La carte d’identité biométrique ne protège pas les données personnelles

	La carte d’identité biométrique ne protège pas les données personnelles

Invité sur les ondes de l'émission matinale Expresso ce mardi 13 juin 2017, Chawki Gaddes, président de l'instance nationale de la protection des données personnelles Tunisienne souligne que le projet de loi relatif à la carte d'identité biométrique présente certains risques sur la vie privée et la protection des données des citoyens. Ceci est valable au niveau des contenus comme à celui des mécanismes de leur création, utilisation et gestion, particulièrement avec les nouvelles technologies d'information et de communication.

Il a aussi attiré l'attention sur le fait que la reconnaissance automatique des personnes constitue une source d'inquiétude en l'absence du cadre légal judicieux pour la protection des libertés et des droits des personnes. A ce stade il ajoute qu'il est nécessaire de prévoir la mise en place du cadre légal pour les utilisations possibles et autorisées de la carte d'identité biométrique.
Quant à l'adresse de la personne sur sa carte d'identité, Chawki Gaddes considère ceci absurde et inacceptable, vu que l'adresse n'est pas un constituant d'identité et que ça pourrait changer.
Sur la même question d'absence de cadre légal, le président de l'instance nationale de la protection des données personnelles a appelé à la nécessité de mettre en place une loi spéciale relative au système des renseignements. Ce dernier est très important, tout Etat dans le monde entier dispose d'un système de renseignement et procède aux opérations d'écoutes téléphoniques, c'est pour cela qu'il faut prévoir une loi convenable, qui permet à l'Etat de protéger la sécurité et la défense nationale…[lire la suite]

Réagissez à cet article

Source : *Chawki Gaddes : La carte d'identité biométrique ne protège pas les données personnelles*

La Police pourrait prochainement consulter vos données personnelles sur Facebook sans autorisation

	La Police pourrait prochainement consulter vos données personnelles sur Facebook sans autorisation

Face à la vague d'attentats qui frappe l'Europe, la Commission européenne discute actuellement de quelques changements dans les réglementations afin de permettre aux forces de Police d'accéder aux données des utilisateurs des services de Google et Facebook, sans autorisation préalable d'un Juge.

Les vagues d'attentat et la peur ambiante sont bien souvent l'occasion pour les gouvernements de voter des lois liberticides, et ce pourrait à nouveau être le cas dans toute l'Europe. La Commission européenne réfléchit actuellement à changer les réglementations afin de permettre aux forces de police d'aller piocher des informations dans les comptes des réseaux sociaux des utilisateurs, sans accord préalable de qui que ce soit.

Concrètement, le projet évoque même la possibilité pour les policiers d'origine étrangère de consulter les données privées des profils de ces réseaux sociaux, afin notamment d'enquêter sur un touriste ou une personne d'un autre pays de l'Union européenne. Exemple : vous partez en Italie pour quelques jours et vous faites arrêter par la police locale, ces derniers pourraient alors éplucher vos profils sociaux pour tenter d'obtenir plus d'informations sur vous, et ce, sans rien demander à la France.

Actuellement, trois projets de ce type ont été proposés et soumis à étude, l'un d'entre eux pouvant être adopté d'ici la fin de l'année 2018. Une des propositions évoque la possibilité de copier les données directement depuis le Cloud de la plateforme sociale afin d'en faire une sauvegarde et éviter la disparition des données en cas d'enquête…[lire la suite]

Commentaire de Denis JACOPINI

Entre Facebook qui analyse et espionne ses membres et les OPJ (Officiers de Police Judiciaire) qui peuvent consulter les données collectées par Facebook, il n'y a qu'un pas pour que ce même type de démarche soit aussi engagée auprès de Google pour qu'on nous mette des radars automatiques sur Internet qui nous flashent dès que quelqu'un en train picoler publie une photo.
Sans plaisanter, ces projets de loi consistent à permettre à des OPJ d'accéder aux zones privées de Facebook, car vous savez que lorsque vous publiez quelque chose sur Facebook, cet ajout peut être public (tout le monde peut le consulter et le voir) ou privé et il n'y a qu'un juge qui peut forcer Facebook à communiquer le contenu privé d'un compte. Ce projet ne changera rien pour ceux qui n'ont rien à se reprocher, et pas grand chose pour ceux qui ont quelques chose à se reprocher. Les OPJ pourrons disposer plus rapidement des contenus privés pour alimenter leurs enquêtes.
Il est fort probable à l'avenir qu'un autre réseau social soit utilisé par les malfrats l'histoire de faire courrier le chat…

Réagissez à cet article

Source : *Europe : la Police pourrait prochainement consulter vos données personnelles sur Facebook sans autorisation*

Importance de l’e-réputation pour une entreprise ou une marque

	Importance de l’e-réputation pour une entreprise ou une marque

---

Également connue sous le nom de « réputation numérique », « cyber-réputation » ou « web-réputation », l'e-réputation est la perception que les internautes se font d'une marque, d'une entreprise ou d'une personne en la recherchant sur Google.
Véritable facteur de différenciation, la notoriété numérique est un ingrédient crucial dans l'image publique qu'a une société ou une personne dans le monde réel. A l'ère du digital et des réseaux sociaux, l'e-réputation devient plus que jamais un enjeu capital.

Importance de l'e-réputation pour une entreprise ou une marque

Internet a conquis tous les secteurs et il n'existe pas une seule société qui n'ait pas de présence digitale (site web, comptes sur les réseaux sociaux, avis…). Les achats en ligne étant devenus une pratique extrêmement courante, les consommateurs ont de plus en plus tendance à vérifier l'opinion que les autres ont d'un produit avant de l'acheter. Selon une étude réalisée par l'IFOP pour Reputation VIP, sur internet, 85 % des consommateurs réalisent des achats et 80 % se renseignent avant d'acheter. Une mauvaise **réputation sur le web** peut désormais être synonyme de pertes colossales. En effet, toujours selon l'étude IFOP, 66% des consommateurs venus chercher un avis avant un achat diffèrent l'achat en cas de commentaires défavorables quand, dans 30% des cas, ils vont même jusqu'à renoncer à l'achat. Ainsi, 96% des internautes sont influencés par l'e-réputation d'une marque lors d'un achat…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *Importance de l'e-réputation pour une entreprise ou une marque*

Un fichier « Top 50 des

arrêts maladies » à La Poste découvert : La Cnil et l’Ordre des Médecins saisis par le syndicat SUD-PTT

	Un fichier « Top 50 des arrêts maladies » à La Poste découvert : La Cnil et l’Ordre des Médecins saisis par le syndicat SUD-PTT

Le syndicat SUD a saisi les autorités après qu'un document Excel répertoriant les arrêts maladies ait été découvert. Le syndicat parle d'un « Top 50 de la honte ».

C'est une histoire qui ne fait pas rire mais alors pas rire du tout les syndicats. Vendredi 2 juin, le syndicat SUD PTT a saisi la Cnil (Commission Nationale de l'Informatique et des Libertés) ainsi que le Conseil national de l'ordre des médecins après la découverte d'un fichier interne à La Poste qui dresse un Top 50 des agents ayant le plus grand nombre de jours d'arrêt maladie.

Un Top 50 qui passe mal

Le fichier, consulté par nos confrères de l'AFP, se présente sous la forme d'un tableau Excel. Dans celui-ci, on y trouve les noms et prénoms des agents des 168 agents de la plateforme logistique de Bonneuil (Val-de-Marne), leur référent, leur service ainsi que le nombre de journées d'arrêt de travail pour chacun. Cette surveillance a été démarrée lors de l'ouverture de la plateforme en janvier 2016.

Le syndicat SUD PTT juge, certes, que ce recensement est « normal, ne serait-ce que pour établir un bilan social en fin d'année ». Mais c'est lorsque l'on clique sur le dernier onglet de ce fichier Excel, un document nommé « Top 50 des arrêts maladie », que le bât blesse. Celui-ci classe de 1 à 50 et par ordre décroissant les agents qui ont le plus d'arrêts maladie (arrêts de travail, accidents du travail et maladie professionnelle confondus). Dans un communiqué, le syndicat SUD PTT le qualifie de « Top 50 de la honte ».

Dans ce classement figure même « le nom d'une personne aujourd'hui décédée », relève SUD PTT, qui s'interroge sur le « but » de ce classement et ses commanditaires, et réclame la destruction du fichier. « Face à ce fichier proprement scandaleux qui stigmatise une bonne partie du personnel », le syndicat a saisi la Commission Nationale de l'Informatique et des Libertés (Cnil), l'Inspection du travail et le Conseil de l'ordre national des médecins.

LIRE AUSSI

…[lire la suite]

Réagissez à cet article

Source : *Un « Top 50 des arrêts maladies » à La Poste : le syndicat SUD-PTT saisit la Cnil et l'Ordre des Médecins – LCI*

Bordeaux : des drones pour mettre des amendes sur les routes

Bordeaux : des drones pour mettre des amendes sur les routes

Comment les drones vont changer nos vies Progressivement, les avions sans pilote se déploient dans de multiples secteurs d'activité, mais le marché, prometteur, peine encore à décoller, freiné par la législation.…[Lire la suite]

Réagissez à cet article

La Chine lance sa loi sur la cybersécurité. Les entreprises sont inquiètes

	La Chine lance sa loi sur la cybersécurité. Les entreprises sont inquiètes

La Chine applique à partir de jeudi sa loi sur la cybersécurité, renforçant encore sa « Grande muraille » informatique, mais des entreprises étrangères s'inquiètent de l'impact de la nouvelle réglementation sur leurs activités.

Cette loi adoptée en novembre dernier ambitionne de protéger les réseaux chinois et les informations personnelles des utilisateurs, à l'heure où le rançongiciel WannaCry a rappelé la vulnérabilité des Etats face aux cyberattaques.
Mais des entreprises ont réclamé au gouvernement chinois un report de l'application de la loi. Elles s'inquiètent notamment des dispositions imprécises du texte et de l'influence qu'il pourrait avoir sur l'informatique dématérialisée (le « cloud ») et le traitement des données personnelles.
Les autorités semblent toutefois vouloir finaliser les règles.
Mi-mai, le directeur de l'Administration chinoise de la cybersécurité (CAC), Zhao Zeliang, a réuni 200 représentants d'entreprises et d'associations professionnelles locales et étrangères au siège de son organisme à Pékin.
La discussion était centrée sur les règles de transfert des données personnelles à l'étranger, ont rapporté des participants à l'AFP. Selon eux, les personnes présentes ont reçu une version actualisée de dispositions de la loi, et l'assurance de M. Zhao que certains des passages les plus polémiques seraient retirés.
Le nouveau document, consulté par l'AFP, ne fait par exemple plus mention de l'obligation controversée pour les entreprises de conserver en Chine les données personnelles de leurs clients.
Mais les appréhensions demeurent.
Les autorités « ne sont pas prêtes » à faire appliquer la loi et il est « très improbable » qu'un changement concret dans la législation intervienne dès le 1er juin, a assuré à l'AFP un participant qui a requis l'anonymat en raison de la sensibilité du dossier.
La Chine surveille déjà drastiquement l'internet, en bloquant les sites qu'elle estime politiquement sensibles, un système surnommé « la Grande muraille électronique » qui n'a toutefois pas empêché des universités et stations-services du pays d'être touchées par l'attaque planétaire du virus WannaCry.
La nouvelle loi sur la cybersécurité interdit aux internautes de publier tout contenu portant atteinte à « l'honneur national », « troublant l'ordre économique et social » ou destiné à « renverser le système socialiste », c'est-à-dire le Parti communiste au pouvoir.
Des entreprises étrangères craignent que la nouvelle loi entrave leur accès au marché chinois…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *La Chine lance sa loi sur la cybersécurité, les entreprises inquiètes – Le Parisien*

Chrome Flaw Allows Sites to Secretly Record Audio/Video Without Indication

Sounds really scary! Isn't it? But this scenario is not only possible but is hell easy to accomplish.A UX design flaw in the Google's Chrome browser could allow malicious websites to record audio or video without alerting the user or giving any visual indication that the user is being spied on.

AOL developer Ran Bar-Zik reported the vulnerability to Google on April 10, 2017, but the tech giant declined to consider this vulnerability a valid security issue, which means that there is no official patch on the way.

How Browsers Works With Camera & Microphone

Before jumping onto vulnerability details, you first need to know that web browser based audio-video communication relies on WebRTC (Web Real-Time Communications) protocol – a collection of communications protocols that is being supported by most modern web browsers to enable real-time communication over peer-to-peer connections without the use of plugins.

However, to protect unauthorised streaming of audio and video without user's permission, the web browser first request users to explicitly allow websites to use WebRTC and access device camera/microphone.

Once granted, the website will have access to your camera and microphone forever until you manually revoke WebRTC permissions.

In order to prevent 'authorised' websites from secretly recording your audio or video stream, web browsers indicate their users when any audio or video is being recorded.

« Activating this API will alert the user that the audio or video from one of the devices is being captured, » Bar-Zik wrote on a Medium blog post. « This record indication is the last and the most important line of defense. »

In the case of Google Chrome, a red dot icon appears on the tab, alerting users that the audio or video streaming is live.

How Websites Can Secretly Spy On You

The researcher discovered that if any authorised website pop-ups a headless window using a JavaScript code, it can start recording audio and video secretly, without the red dot icon, giving no indications in the browser that the streaming is happening…[lire la suite]

***Notre métier** : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.*

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *Chrome Flaw Allows Sites to Secretly Record Audio/Video Without Indication*

Des drones sauveurs de vies

© AFP / Bernard Jaubert	**Des drones sauveurs de vies**

Le Programme Alimentaire Mondial, agence des nations Unies, veut utiliser les nouvelles technologies pour aider les victimes de catastrophes naturelles.

Le **Programme Alimentaire Mondial** teste le « drone humanitaire » grâce à l'aide financière du gouvernement belge (500 000 euros).
En complément des moyens déjà existants, les drones pourraientt aider les populations, notamment lors de catastrophes naturelles.
Lorsque la terre a tremblé dans les montagnes de Katmandou, au Népal il y a deux ans, les secours ont mis près d'une semaine à accéder aux zones les plus reculées à cause du manque de communications. Un temps bien trop long pour secourir les blessés.

Au lendemain du tremblement de terre au Nepal en mai 2015 © Maxppp / Sumit Shrestha
D'où l'idée de se tourner vers les drones…[lire la suite]

Réagissez à cet article

Source : *Demain, des drones sauveront des vies*

Est-ce que le vote électronique des élections Françaises est fiable ?

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	Est-ce que le vote électronique des élections Françaises est fiable ?				

Le vote électronique : nouvelle preuve de manipulation des élites qui peuvent en deux temps trois mouvements truquer les votes comme bon leur semble …

Pendant les élections Françaises, les scellés appliqués sur la machine à voter et l'expertises des systèmes de votes électroniques réalisées par les experts indépendants respectant les **recommandations de la CNIL dans délibération n° 2010-371 du 21 octobre 2010 relative à la sécurité des systèmes de vote électronique** garantit le respect de l'intégrité et de la confidentialité des scrutins.

Réagissez à cet article

A Lire aussi :

Nouveautés dans l'organisation des votes électroniques pour les élections professionnelles
3 points à retenir pour vos élections par Vote électronique
Le décret du 6 décembre 2016 qui modifie les modalités de vote électronique
Modalités de recours au vote électronique pour les Entreprises
L'Expert Informatique obligatoire pour valider les systèmes de vote électronique
Dispositif de vote électronique : que faire ?

La CNIL sanctionne un employeur pour défaut de sécurité du vote électronique pendant une élection professionnelle

Notre sélection d'articles sur le vote électronique

Vous souhaitez organiser des élections par voie électronique ? Cliquez ici pour une demande de chiffrage d'Expertise

Vos expertises seront réalisées par **Denis JACOPINI** :
• Expert en Informatique **assermenté et indépendant** ;
• **spécialisé dans la sécurité** (diplômé en cybercriminalité et certifié en Analyse de risques sur les Systèmes d'Information « ISO 27005 Risk Manager ») ;
• ayant suivi la **formation délivrée par la CNIL sur le vote électronique** ;
• qui n'a **aucun accord ni intérêt financier** avec les sociétés qui créent des solution de vote électronique ;
• et possède une expérience dans l'analyse de nombreux systèmes de vote de prestataires différents.
Denis JACOPINI ainsi **respecte l'ensemble des conditions recommandées** dans la Délibération de la CNIL n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet.
Son expérience dans l'expertise de systèmes de votes électroniques, son indépendance et sa qualification en sécurité Informatique (ISO 27005 et cybercriminalité) vous apporte l'assurance d'une qualité dans ses rapport d'expertises, d'une rigueur dans ses audits et d'une impartialité et neutralité dans ses positions vis à vis des solutions de votes électroniques.
Correspondant Informatique et Libertés jusqu'en mai 2018 et depuis Délégué à La Protection des Données, nous pouvons également vous accompagner dans vos démarches de mise en conformité avec le RGPD (Règlement Général sur la Protection des Données).

Contactez-nous

Source : *LE VOTE ELECTRONIQUE = ESCROQUERIE ! – Agoravox TV*

Que sait de nous Google grâce à nos comportements sur Internet ?

Mondialement connue, la firme américaine Google est utilisée par de nombreux internautes, pour son moteur de recherche, mais aussi pour ses nombreux services gratuits (Gmail, Drive, Youtube, Google Maps…). Seul petit hic ? Le revers de la médaille. Puisque Google exploite vos données sans que vous n'en ayez toujours conscience.

Tout le monde connaît Google pour son moteur de recherche ultra-performant. C'est d'ailleurs le moteur préféré des Français. Fin 2016, selon Netbooster, plus de 94 % d'entre eux l'ont utilisé pour effectuer leurs recherches en ligne. Pour apprécier la démesure de ce chiffre, il suffit de voir la part restante à ses principaux concurrents : moins de 4 % pour Bing (Microsoft) et à peine plus de 2 % pour Yahoo.

Plus de 200 services gratuits…

À travers sa maison mère « **Alphabet** », Google est l'une des premières capitalisations mondiales avec une valeur de 588 milliards de dollars, juste derrière Apple. La firme de Moutain View n'est pas la seule à analyser les données qui lui parviennent. Tous les géants du secteur (Apple, Amazon, Facebook…) le font en s'appuyant sur les traces que nous laissons chaque jour sur Internet. Ils engrangent des milliards de dollars grâce à ces informations personnelles.

Inutile donc d'être un financier avisé pour comprendre que la seule activité de moteur de recherche ne suffit pas à générer de telles entrées d'argent. Google est une pieuvre géante, dont les tentacules s'étendent dans des domaines aussi nombreux que variés. Le système d'exploitation Android, le navigateur Internet Chrome, les vidéos YouTube, la plateforme de téléchargement Google Play, la cartographie Google Maps, la suite bureautique Google Documents, le site de partage de photos Picasa…

Ce sont plus de 200 services proposés gratuitement par l'entreprise. Pour la plupart d'entre eux, la seule contrepartie demandée est l'ouverture d'un compte Gmail, le service de messagerie en ligne maison. L'adresse email et le mot de passe associé deviennent alors vos sésames pour vous identifier et entrer dans la sphère Google, depuis n'importe quel terminal à travers le monde.

… en échange de vos données personnelles

Toute cette gratuité a cependant une face cachée : l'exploitation commerciale de nos données personnelles. En effet, elles représentent une manne financière des plus importante. En acceptant les « **conditions générales d'utilisation** », que nous ne lisons quasiment jamais, nous donnons le droit à Google de tracer et d'utiliser tout ce que nous faisons sur Internet : les sites visités, les achats effectués, les lieux dans lesquels nous nous rendons, les films regardés, les livres lus, la musique écoutée…

L'ensemble de ces données est alors analysé par les puissants ordinateurs de la firme, dans le but créer une sorte de carte d'identité très précise de chaque utilisateur. Ces profils, compilant de très nombreuses données, se revendent à prix d'or aux marques désireuses de cibler au mieux leur publicité. C'est ce que l'on appelle le « **Big Data** ».

Pour profiter gratuitement des services de Google, comme ceux de nombreux autres acteurs des nouvelles technologies, nous devons donc rogner sur notre vie privée, en abandonnant la confidentialité de nos données personnelles. Il existe une formule qui résume parfaitement cette pratique : « **si c'est gratuit, c'est que le produit c'est vous** ! »…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *Données personnelles. Voici ce que Google sait de vous*