# À partir de quel âge peut-on laisser les ados s’inscrire sur les réseaux sociaux ?


À partir de quel âge peut-on laisser les ados s’inscrire sur les réseaux sociaux ?

**Les réseaux sociaux seront-ils bientôt interdits aux moins de 16 ans ? La nouvelle législation européenne sur la protection des données, approuvée le 17 décembre, entend relever l'âge minimum pour pouvoir s'inscrire sans consentement parental.**

**Bruxelles prévoit d'interdire l'accès aux réseaux sociaux aux adolescents de moins de 16 ans, qu'en est-il exactement ?**

Pour le moment, il s'agit d'un accord de principe qui devra être soumis au vote du Parlement européen en 2016. Rien n'est donc fait. Cette disposition, ajoutée à la dernière minute au texte sur la protection des données personnelles, fixe à 16 ans l'âge minimum pour s'inscrire sur les réseaux en ligne. Mais chaque État peut ensuite déterminer ses propres limites entre 13 ans et 16 ans.

La règle n'est pas très contraignante, mais c'est tout de même un progrès puisque, à ce jour, aucune loi française ne fixe l'âge d'utilisation pour les mineurs. Actuellement, nous appliquons le droit américain avec la loi COPPA (Children's Online Privacy Protection Act) qui interdit aux sites de recueillir des données d'enfants de moins de 13 ans, sans consentement parental. Si outre-Atlantique, celle-ci est très contraignante, ce n'est pas le cas en France. Les jeunes peuvent s'inscrire en mentant sur leur âge sans conséquences.

**À partir de quel âge peut-on les laisser s'inscrire ?**

En dessous de 13 ans, ce n'est pas souhaitable car les enfants ne font pas la différence entre vie publique et vie privée. À partir de 13 ou 14 ans, en revanche, ils commencent à acquérir un esprit critique qui leur permet de prendre un peu de recul. Mais la question n'est pas tant l'âge auquel il faut les laisser s'inscrire sur les réseaux sociaux que celui auquel on leur donne un smartphone. Ces petits joujoux sont des réseaux sociaux à eux tout seuls, avec les SMS. Ils donnent en outre accès à tous les sites Internet. Or, la plupart des parents ne pensent pas à installer un contrôle parental.

Il faut donc retarder le plus possible l'acquisition du smartphone, à la fois pour protéger l'enfant des contenus inappropriés et pour qu'il comprenne qu'on peut s'en passer. Un tiers des élèves de CM1-CM2 que je rencontre lors de mes interventions dans les établissements scolaires possède un smartphone. Difficile dans ces conditions de ne pas devenir dépendant.

**Smartphone ou ordinateur, comment accompagner les adolescents sur les réseaux sociaux ?**

Il faut commencer par installer un contrôle parental, quel que soit le terminal. Les parents doivent ensuite expliquer à l'adolescent la stratégie de ces sites Internet qui revendent les données personnelles à des fins publicitaires. Les contenus sont gratuits, mais l'utilisateur devient en quelque sorte un produit commercial. Une fois cette dimension abordée, il faut l'accompagner dans la phase d'inscription en regardant avec lui les différents paramètres du site. Ainsi, il est primordial de limiter l'accès aux publications aux seuls amis, de même qu'il ne faut pas accepter d'inconnus ou de simples connaissances dans son réseau. Il est également essentiel de rappeler à l'adolescent qu'une fois en ligne, les contenus ne peuvent plus être supprimés, ou alors au prix de démarches complexes sans aucune garantie, puisque n'importe qui peut en faire une copie.

Certains réseaux sociaux sont un peu plus encadrés que d'autres. C'est le cas de Facebook, Instagram et WhatsAPP (qui appartiennent au premier) ainsi que Twitter. En revanche, je déconseille fortement Snapchat. Cette application, qui permet d'échanger des photos de manière instantanée et soi-disant éphémère, est beaucoup plus incontrôlable. Quel que soit le site ou l'application, les parents doivent toujours accompagner les adolescents et, a fortiori, les enfants dans l'univers numérique… comme ils le ferraient dans la rue ou sur la route.

---

Réagissez à cet article

Source : *À partir de quel âge peut-on laisser les ados s'inscrire sur les réseaux sociaux ? | La-Croix.com – Actualité*

---

# Apple contre le projet de loi britannique sur le renseignement !


# Apple contre le projet de loi britannique sur le renseignement !

**Le monde semble actuellement « en guerre » contre les projets de loi sur le renseignement qui fleurissent un peu partout dans les pays développés. Et nombreux sont ceux qui prennent part à ces actions. Apple, par exemple, a clairement affiché ses objections face au projet de loi britannique.**

Le monde semble actuellement « en guerre » contre les projets de loi sur le renseignement qui fleurissent un peu partout dans les pays développés. Et nombreux sont ceux qui prennent part à ces actions. Apple, par exemple, a clairement affiché ses objections face au projet de loi britannique.

Pour la firme de Cupertino, affaiblir les techniques de chiffrement, comme le souhaite le gouvernement britannique, reviendrait à diminuer la sécurité des « données personnelles de millions de citoyens respectueux des lois« . La création d'une porte dérobée présente, elle, un risque majeur : « une clef laissée sous le paillasson ne serait pas là uniquement pour les gentils. Les méchants sauraient la trouver également. » Voici en substance les points qu'Apple a voulu souligner à la commission en charge de ce projet de loi.

Autre point sensible : la modification du fonctionnement de iMessage pour pouvoir être écouté « placerait une entreprise comme Apple, dont la relation avec les clients est en partie construite sur un esprit de confiance quant à la confidentialité des données, dans une position très difficile« .

La commission saura-t-elle prendre en compte ce genre de considérations ? À suivre !

---

Réagissez à cet article

Source : *Apple contre le projet de loi britannique sur le renseignement !*

# Arnaques et usurpation de vos données personnelles sur internet au Burkina Faso


Arnaques et usurpation de vos données personnelles sur internet au Burkina Faso

**Face à la multiplication des plaintes pour piratage de comptes mails, usurpation d'identités sur les réseaux sociaux, Facebook notamment, suivi d'arnaques ou de chantage, enregistrées par la Commission de l'Informatique et des Libertés (CIL), il me plaît de rappeler quelques bonnes pratiques à adopter pour éviter de tomber dans le piège des cyberdélinquants.**

**Ainsi, il convient de prendre les précautions suivantes :**

• Ne pas répondre à un courrier électronique (mail) ou à un message dans lequel votre mot de passe, votre adresse mail, votre numéro de compte bancaire, etc. sont demandés pour quelque raison que ce soit ;

• Eviter de saisir ou communiquer ses informations personnelles confidentielles (mot de passe, coordonnées financières…) sur un ordinateur dont on n'a pas l'assurance qu'il est sécurisé ;

• Eviter d'accepter les invitations d'inconnus sur les réseaux sociaux, Facebook notamment ;

• Eviter d'échanger des contenus inappropriés (photos, vidéos intimes) sur les réseaux sociaux en général et sur Facebook en particulier ;

• Eviter de se connecter aux réseaux internet public (wifi ouvert, des aéroports, des salles de conférences…) ;

• Utiliser un logiciel anti-virus, activer le pare-feu pour un minimum de protection de vos ordinateurs personnels, veiller à leurs mises à jour.

La protection de vos données personnelles, notre préoccupation.
**LA PRESIDENTE**

---

Réagissez à cet article

Source : *Arnaques et usurpation de vos données personnelles sur internet : conseils (…) – leFaso.net, l'actualité au Burkina Faso*

# Vous avez eu un drone en cadeau à Noël, voici vos nouveaux droits, devoirs et obligations

| | |
|---|---|
|  | Vous avez eu un drone en cadeau à Noël, voici vos nouveaux droits, devoirs et obligations |

**Le 23 décembre, la DGAC (Direction Générale de l'Aviation Civile) a mis en ligne les évolutions réglementaires en matière de drones, aéromodèles, etc. Elles se veulent plus lisibles et mieux adaptées aux besoins.**

Si le Père Noël vous apporte un drone, voici quelque chose qui devrait vous intéresser : ce que vous avez le droit de faire ou non avec, les règles à respecter, etc.

Tout d'abord, sachez que deux textes datant du 17 décembre 2015 définissent désormais la réglementation pour l'usage de drones. Il s'agit d'un arrêté relatif à la conception, aux conditions d'utilisation et aux qualifications des télépilotes et d'un autre arrêté relatif aux conditions d'insertion dans l'espace aérien.
Comme le rappelle la DGAC, les deux textes font la distinction entre les différents pilotes : professionnels ou non. Par exemple, « lorsque cette utilisation est limitée au loisir et à la compétition, on parle d'aéromodèles ». Ce sont les drones achetés dans les grandes surfaces ou des boutiques high-tech. D'autre part, on évoque les drones réservés à une utilisation professionnelle.

**Règles basiques**
Si l'espace aérien est libre en-dessous de 150 mètres, il faut toutefois respecter certaines consignes basiques :
• Voler en dehors des agglomérations et des rassemblements de personnes ou d'animaux ;
• Voler en dehors des zones proches des aérodromes ;
• Et voler en dehors d'espaces aériens spécifiquement réglementés qui figurent sur les cartes aéronautiques.
• Il est également interdit de survoler des villes ou des rassemblements de personnes sans autorisation préfectorale.
• Dans tous les cas, le « télépilote d'un drone est responsable des dommages causés par l'évolution de l'aéronef ou les objets qui s'en détachent aux personnes et aux biens de la surface (article L.61613-2 du code des transports) ».

**Protection de la vie privée**
Le texte compte tout un tas d'autres interdits. Notamment, les personnes sourdes ne peuvent pas piloter d'aéromodèles puisqu'un pilote doit toujours être en mesure de détecter visuellement et auditivement les autres drones. Il est aussi interdit de voler la nuit, ou de piloter un drone depuis une voiture.

La DGAC rappelle aussi que la « prise de vue aérienne est réglementée par l'article D133-10 du code de l'aviation civile », afin de veiller à la protection de la vie privée. Une amende de 45 000 euros et d'un an d'emprisonnement est prévue s'il y une volonté manifeste de porter atteinte à l'intimité de la vie privée d'autrui.

---

Réagissez à cet article

Source : *Un drone à Noël ? Voici vos nouveaux droits et devoirs*

---

# Comment effacer ses données personnelles sur les moteurs de recherche ?


Comment effacer ses données personnelles sur les moteurs de recherche ?

**Lorsque vous êtes sur Internet, vous êtes suivi à la trace et vos données sont transformées en outil marketing. Il faut donc penser à supprimer les données personnelles et privées, indiquées sur les moteurs de recherche pour préserver un sa vie privée.**


Suite à l'arrêt de la Cour de Justice de l'Union Européenne (CJUE) en date du 13 mai 2014, vous disposez de deux moyens pour supprimer les informations vous concernant sur Internet.

**Déposez une requête auprès du site d'origine**
Il est possible de contacter directement le responsable du site d'origine en vous référant directement aux conditions générales du portail ou aux mentions légales. Si vous ne parvenez pas à avoir ces informations, utilisez sans tarder la base de données publique « whois ». Lorsque vous avez en main les coordonnées recherchées, il vous suffit d'adresser un courrier exposant votre souhait et l'impact de la publication de vos données personnelles sur votre vie privée.
Le site dispose d'un délai de deux mois pour vous répondre. S'il refuse ou s'il ne répond pas, vous pouvez envoyer une plainte à la CNIL avec une copie de la missive expédiée au responsable du site et sa réponse.
Même si vous avez réussi à supprimer vos données personnelles sur un site, les résultats des moteurs de recherche peuvent également conserver des traces de celles-ci durant une certaine période. Il s'agit de « caches », c'est-à-dire des copies des pages visitées par les robots d'indexations des moteurs de recherche.
Si vous tombez encore sur vos données après que le contenu jugé litigieux ait été retiré par le responsable du site d'origine, pas de raison de paniquer ! Cela vient du fait que ces robots ne parcourent les sites que toutes les deux à trois semaines environ. D'ailleurs, Google et Bing proposent des procédures pour faire disparaitre définitivement ces caches. Il suffit de suivre les procédures indiquées pour faire disparaître ces données personnelles des résultats de recherche.

**Adressez-vous directement au moteur de recherche**
En parallèle, il est possible pour un internaute de demander au moteur de recherche un déréférencement d'une page qui porte atteinte à sa vie privée ou à son e-réputation. Pour le cas de Google, il suffit de remplir un formulaire afin de solliciter que le géant américain supprime les résultats de recherche qui se rapportent à vos données. Il en est de même pour Bing, le moteur de recherche de Microsoft. Comme pour le cas précédent, vous pouvez saisir la CNIL en l'absence de réponse ou si vous n'êtes pas satisfait de la réponse apportée.
Bien qu'il soit possible d'effacer les données personnelles publiées en ligne, mieux vaut rester prudent et réfléchir à deux fois avant de vous identifier sur un site ou de divulguer des informations privées.

Réagissez à cet article

Source : *Comment effacer ses données personnelles sur les moteurs de recherche ?*

---

# Un décret autorise les captations de données et de conversations Skype en temps réel


Un décret autorise les captations de données et de conversations Skype en temps réel

**Dans le calme d'un dimanche précédent le début des vacances de Noël, le gouvernement a publié au Journal officiel un décret autorisant les forces de l'ordre à surveiller toutes les informations apparaissant sur l'ordinateur d'un suspect (de ses conversations Skype à ses sites consultés), dans le cadre de procédures judiciaires.**
Permettre à des enquêteurs de capter en temps réel (et à distance) les données informatiques de suspects, c'est possible. Depuis le vote de la LOPPSI de 2011, l'article 706-102-1 du Code de procédure pénale autorise en effet les officiers et agents de police judiciaire à accéder et enregistrer des données « telles qu'elles s'affichent sur un écran » ou telles que l'utilisateur d'un ordinateur « les y introduit par saisie de caractères » – et ce à partir du moment où un juge d'instruction a émis une ordonnance motivée en ce sens, prise après avis du Procureur de la République.
Cette procédure, activable uniquement pour des crimes et délits relativement graves (terrorisme, association de malfaiteurs, meurtre, crime de fausse monnaie, escroquerie ou prêt illicite de main d'œuvre en bande organisée, etc.), a même été élargie suite à l'adoption de la loi anti-terroriste de novembre 2014 aux données « reçues et émises par des périphériques audiovisuels ». L'objectif ? Pouvoir capter aussi les sons, comme ceux d'une conversation Skype par exemple.

**Captation de tout ce qui apparaît à l'écran, les conversations Skype, etc.**
Avec ce décret entré en vigueur ce lundi 21 décembre 2015, le gouvernement vient de permettre l'application de ces dispositions en autorisant la création de traitements de données à caractère personnel, destinés à recevoir les fameuses informations extirpées par les forces de l'ordre dans ce type de procédures. « Les traitements autorisés par le présent décret permettent de collecter, enregistrer et conserver les données informatiques ainsi captées et de les mettre à la disposition des enquêteurs de la police et de la gendarmerie nationales comme de la douane judiciaire », précise le texte.
Les opérations, bien que placées sous le contrôle du juge, permettront aux services de se pencher sur « l'ensemble des données captées », y compris s'il s'agit de données personnelles sensibles. Toutes les informations enregistrées devront être « conservées dans le traitement jusqu'à la date de clôture des investigations ». À ce moment, poursuit le décret, elles seront « placées sous scellés fermés et effacées ». Une transcription des enregistrements effectuée par les forces de l'ordre devra néanmoins être transmise à l'autorité judiciaire, pour être versée au dossier de la procédure – en vue d'un éventuel procès.
En donnant son avis sur ce qui n'était alors qu'un projet de décret, la Commission nationale de l'informatique et des libertés (CNIL) prévenait l'exécutif que l'utilisation de tels dispositifs de surveillance risquait de conduire à la collecte de « données relatives à d'autres personnes que l'utilisateur [suspecté], telles que, par exemple, l'identité des personnes en relation avec l'utilisateur du système d'information surveillé ».

La gardienne des données personnelles affirmait par ailleurs que le gouvernement ne faisait pas explicitement référence à la mise en œuvre de dispositifs de reconnaissance vocale ni d'analyse comportementale des dynamiques de frappe au clavier (keylogging). « Si de tels mécanismes devaient à l'avenir être mis en œuvre, la commission devra être saisie pour avis sur un projet de décret modificatif prévoyant expressément le recours à de tels dispositifs » mettait-elle en garde.

**Un dispositif qui n'était pas encore totalement opérationnel en avril dernier**
Tout en regrettant « de ne pas avoir été destinataire de l'ensemble du dossier technique (…), certains éléments n'ayant été communiqués qu'à l'Agence nationale de la sécurité des systèmes d'information (ANSSI) », la CNIL soutenait qu'au moment de rédiger son avis, le dispositif prévu par le ministère de l'Intérieur « ne permet[tait] pas encore la captation de données émises ou reçues par des périphériques audiovisuels ». La délibération de l'autorité administrative indépendante date toutefois du 2 avril 2015, ce qui signifie que les choses ont pu grandement évoluer depuis…
La CNIL ajoutait néanmoins qu'elle prenait acte « que lorsqu'un nouveau dispositif aura été développé dans cette perspective, des informations complémentaires ser[aient] portées à sa connaissance ». Nous n'avons cependant pas réussi à joindre l'institution afin de savoir si elle avait depuis obtenu de nouveaux éléments.

Sur un plan technique, la CNIL expliquait qu'au regard des éléments à sa disposition, « la solution retenue pourra s'adapter à l'environnement applicatif des utilisateurs visés par une enquête (système d'exploitation, applications tierces, etc.). Des tests de fonctionnement seront exécutés afin de s'assurer de la correcte adaptation de l'outil à l'environnement de chaque utilisateur. Une procédure de suppression automatique de l'outil sur les terminaux informatiques visés est prévue. L'architecture de collecte sera en outre pourvue de mesures visant à assurer la sécurité et le cloisonnement des données collectées. »
Rappelons enfin que la récente loi sur le renseignement permet à de nombreux services d'utiliser des dispositifs intrusifs à l'insu des personnes surveillées (à l'image des ISMI catcher), sans toutefois qu'un juge soit cette fois mis dans la boucle…

---

Réagissez à cet article

Source : *Un décret autorise les captations de données et de conversations Skype en temps réel*

---

# Les entreprises doivent

# prendre au sérieux la protection des données


## Les entreprises doivent prendre au sérieux la protection des données

---

**L'intelligence économique est devenue un mode de gestion (Le management est la mise en ?uvre des moyens humains et matériels d'une entreprise pour (…)) et de gouvernance de l'entreprise. Cet ouvrage réfléchit sur la démarche que le chef d'entreprise peut entreprendre pour éclairer ses décisions, garder sa marge de manoeuvre de compétitivité et toutes ses possibilités de développement afin de sécuriser sa pérennité.**

**Traitement de l'information et renseignements**

Un renseignement utile peut être obtenu de façon proactive, active, ou réactive.

Le cycle de renseignement pour l'entreprise doit s'intégrer au processus de veille stratégique sur les différents volets de l'intelligence économique : veille technologique, veille d'image, veille concurrentielle, etc.

L'intelligence économique distingue trois niveaux d'information utile au renseignement :

image: http://www.atlantico.fr/sites/atlantico.fr/files/u65387/2015/12/capture_2_0.jpg

L'intelligence économique ne cherche pas à obtenir l'information noire. Elle se limite à l'information que l'on peut obtenir par des moyens légaux (ex : pour se protéger des problèmes de réputation, d'escroquerie, de fraude, de cybercriminalité, de propriété intellectuelle, de savoir-faire, de brevets, etc.).

Il s'agit surtout de formaliser de façon pragmatique, ou de rendre systématique, une démarche proactive de veille dans ce domaine, notamment pour l'obtention de l'information « grise ».

Les PME sont souvent très en retrait sur la construction du savoir (ex : suivi des avancées des concurrents, organisation de la veille juridique, réglementaire, lobbying, etc.).

Sécurité et protection de l'information

Trop peu d'entreprises prennent au sérieux la protection des données. Il devient impératif de disposer d'un solide processus de sauvegarde, de prévention, d'action, et de réaction aux pannes et aux attaques informatiques. Notons ici que certaines entreprises sensibles aux problématiques de reprise après incident commencent à considérer les prestations d'externalisation applicatives (Cloud computing ou autres solutions) pour optimiser le niveau de sécurité des données.

Quantité et gouvernance des données

Les données sont la base de l'information, et comme le disent souvent les anglo-saxons: « data is the oil of the 21st century ». Savoir chercher et collecter l'information, la traiter et la diffuser (tout en protégeant la part de données sensibles qui doivent être protégées), constitue une tâche prioritaire de tous les acteurs économiques, et la définition même de l'intelligence économique.

image: http://www.atlantico.fr/sites/atlantico.fr/files/u65387/2015/12/capture_3_0.jpg

Le pouvoir c'est l'information, mais à condition qu'elle soit de qualité …

La direction et les organes sociaux doivent s'appuyer sur des informations de qualité (fiables, précises, actualisées)

Read more at http://www.atlantico.fr/decryptage/entreprises-doivent-prendre-au-serieux-protection-donnees-gouvernance-et-intelligence-economique-en-pme-georges-nurdin-daniel-2494228.html##Vrl3qqLdiB14upbK.99

---

Réagissez à cet article

Source : *Marketing/ Les entreprises doivent prendre au sérieux la protection des données*

---

# Les principales mesures du nouveau règlement européen

# sur la protection des données


## Les principales mesures du nouveau règlement européen sur la protection des données

**L'UE a approuvé le 15 décembre au soir le règlement sur la protection des données, qui renforce considérablement les pouvoirs de sanction des Cnil nationales.**
La Commission européenne, le Parlement européen et le Conseil européen, qui travaillent depuis cet été à la constitution d'un compromis, se sont entendus le 15 décembre au soir sur un règlement européen sur la protection des données, qui harmonise des législations nationales très variées (voire inexistantes) pour donner aux citoyens un meilleur contrôle sur la façon dont leurs données sont collectées et utilisées. Comme tout règlement, celui-ci n'aura pas besoin d'être transposé en droit national et s'appliquera directement à partir du début 2017.

**Parmi les principales mesures approuvées, on trouve :**
Un important pouvoir de sanction accordé aux différentes « Cnil » nationales, qui pourront infliger des amendes allant jusqu'à 4% du chiffre d'affaires mondial (jusqu'à un certain plafond) des entreprises qui utilisent à mauvais escient les données numériques des gens, notamment en y accédant sans leur consentement. Autrement dit, des amendes pouvant atteindre plusieurs millions d'euros qui devraient a minima constituer une bonne dissuasion. Toutefois, pour ne pas empêcher les entreprises de tirer profit du big data, elles pourront traiter librement les données une fois effacée l'identité précise des utilisateurs.
L'obligation, pour les entreprises victimes de fuite de données, de signaler leur cas aux régulateurs nationaux sous trois jours, sous peine là encore de fortes amendes.
Le droit à l'oubli, entériné par le règlement, qui permet aux citoyens européens de demander à supprimer des informations en ligne qui les concernent mais ne sont plus pertinentes.
La portabilité des données, qui permet aux utilisateurs de demander le transfert de leurs données d'une plateforme vers une autre.
L'obligation, pour les moins de 16 ans, de demander une autorisation parentale avant de pouvoir utiliser des services tels que Facebook, Snapchat ou Instagram. Bruxelles proposait 13 ans comme aux Etats-Unis, mais certains pays dont la France ont poussé pour relever cette majorité numérique. Chaque Etat membre est toutefois libre d'y déroger.

L'extension de ces nouvelles règles à toutes les sociétés qui comptent des utilisateurs dans l'Union européenne, même si elles sont basées hors de l'UE. Dans la Silicon Valley par exemple.
Autrement dit, le règlement se fait beaucoup plus protecteur des citoyens européens que la législation équivalente aux Etats-Unis, mais également bien plus sévère à l'égard des sociétés qui y contreviendraient.
Naturellement, les géants américains ont protesté en accusant l'Union de les cibler injustement, au détriment de leurs petits rivaux européens. Ils estiment en particulier que lier les sanctions au chiffre d'affaires mondial n'a pas de sens. Mais l'UE, qui a toujours rejeté ces accusations, est restée ferme. Les grandes plateformes US ont donc sans doute du souci à se faire, à l'instar d'un Facebook qui a déjà eu maille à partir avec les régulateurs nationaux en France, en Espagne, en Allemagne, aux Pays-Bas et encore récemment en Belgique.

---

Réagissez à cet article

Source : *Les principales mesures du nouveau règlement européen sur la protection des données | CHABERT CATHERINE*

# La SNCF va épier ses voyageurs


## La SNCF va épier ses voyageurs

**Plutôt que de surveiller ses millions de passagers de la même façon, la SNCF va tenter de les filtrer au moyen d'un logiciel qui prétend isoler les comportements présentant un risque.**

Face à la menace terroriste, la SNCF teste la réponse technologique. Dans quelques gares, la compagnie ferroviaire s'est déjà équipée d'un logiciel d'analyse du comportement des voyageurs au travers des caméras de vidéosurveillance existantes. À défaut de filtrer tous les passagers avec des portiques de sécurité tels que proposés par la ministre de l'Écologie, la société publique va essayer de détecter les attitudes suspectes.

Stéphane Volant, le secrétaire général de l'entreprise publique, a expliqué dans les grandes lignes à l'AFP le fonctionnement de ce logiciel, dont l'analyse se base sur « le changement de température corporelle, le haussement de la voix ou le caractère saccadé de gestes qui peuvent montrer une certaine anxiété ». Une vidéosurveillance qui se veut donc intelligente, mais qui risque de générer énormément de faux positifs.

## Vers un nouveau cap dans la surveillance

Avec cette expérimentation – qui s'étendra aux colis abandonnés -, la SNCF veut aussi mesurer le niveau d'acceptabilité des voyageurs pour ce genre de technologie. Mais au quotidien, personne ne verrait jamais ces logiciels, puisque les caméras elles-mêmes ne différeront pas. Le seul changement perceptible pour le public sera peut-être le nombre d'interpellations préventives de gens à l'attitude jugée suspecte…

## Vidéosurveillance gare

Alors que ces tests auraient vocation à durer et que ce logiciel – dont le nom n'a pas été révélé – pourrait être étendu aux 40 000 caméras de la SNCF, se pose la question de la protection de la vie privée. Sur ce point, la compagnie ferroviaire a déjà répondu que ces expérimentations sont menées sous le contrôle de la Cnil.

Dans sa boîte à outils sécuritaire, la société lancera au printemps prochain une application mobile pour les voyageurs afin qu'ils signalent un danger. La SNCF imagine aussi équiper ses agents de caméras. Quant aux portiques, ils seront adoptés pour l'accès aux trains Thalys, en réponse à l'attentat déjoué au mois d'août. Gageons que les trains qui arrivent en retard ne génèrent pas trop de hausse de température corporelle.

---

Réagissez à cet article

Source : *Surveillance : la SNCF va épier ses voyageurs*

---

# Données personnelles – L'Union européenne tient son règlement


Données personnelles – L'Union européenne tient son règlement

---

**Il aura fallu 3 ans de discussions et même si quelques détails restent à formaliser, tout le monde est d'accord sur le Règlement européen sur les données personnelles.**

Il aura fallu 3 ans de discussions et même si quelques détails restent à formaliser, tout le monde est d'accord sur le Règlement européen sur les données personnelles. Le Parlement, le Conseil et la Commission ont mis fin à leurs discussions en « trilogue », étape habituelle de construction d'un cadre législatif à l'échelle européenne. Ce texte très attendu entrera en vigueur au 1er janvier 2018. Il remplacera enfin la réglementation obsolète et disparate qui régit actuellement la vie privée des consommateurs de 28 pays européens. En voici les principales mesures.

**Données personnelles – : L'Union européenne tient son règlement**

L'Europe va enfin disposer d'un cadre réglementaire adapté à l'ère du numérique pour les données personnelles de ses citoyens. En clôturant leurs discussions, le 15 décembre, le Parlement, le Conseil et la Commission ont validé un texte dont les prémisses remontent à 2012. Finalement, leur version varie d'ailleurs assez peu de celle adoptée par le Parlement européen il y a 2 ans. Le nouveau règlement européen renforce la protection de la vie privée, ce dont L'UFC-Que Choisir se réjouit.

Les nouvelles règles, qui s'appliqueront au 1er janvier 2018, permettront à chacun de mieux maîtriser ses données personnelles. Concrètement, elles contraindront les sites Internet à informer très clairement les consommateurs sur la collecte et le traitement de leurs données, ce qu'ils devront expressément accepter. Le nouveau règlement définit par ailleurs un droit à la portabilité des données : il sera plus facile de transférer les données personnelles d'un prestataire de services à un autre. Par exemple, si vous passez d'Outlook à Gmail, vous pourrez rapatrier simplement vos messages, vos contacts et tous vos fichiers stockés dans le cloud. Pratique.

Précisons que sur ces deux points, le texte européen va plus loin que la loi (française) pour une République numérique, qui sera débattue au Parlement début 2016.

**Du droit à l'oubli au droit au déréférencement**

Autre mesure importante, le renforcement du droit à l'oubli numérique : si vous le demandez, et si aucun motif légitime ne s'y oppose, Google ne pourra plus indexer dans son moteur de recherche les pages Internet qui vous concernent. Petite subtilité : cela ne contraint pas les sites Internet à supprimer ces pages, c'est pourquoi il est plus juste de parler d'un « droit au déréférencement ». Cette mesure entérine une récente décision de la CJUE (Cour de justice de l'Union européenne), qui avait fait jurisprudence en la matière (lire aussi notre enquête Droit à l'oubli : Google seul juge).

Le Règlement européen valide une autre décision récente de la CJUE, qui a fait beaucoup de bruit au mois d'octobre dernier en invalidant l'accord du Safe Harbor. C'est désormais acté, les entreprises établies hors d'Europe devront se conformer à la réglementation européenne pour pouvoir offrir leurs services dans l'Union : Facebook ne pourra plus se cacher derrière ses bureaux américains pour exploiter comme bon lui semble les données de ses abonnés français ou italiens. Toute comme lui, les autres géants du Net devront en outre héberger en Europe les données des consommateurs européens.

Gare aux entreprises, européennes ou pas, qui manqueraient à leurs nouvelles obligations : le règlement prévoit des sanctions financières importantes (les montants exacts devront attendre le texte définitif, mais selon toute vraisemblance elles pourront atteindre 200 000 000 € ou 4 % du chiffre d'affaires mondial annuel d'une entreprise).

Le texte définitif doit encore être formellement adopté par le Parlement européen et le Conseil début 2016.

---

Réagissez à cet article

Source : *Données personnelles – L’Union européenne tient son règlement – UFC Que Choisir*