Différentes lois et règlements collectifs de travail déterminent ce qu'il a le droit de faire, ou non.

En cas de conflit, la personne de confiance au travail, le syndicat ou l'Autorité de protection des données peut intervenir. Étant donné la relation d'autorité entre l'employeur et le salarié, ce dernier n'entreprend souvent une telle démarche qu'après licenciement. Il peut également se tourner vers le tribunal du travail.

UN EMPLOYEUR PEUT-IL RECHERCHER LE PROFIL D'UN CANDIDAT SUR LES MÉDIAS SOCIAUX ?

Les médias sociaux offrent des occasions de sortir du lot en tant que postulant. Sur LinkedIn, une personne peut valoriser des compétences, des diplômes et des expériences de travail. Sur Instagram, elle peut montrer son travail personnel. Sur Twitter ou Facebook, elle peut se démarquer par des posts publics, reflets de ses motivations et de sa personnalité.

Les médias sociaux peuvent donner aux postulants ce petit plus par rapport à leurs concurrents armés de leurs seuls CV et lettres de motivation. En effet, les recruteurs écument eux-mêmes la toile à la recherche d'informations intéressantes sur les candidats.

En tant que candidat, vous avez le devoir de transmettre à votre employeur potentiel tous les renseignements dont il a besoin pour prendre une décision quant à votre candidature. Si les informations ne sont pas pertinentes pour le poste, elles peuvent rester privées.

Les employeurs veulent connaître un maximum d'informations. Ils font une recherche sur le candidat et jettent un œil à son profil. Le postulant apparaît régulièrement sur des photos où l'alcool coule à flots ? Il aime des publications douteuses? Lorsque le profil est public, il est difficile de démentir les faits.

Les employeurs ne peuvent créer un dossier, en ligne ou sur papier, avec les données trouvées. S'ils souhaitent le faire, ils doivent pouvoir prouver que cela est nécessaire et pertinent et en avoir averti le candidat.

Certains employeurs résolvent ce problème en mentionnant dans l'offre d'emploi que des recherches sont effectuées sur les candidats. Il est cependant strictement interdit de conserver des informations 'sensibles' comme l'origine ethnique, l'orientation sexuelle ou encore les convictions religieuses ou politiques.

Parfois, certains employeurs potentiels envoient une demande d'ajout à une liste d'amis à un candidat afin d'avoir accès à son profil. Ceci n'est pas acceptable mais le candidat n'ose pas toujours refuser, par peur de compromettre ses chances. Dans ce cas, une solution consiste à accepter la demande, mais à renforcer les paramètres de confidentialité pour cet 'ami'.

CHECK-LIST
POSTULER À L'ÈRE NUMÉRIQUE

- Passez vos posts sur les médias sociaux au peigne fin afin de supprimer tout contenu éventuellement 'compromettant'.
- Renforcez vos paramètres de confidentialité pour que seuls vos 'amis' aient accès à vos posts.
- Tapez votre nom dans les principaux moteurs de recherche pour voir ce qui apparaît à votre sujet.
- Vos écarts de jeunesse ont laissé des traces en ligne ? Vous avez le droit de demander d'effacer ces informations. Découvrez comment faire à la page 19.

POUVEZ-VOUS CONSULTER LES MÉDIAS SOCIAUX AU TRAVAIL ?

Les employeurs ne sont pas systématiquement opposés à l'utilisation des médias sociaux sur le lieu de travail. De nombreuses entreprises sont actives sur LinkedIn, Facebook ou Twitter et encouragent leurs collaborateurs à partager des nouvelles ou des offres d'emploi sur leurs propres réseaux sociaux, en tant qu'**ambassadeurs de l'entreprise**.

Par contre, ils veulent éviter de perdre du temps de travail ou d'endommager le réseau informatique de l'entreprise avec des virus importés par des internautes imprudents. Prendre un selfie au bureau ou se connecter aux médias sociaux avant une réunion avec un client potentiel peut également comporter un risque pour la sécurité de l'entreprise.

C'est pourquoi la plupart des entreprises ont établi leurs propres règles sur l'utilisation des médias en ligne dans le **règlement de travail** ou disposent d'une **politique Internet** distincte régissant les comportements de navigation autorisés (ou non). L'employeur a le droit de **fixer des limites** à l'utilisation privée des moyens de télécommunication qu'il met à disposition. Il peut ainsi limiter l'usage privé des e-mails ou d'Internet et ne l'autoriser que pendant la

pause de midi, ou exclure certains sites Web. Il peut aussi l'interdire totalement.

L'employeur a également un **droit de contrôle**. Lorsqu'il suspecte un abus de la part d'un employé, il doit suivre une procédure stricte afin de le démontrer. Si un conflit est porté devant le tribunal, celui-ci regardera, entre autres, s'il existe une politique définissant l'usage d'Internet, si celle-ci a été clairement communiquée, quel a été le comportement de navigation du salarié (ou ex-salarié), et comment l'employeur l'a découvert.

COMMENT UN EMPLOYEUR PEUT-IL CONTRÔLER LES MOYENS DE COMMUNICATION EN LIGNE SUR LE LIEU DE TRAVAIL ?

Un employeur peut vérifier si les collaborateurs ne consultent pas (trop) Internet et leur adresse e-mail à des fins privées ou s'ils vont sur Facebook pendant les heures de travail. Il existe toutefois des **règles strictes** sur la façon dont il peut exercer cette surveillance, afin de garantir un équilibre entre son droit au contrôle et la vie privée du salarié.

Les motifs de contrôle sont divers : éviter une faute professionnelle, préserver les intérêts de l'entreprise, garantir le bon fonctionnement des systèmes informatiques ou vérifier le respect du code de conduite en ligne. Ces contrôles doivent avoir un objectif concret et porter le moins possible atteinte à la vie privée.

L'employeur **ne peut surveiller en permanence les activités en ligne des salariés**. Les contrôles doivent être annoncés. Si un employeur souhaite démontrer un abus individuel, il doit d'abord effectuer un contrôle général et rechercher des anomalies, comme une haute consommation de données mobiles inexplicable. S'il remarque des éléments suspects, il doit d'abord informer les salariés du résultat de ce contrôle. Si, après un nouveau contrôle, il constate des problèmes et a des motifs raisonnables de suspecter un abus, l'employeur peut contrôler les données d'un salarié en particulier.

POUVEZ-VOUS CRITIQUER UN EMPLOYEUR SUR LES MÉDIAS SOCIAUX ?

Un employeur a droit à la **loyauté, au respect et à la discrétion de la part de ses salariés**. En tant que salarié, vous ne pouvez aucunement mettre en danger l'entreprise ou lui nuire par vos actes. Un employeur doit avoir la garantie que vous ne diffuserez pas d'informations confidentielles ou préjudiciables.

Les employeurs doivent, **dans une certaine mesure, pouvoir accepter la critique**. Néanmoins, les employés n'en ont pas pour autant tous les droits, et certainement pas celui de vider leur sac sur un forum public, ce qui peut entraîner des conséquences extrêmement préjudiciables. Régulièrement, des ex-salariés comparaissent devant le tribunal du travail afin de contester leur licenciement suite à un dérapage numérique.

> *Un cadre dans une entreprise notée en bourse a posté à plusieurs reprises des remarques au sujet de son employeur et ce peu, après la publication de (mauvais) résultats semestriels, accompagnés de commentaires. Lorsque le directeur des ressources humaines s'en est aperçu, le cadre en question a été mis à la porte. Devant le tribunal du travail, il a ensuite invoqué son droit à la vie privée, mais cet argument a été balayé. Le juge a tenu compte du caractère public des posts et du moment où ceux-ci ont été publiés, du fait que l'entreprise était notée en bourse et du poste de cadre de l'employé.*

Si vous postez un contenu critique envers votre employeur à l'attention d'un collègue ou d'un supérieur, ou si vous vous faites porter malade pour une petite escapade et postez ensuite des photos de votre excursion sur un réseau social, vous n'êtes jamais sûr que cela ne sera pas signalé. Lorsque des posts entraînent le licenciement, dans bien des cas, **ce sont des collègues et des amis en ligne qui ont dénoncé la personne**.

Une assistante de cuisine a été licenciée pour faute grave après avoir insulté un agent de maintenance. Devant le tribunal du travail, elle a fait valoir que le post ne pouvait pas être utilisé comme preuve car une de ses collègues avec laquelle elle était 'amie' sur Facebook avait transmis le message à leur employeur. Le tribunal a cependant estimé qu'il s'agissait de propos 'publics'.

De sévères critiques envers l'employeur ou l'expression d'opinions extrémistes peuvent être un motif de licenciement pour faute grave. Si vous contestez votre licenciement, le juge peut estimer que les déclarations sur les médias sociaux constituent une faute professionnelle parce qu'elles **nuisent à l'image de l'entreprise, vont à l'encontre de ses valeurs ou peuvent offenser des collègues ou clients**.

Le comptable d'une organisation liégeoise pour l'insertion sociale a posté des liens vers des vidéos du comédien français Dieudonné, condamné en Belgique pour négationnisme. Son employeur lui avait déjà demandé de ne plus recommencer et il s'y était engagé par écrit. Lorsqu'il a recommencé à 'aimer' des messages xénophobes, il a été mis à la porte. Le comptable a alors invoqué sa liberté d'opinion. La cour du travail a confirmé le licenciement, car, selon le juge, l'image de l'ASBL avait été entachée.

En règle générale : **plus le contenu est public, moins vous pouvez invoquer votre droit à la vie privée**. Un tribunal peut aussi prendre d'autres éléments en considération : si vous avez déjà émis la critique en interne sans avoir été entendu, comment celle-ci a été formulée (par exemple au moyen d'injures personnelles), si vous exercez une fonction de cadre et donc un rôle de modèle, ou encore si vous comptez de nombreux collègues ou clients parmi vos amis en ligne.

Aujourd'hui, les réseaux sociaux se sont déjà largement popularisés. Pour la plupart, nous savons qu'il vaut mieux y être prudents. Et pourtant, on ne le rappellera jamais assez : la notion de « privé » n'existe pas sur les médias sociaux. Certes, vous pouvez configurer

vos paramètres de confidentialité pour que seuls vos amis en ligne puissent voir vos publications. Mais vous ne pouvez jamais être certain que votre post ne sera pas diffusé au-delà de vos intentions. Si vous souhaitez éviter que vos collègues ou votre employeur aient vent de quelque chose, mieux vaut ne pas le mettre en ligne.

QUE POUVEZ-VOUS FAIRE CONTRE LES PROPOS HAINEUX EN LIGNE ?

La liberté d'expression est un droit fondamental mais ce droit n'est pas souverain. Les propos incitant à la haine ou propageant ou défendant la haine sont punissables. Il n'est pas toujours facile de fixer une frontière entre liberté d'expression et messages de haine. Car les avis critiques, inquiétants, choquants et même offensants doivent pouvoir être exprimés.

Vous êtes passible de sanctions si vous incitez à la discrimination, à la haine, à la violence ou à la ségrégation envers des tiers dans l'espace public, délibérément et avec un objectif précis, si vous diffusez des idées de haine ou de supériorité raciales, si vous niez le génocide perpétré par le régime nazi, si vous exprimez par écrit des insultes racistes – y compris sur Internet. La Belgique dispose également d'une loi antisexisme qui punit les gestes ou les actes par lesquels une personne est méprisée en public sur la base de son genre.

Vous pouvez :

- **Demander au gestionnaire ou au modérateur de la page de supprimer le message.**
- **Signaler les posts haineux ou discriminatoires à Facebook ou Twitter.** Ces derniers peuvent les supprimer quand un utilisateur les signale. Ils pourront décider de mettre ces messages hors ligne voire de bloquer temporairement ou définitivement le profil.
- **Réagir vous-même.** Vous pouvez entamer le dialogue avec l'auteur du post, de façon correcte et polie, contester les mensonges preuves à appui, exprimer votre mécontentement ou votre indignation, ou poster des messages positifs pour contrebalancer cette opinion.

Plus d'informations sur les moyens de réagir aux messages de haine :
www.unia.be/fr/domaines-daction/internet/que-faire-face-a-des-messages-de-haine-sur-les-reseaux-sociaux

L'EMPLOYEUR PEUT-IL CONSULTER LES E-MAILS DE SES SALARIÉS ?

Les règles relatives aux autres données en ligne sont également valables pour les e-mails. Si **la politique de l'entreprise** stipule qu'il est interdit d'utiliser votre boîte mail au travail à des fins privées et que vous outrepassez cette règle, vous êtes en tort. L'employeur a **donc le droit de surveiller les e-mails à des fins professionnelles**.

Un employeur **ne peut pas consulter le contenu d'une boîte mail personnelle**. Il peut cependant jeter un œil aux boîtes mail non personnalisées comme info@, liées à une fonction. En cas de maladie, l'employeur doit pouvoir vérifier si votre boîte mail contient des documents ou messages à traiter.

Mais qu'en est-il des boîtes mail professionnelles pouvant aussi – dans une certaine mesure – être utilisées pour envoyer des messages privés ? L'employeur n'a alors pas de sauf-conduit pour contrôler en continu et sans réserve les e-mails de ses collaborateurs, même si, dans ce cas, la balance penche plutôt en sa faveur qu'en celle des employés.

C'est pourquoi l'Autorité de la protection des données conseille d'utiliser une **double boîte mail** : une pour les messages professionnels, l'autre pour la communication privée. Certains employeurs demandent à leurs collaborateurs de **conserver les e-mails privés dans un dossier distinct** s'ils n'ont pas de boîtes mail séparées. La plupart des gens possèdent aujourd'hui un **smartphone** grâce auquel ils peuvent consulter leurs messages privés sur leur propre appareil.

4. SANTÉ

Les applications en ligne ont fait souffler un vent de révolution dans le secteur des soins de santé. Les plateformes en ligne entre professionnels de la santé permettent un meilleur suivi des patients. Grâce aux applis mobiles médicales, les patients atteints d'arythmie cardiaque par exemple ne doivent plus filer aux urgences à chaque malaise et les diabétiques peuvent mesurer leur taux de sucre via un capteur dans leur smartphone. Les applis 'lifestyle' aident à mieux dormir ou à bouger plus. Il faut toutefois rester vigilant pour éviter que nos données sanitaires ne tombent entre de mauvaises mains.

DONNÉES MÉDICALES = DONNÉES SENSIBLES

Le partage de vos données médicales via des plateformes en ligne permet aux prestataires de soins d'avoir directement un aperçu de votre état de santé. Ils savent ainsi pour quelles maladies vous êtes soigné, quels examens ont été réalisés et quels médicaments vous prenez. Un outil bien pratique pour les généralistes de garde ou un service d'urgence.

Néanmoins, vos données médicales sont des données très sensibles. Leur enregistrement et utilisation sont soumis à des règles strictes. Vous devez donner votre autorisation avant que celles-ci ne soient collectées, enregistrées, ou partagées. Leur partage doit être hautement sécurisé.

GÉRER VOS DONNÉES MÉDICALES EN LIGNE

Les autorités fédérales garantissent la sécurité de vos données médicales en ligne. Grâce à elles, seules certaines personnes peuvent demander et obtenir l'accès à vos informations médicales et ces renseignements ne sont lisibles que par les personnes autorisées.

En tant que patient, vous devez donner votre **consentement éclairé** pour le partage de vos données médicales en ligne. Pour ce faire, vous pouvez passer par votre généraliste, votre pharmacien ou votre hôpital. Vous pouvez également vous en charger vous-même en ligne via le site Web **www.masante.belgique.be**.

Vous pouvez **retirer** ce consentement **à tout moment**. Vous pouvez ajouter certains médecins à la liste des professionnels autorisés à accéder à vos données médicales. Vous pouvez aussi retirer cette permission pour un médecin spécifique, après une expérience désagréable par exemple.

Vous pouvez retrouver vos données médicales sur **www.masante.belgique.be** et les consulter. Vous pouvez gérer vos relations avec vos différents médecins traitants et refuser que certains accèdent à des documents spécifiques. Vous pouvez également demander qui a consulté vos données.

Les autorités fédérales soutiennent des **plateformes régionales de professionnels de la santé ou du bien-être de première ligne** : Vitalink (Flandre), BruSafe (Bruxelles) et Intermed (Wallonie). Ils enregistrent des données médicales, mais seuls les prestataires de soins dotés de votre autorisation ont accès à ces informations.

Pour de plus amples informations à ce sujet vous pouvez contacter votre mutuelle.

POUVEZ-VOUS UTILISER DES APPLIS DE SANTÉ EN TOUTE SÉCURITÉ ?

APPLIS MÉDICALES

Imaginez que vous souffrez d'arythmie cardiaque. Chaque malaise peut constituer un signal d'alarme. Vous aimeriez obtenir une réponse rapide : est-ce ou non une fausse alerte ? Jusqu'il y a peu, une petite visite aux urgences était le moyen le plus rapide d'obtenir ce verdict. Désormais, il existe une application médicale : vous touchez du doigt votre smartphone, et celle-ci mesure votre rythme cardiaque, détecte si tout est normal, et envoie ces données à votre médecin traitant. Celui-ci peut alors réagir, si nécessaire.

Ces applis peuvent radicalement changer la vie d'un patient. Elles peuvent rendre les traitements plus ciblés et plus efficaces. Grâce à ces applis, les médecins peuvent suivre étroitement l'état de leurs patients, à distance, et intervenir plus vite quand c'est nécessaire, afin de diminuer les éventuelles conséquences. Finies les consultations superflues, le patient gagne en tranquillité d'esprit.

Un modèle d'évaluation est en cours d'élaboration par les autorités fédérales. Celui-ci devra déterminer si certaines applis entrent en ligne de compte pour l'avis/la prescription d'un conseiller médical, et s'ils entrent en ligne de compte pour le remboursement par les autorités, via la mutualité – toujours dans le cadre d'un traitement médical plus vaste. Ces applis devront entre autres démontrer qu'elles sont sécurisées, protègent strictement la vie privée du patient et apportent une plus-value en matière de santé.

APPLIS 'LIFESTYLE'

Les magasins d'applis regorgent d'applications 'lifestyle' qui promettent d'améliorer votre forme mentale et physique. Beaucoup sont pratiques et utiles. Elles peuvent vous encourager à faire du sport, perdre du poids, améliorer votre sommeil ou vous rappeler

de prendre vos médicaments à temps.

Ces applis collectent également des données très personnelles : votre rythme cardiaque, votre pression sanguine, vos mouvements, votre poids, vos habitudes alimentaires et votre localisation. Des données sensibles particulièrement protégées par la loi sur la vie privée et confiées, parfois sans grande réflexion, aux coachs de santé numériques.

Ces coachs numériques poursuivent des objectifs commerciaux. Ils ne sont pas soumis au secret médical. Leurs pratiques ne reposent pas toujours sur des fondements scientifiques ou médicaux. Des enquêtes ont démontré que de nombreuses applis de santé ne traitent pas les données de leurs utilisateurs de façon sécurisée et se jouent parfois de la vie privée. Les données sont alors transmises à des tiers, sans que l'utilisateur en soit averti.

Ces applis 'lifestyle' ne sont pour ainsi dire soumises à aucun contrôle. C'est donc à vous d'être vigilant. Si vous les utilisez et voulez éviter que vos données ne terminent entre les mains d'un assureur ou d'un producteur de produits amincissants, mieux vaut prendre quelques mesures de précaution.

CHECK-LIST APPLIS
page 15

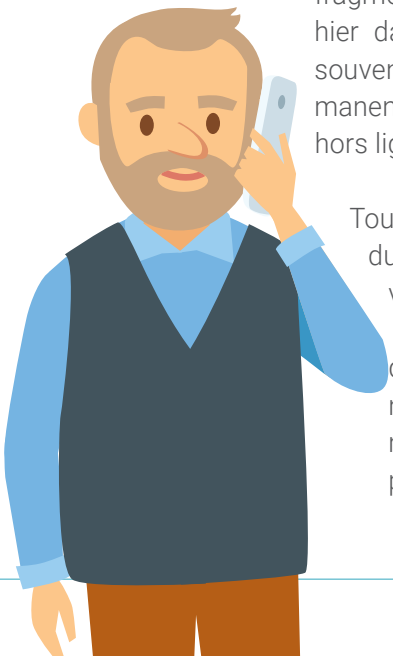
5. APRÈS VOTRE DÉCÈS

Nous avons tous une importante vie en ligne. Des dizaines de mots de passe de comptes, profils sur différents médias sociaux et adresses e-mail. Notre profil sur les médias sociaux reflète notre vie, renferme nos souvenirs et les récits de notre vie quotidienne.

Qu'advient-il de cette vie numérique lorsque l'on rend son dernier soupir ? De plus en plus souvent, nous ne pensons plus seulement à l'avenir de notre argent et de nos biens ou à nos volontés pour notre enterrement mais aussi au traitement postérieur de toutes ces traces numériques, qui représentent une bonne partie de notre vie.

HÉRITAGE NUMÉRIQUE : QUELLES TRACES LAISSEZ-VOUS ?

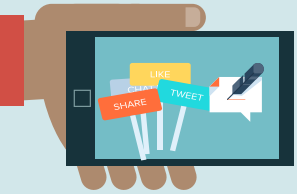
Journaux intimes, lettres, albums photo, carnets d'adresses, collections de livres, de disques ou de CD, extraits de compte… Tous ces fragments de notre vie, que nous conservions hier dans notre maison, trouvent aujourd'hui souvent leur place en ligne. Nous créons en permanence des données numériques, en ligne et hors ligne, sur notre ordinateur.



Toutes ces données constituent votre produit numérique personnel (PNP). Lorsque vous décédez, elles deviennent votre héritage numérique. Différents types de droits peuvent s'appliquer à ce produit numérique personnel : droits extrapatrimoniaux, droits patrimoniaux, droits de la personnalité, droits d'auteur.

VOTRE PRODUIT NUMÉRIQUE PERSONNEL EST COMPOSÉ DE CINQ TYPES DE DONNÉES :

1. **Les documents que vous avez créés hors ligne, sur votre ordinateur (portable).**



2. **Le contenu en ligne et sur les médias sociaux, que vous avez créé vous-même**, y compris les données sur le Cloud; vos droits de nom de domaine et vos contrats avec des entreprises publicitaires si vous tenez un blog ; votre musique; vos présentations; vos vidéos; blogs; microblogs; ou encore vos contributions à un wiki (une application web où la création, la modification et l'illustration se fait en collaboration, comme wikipedia).

3. **La communication**, par exemple votre e-mail avec carnet d'adresses et liste de contacts en ligne ; votre téléphonie par Internet avec carnet d'adresses et liste de contacts en ligne; ou vos chats avec liste de contacts.

4. **Votre activité commerciale et vos transactions électroniques, comme vos e-finances** : l'e-banking ; les e-assurances ; les e-paiements avec vos décomptes et avoirs ou les factures de votre fournisseur télécom ou fournisseur d'électricité ; les actions ou dossiers-titres exclusivement consultables en ligne ; les moyens de paiement existant uniquement en ligne comme les bitcoins ; les services en ligne du gouvernement comme Tax-on-Web ; le shopping en ligne par exemple ; les réservations en ligne de voyages et de transport, souvent liées à un système de fidélité.

5. **La lecture en ligne** via des e-books; **les jeux en ligne** impliquant la constitution (parfois indirecte) d'un patrimoine virtuel ; des sites de paris en ligne ou applications de poker sur lesquels vous possédez des avoirs ; de **la musique en ligne** ; ou des films ou programmes TV téléchargés légalement.

*La réalisation d'une **empreinte numérique** – un aperçu de toutes vos traces numériques – peut s'avérer pratique. Il ne faut alors pas oublier de la mettre à jour de temps en temps.*

QU'ADVIENT-IL DES DONNÉES DE CET HÉRITAGE NUMÉRIQUE APRÈS VOTRE DÉCÈS ?

Si vous n'avez pris aucune disposition et n'avez pas réalisé d'empreinte numérique, vos héritiers peuvent avoir du mal à rassembler les différents éléments de cet héritage numérique et tous vos comptes. Ils ne savent pas quels comptes en ligne vous utilisiez, ou n'en connaissent pas le mot de passe. Dans ce cas, ces données peuvent soit continuer simplement d'exister, soit être supprimées par les fournisseurs de ces services en ligne après une période d'inactivité.

QU'ADVIENT-IL DE VOTRE COMPTE SUR LES MÉDIAS SOCIAUX APRÈS VOTRE DÉCÈS ? PEUT-IL RESTER OUVERT ?

De nombreux fournisseurs de services – mais pas tous – ferment un compte dès qu'ils apprennent le décès de son propriétaire, ou suppriment les comptes après une période d'inactivité. Si tel n'est pas le cas, et si vous n'avez pas laissé d'instructions, vous continuez à vivre comme « **zombie numérique** », et recevez des vœux d'anniversaire et demandes 'outre-tombe'.

Certaines entreprises possèdent un '**mécanisme de clôture et de gestion**' : vous pouvez choisir vous-même la façon dont votre compte devra être géré après votre décès.

FACEBOOK

Sur Facebook, vos héritiers et vous avez **trois possibilités** :

- Vos héritiers peuvent faire **supprimer** le compte Facebook. Ils doivent alors prouver qu'ils font partie de votre famille proche. Ils doivent fournir une copie du certificat de décès. Facebook supprime le compte, avec toutes les photos et les posts.
- Vos héritiers peuvent transformer votre profil en un **compte de commémoration**. Celui-ci est alors précédé de la mention « en souvenir de ». Votre compte est conservé tel que vous l'avez laissé. N'importe qui peut demander ce statut de commémoration, mais cette personne doit fournir votre nom, date de décès, et une

mention en ligne de votre décès. Personne ne peut apporter de modifications à un profil doté d'un statut de commémoration.

- Vous pouvez désigner vous-même un **contact légataire** via vos paramètres de sécurité. Après votre décès, cette personne pourra accéder à votre compte. Il ou elle pourra alors réagir à des messages, par exemple, ou modifier votre photo de profil. La page devient ainsi un lieu de rassemblement pour la famille et les amis pour raviver des souvenirs, et commémorer votre vie. Votre contact légataire doit avoir plus de 18 ans pour pouvoir gérer votre compte et avoir lui-même un compte Facebook. Cette personne de contact peut également enregistrer des données, comme des photos et des vidéos, sur un support externe. Il n'a cependant pas accès à vos messages privés.

Vous trouverez de plus amples informations sur le contact légataire sur les Pages d'aide de Facebook.

GOOGLE

Google (Gmail et Google+, Blogger.com, Google Photos) dispose depuis longtemps déjà du Gestionnaire de compte inactif. Grâce à ces préférences relatives à l'inactivité, vous décidez vous-même de ce qu'il adviendra de votre compte Google après votre décès. Vous pouvez indiquer à partir de quand Google doit considérer votre compte comme inactif, et ce qu'il doit faire de vos données. Vous pouvez partager votre compte avec une personne de confiance qui pourra se charger de la clôture (par exemple télécharger certaines données comme des e-mails ou des photos) ou demander à Google de supprimer votre compte.

Si vous n'avez pris aucune disposition avant votre décès, vos héritiers peuvent également prendre contact avec Google. Ils doivent alors prouver que vous êtes décédé et qu'ils sont membres de votre famille et jouissent d'un droit acquis sur votre héritage.

Plus d'informations sur la page Informations personnelles et confidentialité de Google.

TWITTER

Lorsque Twitter est informé du décès d'un utilisateur (avec mention du nom et des coordonnées de contact du requérant, ainsi que son lien de parenté avec le défunt, le pseudo Twitter du défunt, et un avis officiel de décès), il ferme le compte et/ou permet à la famille de télécharger les tweets publics.

YAHOO

Yahoo (y compris Flickr et Tumblr) protège strictement la vie privée de ses utilisateurs, même lorsqu'ils ne sont plus. Votre compte n'est pas transmissible et tous les droits sur votre Yahoo ID ou le contenu de votre compte expirent après votre décès. Dès que Yahoo reçoit une copie du certificat de décès, le compte et son contenu sont supprimés.

Pour plus d'informations, consultez les conditions générales de Yahoo.

LA VIE PRIVÉE S'ARRÊTE-T-ELLE APRÈS VOTRE DÉCÈS ?

Les *droits de la personnalité* (le droit à la vie privée, le secret de la correspondance, le droit à l'image, le droit à l'honneur et à la bonne réputation) ne sont, en principe, plus valables après votre décès. Vos héritiers ont donc le droit de lire vos e-mails ou autres correspondances numériques, tout comme ils peuvent lire vos lettres ou vos journaux intimes – même si vous y êtes opposé.

Toutefois, les fournisseurs tiennent également compte du respect de la vie privée des tiers. Il peut s'agir, par exemple, des personnes qui ont envoyé ou reçu un e-mail. Dans ce cas, quelle est la priorité ? Le droit de vos héritiers à lire vos e-mails ou le respect de la vie privée de l'expéditeur ?

C'est pourquoi plusieurs fournisseurs de services en ligne désactivent votre compte automatiquement après une période d'inactivité. D'autres désactivent votre compte ou le font passer en mode commémoration dès qu'ils apprennent votre décès. Vous pouvez opter pour ces fournisseurs si vous souhaitez éviter que vos héritiers ne lisent vos e-mails. Vous pouvez également désigner une personne de confiance comme exécuteur testamentaire. Cette personne peut alors trier ou supprimer vos e-mails.

POUVEZ-VOUS INCLURE VOTRE COLLECTION MUSICALE SUR LE CLOUD DANS UN TESTAMENT ?

Cela dépend du propriétaire des données ou du compte, soit la personne qui en a le contrôle. Tout comme pour l'héritage classique, vous ne pouvez léguer votre collection musicale ou les archives de votre blog que si vous êtes vous-même le propriétaire ou le détenteur de cet héritage numérique.

Dans le cas de software as a service (software qui est offert comme service en ligne, comme la biblio-

thèque musicale de iTunes) vous disposez d'un droit d'usage, pas d'un droit de propriété. Les conditions générales des blogs, bibliothèques numériques et collections musicales indiquent la plupart du temps qu'il s'agit d'un droit d'usage personnel, exclusif, temporaire, et non transmissible. Vous ne pouvez donc pas transmettre des collections en ligne. Par contre, vous pouvez demander un aperçu ou une copie de la liste des titres musicaux ou des livres achetés. Cela peut avoir une valeur émotionnelle pour un proche.

L'accès à un compte est personnel et non transmissible. Peut-être envisagez-vous de communiquer vos mots de passe à vos héritiers pour que ceux-ci puissent profiter de votre bibliothèque musicale personnelle. Dans ce cas, ceux-ci enfreignent les conditions d'utilisation.

POUVEZ-VOUS UTILISER UN TESTAMENT POUR VOTRE HÉRITAGE NUMÉRIQUE ?

Les **initiatives commerciales** relatives à l'héritage numérique poussent comme des champignons. Elles ont un point commun : vous devez désigner une personne de confiance pour accomplir vos dernières volontés, les faire respecter.

L'avantage de ces initiatives, c'est qu'elles offrent un forum permettant de clôturer en même temps toutes vos identités et vos comptes numériques. Après votre décès, les personnes de confiance que vous avez désignées reçoivent un aperçu de vos dernières volontés concernant votre héritage numérique, et les codes d'accès nécessaires pour s'en occuper.

Vous pouvez aussi régler la gestion de cet héritage numérique, comme le reste de votre patrimoine, dans un **testament**. Un notaire pourra vous conseiller à ce sujet. Vous pouvez désigner un 'exécuteur testamentaire' qui gèrera vos données numériques après votre décès. Il pourra par exemple supprimer des documents de votre ordinateur ou assurer la postérité de certaines données en ligne, qui sont

normalement automatiquement désactivées après un certain laps de temps.

Vous lui léguez alors un document avec tous les mots de passe et vos comptes numériques, pour qu'il puisse s'occuper de votre héritage. Vous pouvez aussi le désigner comme exécuteur testamentaire numérique sur vos différents comptes en ligne. Dans certains cas, cela n'est même pas nécessaire. Facebook, par exemple, accepte que l'exécuteur testamentaire puisse être le contact légataire, sans qu'il ne doive suivre toute la procédure *(voir plus haut)*.

QUI PEUT ÊTRE EXÉCUTEUR TESTAMENTAIRE ?

L'exécuteur testamentaire numérique doit d'abord être une personne en qui vous avez confiance. En effet, celui-ci devra souvent traiter ou détruire des documents confidentiels. Parfois, il doit répartir des documents personnels et photos de comptes numériques, ou encore des messages et des codes d'accès entre les héritiers. Bien entendu, veillez à choisir une personne qui s'y connait dans le domaine numérique.

Même si vous avez déjà tout répertorié, et désigné l'exécuteur testamentaire, il se peut que celui-ci se voie refuser l'accès aux comptes. En effet, la plupart des conditions générales indiquent que l'accès au compte est strictement personnel. Le fournisseur peut alors détruire les données ou fournir certaines informations (par exemple le dernier e-mail, blog ou post) et puis décider s'il les détruit ou les conserve.

Nous tenons à remercier Hans Graux, Elke Boudry, Eva Lievens, Isabelle Marchand, Nele Broothaerts, Rika Ponnet, Elisabeth Adriaens et Yung Shin Van Der Sype pour leurs conseils avisés et leur relecture attentive. Merci aussi à tous ceux et celles qui ont accepté de répondre à nos questions ou nous ont aidés dans la recherche d'informations.

SOURCES

Sociale media. Actuele juridische aspecten. Peggy Valcke, Pieter Jan Valgaeren en Eva Lievens (eds.). Intersentia, 2013.

Privacywetgeving in de praktijk. Hans Graux en Jos Dumortier. UGA, 2009.

Privacy binnen de gezondheidssector: knelpunten door de ontwikkeling van nieuwe technologieën zoals mobile health. Sarah Gilson. Masterproef Faculteit Rechtsgeleerdheid Universiteit Gent, 2016-2017.

Sociale media tijdens en na de arbeidsrelatie: bespreking en rechtsvergelijkend onderzoek. Elisabeth Standaert. Masterproef Faculteit Rechtsgeleerdheid Universiteit Gent, 2015-2016.

Cette publication a été fabriquée à faibles émissions, de la mise en page et le tirage jusqu'à la finition et le transport. Imprimée sur papier récyclé non couché Circle Premium White Offset 100% FSC®. La production de Circle Premium White Offset 100% FSC® est basée sur la notion du recyclage avancé, limitant l'impact sur l'environnement et en soutenant une croissance verte et durable

NOTES

COLOPHON

INTERNET & MOI

PROTECTION, LIMITES, OPPORTUNITÉS

Deze publicatie is ook beschikbaar in het Nederlands, met als titel: Mijn leven online. Mogelijkheden en valkuilen

Une co-édition de la Fondation Roi Baudouin, rue Brederode, 21 à 1000 Bruxelles et de la Fédération du Notariat, rue de la Montagne, 30-32 à 1000 Bruxelles

Auteur
Isa Van Dorsselaer. Relecture: Virginie De Potter

Traduction
Home Office

Coordination pour la Fondation Roi Baudouin
Dominique Allard & Brigitte Duvieusart

Coordination pour la Fédération du Notariat
Bart Azare & Sandra Ichertz

Concept graphique
Welcome Back Victoria, victoria.be

Cette publication peut être consultée et téléchargée gratuitement sur le site de la Fondation Roi Baudouin: www.kbs-frb.be et sur celui de la Fédération du Notariat: www.notaire.be.

Dépôt légal D/2848/2018/22
Numéro de commande 3605
Septembre 2018

Fondation
Roi Baudouin

Agir ensemble pour une société meilleure

Fondation Roi Baudouin
Rue de Brederode 21
1000 Bruxelles
info@kbs-frb.be
02-500 4 555

NOTAIRE.BE

Fédération du Notariat (Fednot)
Rue de la Montagne 30-32
1000 Bruxelles
fednot@fednot.be
02-505 08 11