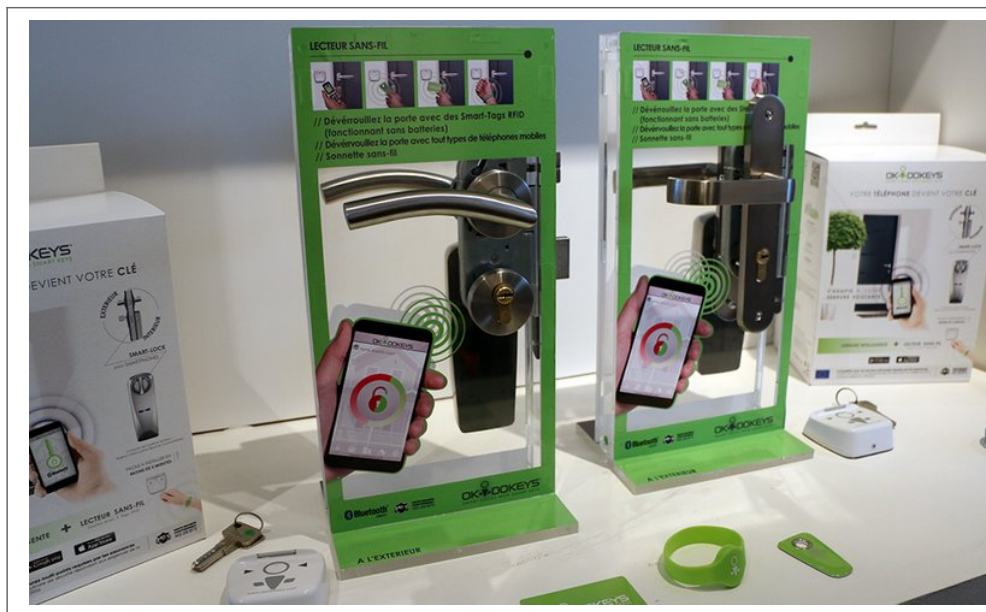


Okidokeys : la serrure connectée à la française bientôt disponible



Okidokeys
: la
serrure
connectée
à la
française
bientôt
disponible

En vente depuis 6 mois aux Etats-Unis, la serrure connectée de l'entreprise française Okidokeys s'apprête à être commercialisée en Europe. Que se cache-t-il vraiment derrière ce produit, destiné à être installé très rapidement sur n'importe quelle porte ?

Assez peu connue du grand public, l'entreprise française Okidokeys est pourtant l'une des pionnières en matière de serrure connectée. Il s'agit d'une filiale d'OpenWays, dont le cœur de métier cible, à la base, les hôtels, dont certains utilisent depuis longtemps déjà des systèmes de clés électroniques pour l'ouverture des portes des chambres. Okidokeys cible de son côté les particuliers désireux d'utiliser la ou les serrures de leur logement d'une autre manière, principalement avec un smartphone, mais pas seulement. Car la serrure connectée, si elle se présente sous une unique forme de base, peut être complétée par différents éléments qui permettent d'en renforcer l'usage. La serrure en elle-même s'installe à l'intérieur du logement, sur une serrure déjà existante. La mise en place n'est censée prendre que quelques minutes, et tout le nécessaire, jusqu'au tournevis, est inclus dans la boîte. Certains impératifs doivent être vérifiés avant l'achat : la serrure de base doit notamment disposer impérativement d'un cylindre européen pour être compatible. L'épaisseur de la porte doit également être contrôlée.



Le maître des clés

« Par rapport aux serrures américaines, qui ont souvent de simples loquets, les serrures européennes ont été un défi » explique Pascal Metivier, le PDG d'Okidokeys. « La principale difficulté a été d'adapter le mécanisme qui ouvre la porte aux serrures 3 ou 5 points. » Les assurances demandent généralement la présence d'une serrure 3 points minimum pour la couverture d'un logement. La serrure d'Okidokeys est compatible avec ce type d'installation.

Concrètement, le « robot », une fois installé, agit sur le cylindre de la porte pour l'ouvrir ou la verrouiller. Le reste est essentiellement l'affaire de la connectique Bluetooth, qui permet de connecter un smartphone pour interagir avec la serrure. Tout est chiffré en 256 bits AES, une mesure de protection très répandue et efficace, assure l'entreprise. La clé de chiffrement est différente pour chaque serrure : pas de risque de voir sa porte ouverte par un voisin qui aurait le même modèle.

Différentes clés peuvent être programmées par le biais d'une interface Web, elle aussi sécurisée. L'administrateur peut autoriser, gratuitement, jusqu'à 10 personnes à accéder à jusqu'à 5 serrures. Des plages horaires et des jours peuvent être délimités, pour, par exemple, autoriser une femme de ménage à entrer seulement à certains moments.

Différents paramètres peuvent également être réalisés par le biais de l'application mobile, disponible sur iOS et Android. On peut, par exemple, autoriser temporairement l'ouverture d'une porte quand le smartphone en est proche : pratique quand on a les bras chargés. La serrure peut également se fermer automatiquement.

Bien évidemment, tout ceci n'empêche pas d'utiliser une bonne vieille clé manuelle, qui garde la priorité sur la serrure à l'extérieur. A l'intérieur, un loquet permet de fermer la porte à la main.



RFID, NFC et CAC à la rescousse

La serrure fonctionne à l'aide de 4 piles LR6, pour une autonomie d'un an. Lorsque les piles arrivent en fin de vie, le système le fait savoir 6 semaines à l'avance, et insiste de plus en plus pour qu'on les change, jusqu'à empêcher la fermeture électronique.

Le vrai risque question autonomie concerne davantage le smartphone : si on n'a plus de batterie et pas de vraie clé sur soi, comment faire ? Okidokeys a la réponse : il s'agit d'une sonnette connectée, qui dispose de plusieurs systèmes de lecture. Outre le NFC d'un téléphone, elle peut lire des puces RFID programmées à l'avance pour l'ouverture de la porte. Ces dernières sont disponibles sous la forme de cartes à mettre dans son portefeuille, de porte-clés ou encore de bracelets étanche. Une solution de secours, mais également de nécessité si on ne dispose pas d'un smartphone. En cas de perte, ces éléments peuvent être rapidement désactivés sur le site.

La sonnette connectée intègre également le système CAC, pour « crypto acoustic credential ». Ce dispositif, utilisé dans certains hôtels, permet d'utiliser un téléphone mobile « traditionnel » pour ouvrir une porte à l'aide d'une séquence sonore sécurisée. L'utilisateur reçoit un SMS avec un code, il doit ensuite appeler un numéro vert, qui va jouer un son pour la sonnette. Cette dernière est capable de l'interpréter, de le valider et d'ouvrir la porte si tout est en règle.

Une ouverture à Internet

A ce stade, tout se passe en local. Mais Okidokeys propose également un pack incluant un module, appelé Gateway, qui se connecte à une box et relie donc la serrure à Internet. Il est ainsi possible de savoir, en temps réel sur son smartphone, si la porte a été ouverte, et par quel moyen. La serrure intègre également une alarme, qui va retentir en cas d'entrée forcée. Là encore, l'administrateur est prévenu à distance, à condition de disposer de cette extension Internet.



Okidokeys dongle

On se retrouve donc face à trois solutions : la serrure de base, celle avec la sonnette et les tags, et celle qui permet, en plus du reste, de connecter le site à Internet. Tout ceci à un prix non négligeable : le premier pack est proposé au tarif de 250 euros, le second à 350 et le troisième à 450.

La démonstration d'Okidokeys est efficace et le système est convaincant. Néanmoins, il apparaît également destiné à des personnes qui ont un besoin important d'optimiser l'accès à leur logement. Si la démarche commence à avoir du sens dans un environnement familial – où les parents donneront des bracelets RFID aux enfants, par exemple – il en a presque encore plus dans le cadre d'une location mesurée, pour les adeptes de services de type Airbnb. Ce n'est d'ailleurs pas pour rien si l'interface en ligne passe en mode payant – 35 euros par an – si l'on désire enregistrer plus de 10 utilisateurs et plus de 5 serrures.

Les trois packs seront disponibles en France à partir du mois de janvier 2015.

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire...

Source : http://www.clubic.com/mag/maison-connectee/actualite-744009-okidokeys-serrure-connectee-francaise-disponible.html?estat_svc=s%3D223023201608%26crmID%3D639453874_775958436

Twitter : les données des applications mobiles servent à mieux cibler les publicités



Twitter : les données des applications mobiles servent à mieux cibler les publicités

Technologie : Les annonceurs travaillant sur Twitter peuvent désormais exploiter les données d'utilisation des applications mobiles pour affiner leurs campagnes. Mais les usagers ont la possibilité de désactiver le suivi de leurs habitudes.

Il y a quelques semaines, Twitter annonçait qu'il allait commencer à collecter des informations sur l'usage des applications mobiles afin de rendre les contenus plus pertinents. Cela se traduit aujourd'hui par un nouvel outil mis à la disposition des publicitaires qui prend le nom de "tailored audiences" ou "public adapté". Ces derniers vont désormais pouvoir cibler leurs réclames en se basant sur les données issues des applications mobiles : fréquence d'utilisation, nombre d'installations, achats in-app, inscriptions.

Par exemple, un annonceur pourra cibler une personne ayant installé son application mais qui ne s'est pas encore enregistré ou n'a pas fait d'achat. Mais Twitter a pris soin d'offrir à ses membres la possibilité de refuser ce ciblage en désactivant la fonction depuis les paramètres de leur application Android ou iOS. (Eureka Presse)

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire...

Source :

<http://www.zdnet.fr/actualites/twitter-les-donnees-des-applications-mobiles-servent-a-mieux-cibler-les-publicites-39811067.htm>

Les ministres de l'UE reviennent sur le guichet unique pour la protection des données



Les ministres de l'UE reviennent sur le guichet unique pour la protection des données

Deux ans après la proposition de s'adresser à une unique autorité pour gérer les questions de protection de données dans l'Union européenne, les ministres de la Justice de l'UE envisagent une autre solution, impliquant plusieurs autorités. Un abandon qui contrarie la coalition ICDP où l'on retrouve Google, Facebook, Microsoft, Apple et Yahoo.

Les pays membres de l'Union européenne sont revenus la semaine dernière sur une proposition de 2012 visant à diriger les fournisseurs de technologies tels que Google, Facebook, Microsoft ou Apple vers une seule autorité habilitée à gérer les questions de protection de données en Europe. L'objectif de ce projet était d'éviter de devoir s'adresser à chaque autorité de protection de données des 28 pays membres de l'UE. La question avait été débattue par les ministres de la Justice et la proposition élaborée par la Commission européenne constituait l'un des piliers de la réforme de la protection de données dans l'UE.

Mais la semaine dernière, lors d'une nouvelle réunion des ministres de la Justice et de l'Intérieur à Bruxelles, à laquelle ont assisté Christiane Taubira, ministre de la Justice, et Bernard Cazeneuve, ministre de l'Intérieur en France, une majorité s'est dégagée pour une autre proposition, suggérée par les Italiens. Ces derniers occupent jusqu'au 31 décembre la présidence tournante du Conseil européen où se rencontrent les ministres pour coordonner les différentes politiques.

Un processus qui risque d'être très lourd, estime l'ICDP

Cette fois, la proposition suggère un mécanisme qui se déclencherait uniquement dans les cas transfrontaliers les plus importants. Celui-ci consisterait à faire coopérer les différentes autorités de protection de données concernées afin de déboucher sur une décision conjointe. Cette proposition n'emporte évidemment pas les faveurs des fournisseurs de technologie. L'ICDP, Industry Coalition for Data Protection (qui regroupe 18 associations représentant des milliers de sociétés européennes et internationales, dont Google, Facebook, Microsoft, Apple et Yahoo), a exprimé sa déception. Dans une lettre envoyée aux ministres avant leur réunion, elle estime que cela semble créer un mécanisme plus compliqué. Pour elle, cela pourrait conduire à impliquer toutes les autorités de protection de données dans la grande majorité des cas examinés. Couplé à la possibilité que chaque autorité puisse opposer son veto à une décision, cela rendrait le processus très lourd.

Même son de cloche du côté de la CCIA (Computer and Communications Industrie Association) qui représente des sociétés Internet européennes et américaines. L'un des ses porte-parole estime qu'il faut un guichet unique qui permettrait aux grandes entreprises technologiques comme aux PME de ne s'adresser qu'à un seul régulateur, quel que soit le nombre de pays dans lesquels ils interviennent. Ces dispositions seront à nouveau abordées par le Conseil européen dans les prochains mois.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire...

Source

<http://www.lemondeinformatique.fr/actualites/lire-les-ministres-de-l-ue-reviennent-sur-le-guichet-unique-pour-la-protection-des-donnees-59534.html>
par Loek Essers / IDG News Service (adapté par Maryse Gros)

La protection des données personnelles, un « droit fondamental »

1001010010000101110010101110101
DONNÉES PERSONNELLES010001010
0101100101010100010101010000110
SPAM1010101000111001011010000
110010011101010001110110101000
1**COOKIES**00101111011011011010
0000110101011110110011011000
1001101010001110110001100100
VIE PRIVÉE000001000110111
1010001010101000101011

La protection
des données
personnelles
un « droit
fondamental »

Les régulateurs européens, réunis au sein du G29, rappellent la nécessité de ne pas traiter les données personnelles comme un seul « objet de commerce ».

Les autorités européennes de régulation des données ont affirmé lundi dans une déclaration commune au ton très politique que la protection des données personnelles était un « droit fondamental » sur lequel l'Union européenne ne pouvait transiger. Un an et demi après les révélations d'Edward Snowden, les régulateurs européens réunis au sein du G29 ont rappelé lors d'un colloque la nécessité de ne pas traiter les données personnelles comme un seul « objet de commerce ».

Faisant référence au traité de libre-échange transatlantique, les « Cnil » (Commission nationale de l'informatique et des libertés, NDLR) soulignent que « le niveau européen de protection des données ne peut être érodé (...) par des accords bilatéraux ou internationaux ». Elles demandent ainsi l'application stricte des nouvelles règles de protection des données de l'Union, en cours de négociation, qui doivent être considérées « comme des principes internationaux impératifs en droit international public et privé ».

« Tous les corpus de protection des données doivent être considérés comme des lois de police », a affirmé Isabelle Falque-Pierrotin, présidente de la Cnil française, qui appelle également à la mise en place d'actions judiciaires collectives sur le modèle des class actions. Le G29 juge par ailleurs « inacceptable sur le plan éthique (...) la surveillance secrète, massive et indiscriminée de personnes en Europe ».

« Le pétrole de demain »

« La conservation, l'accès et l'utilisation de données par les autorités nationales compétentes doivent être limités à ce qui est strictement nécessaire et proportionné dans une société démocratique », soulignent les « Cnil ». Le Premier ministre Manuel Valls a promis à ce sujet qu'un projet de loi « garantira un contrôle effectif et indépendant de l'intégralité des actes dérogatoires au droit commun accomplis par les services de renseignement ». Il a appelé également à une simplification des conditions générales d'utilisation et à un droit à l'oubli renforcé pour les mineurs.

Le stockage des données personnelles collectées par des entreprises privées doit enfin, selon les régulateurs, pouvoir être contrôlé par une autorité européenne indépendante. « Les données européennes doivent être stockées en Europe », a indiqué Thierry Breton, P-DG d'Atos et ancien ministre de l'Économie. « Il est temps de protéger ces mines d'or (...), ce sera le pétrole de demain », a-t-il ajouté.

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire...

Source

http://www.lepoint.fr/societe/la-protection-des-donnees-personnelles-un-droit-fondamental-08-12-2014-1887990_23.php

The European Data Governance

Forum – CNIL

 <p>Le Net Expert INFORMATIQUE Protection des données personnelles Sécurité Informatique - Cybercriminalité</p> <p>vous informe...</p>	<h2>European Data Governance Forum – CNIL</h2>
---	--

Le G29 et la CNIL organisaient le 8 décembre une conférence internationale qui se tenait à l'UNESCO. La conférence avait pour thème : Protection des données, innovation et surveillance : quel cadre éthique pour l'Europe ?

2015 est une année charnière pour la protection de la vie privée, avec l'adoption du règlement de l'Union Européenne sur la protection des données, la poursuite des négociations commerciales internationales et les décisions finales à prendre sur la gouvernance de l'internet. Cette période est cruciale pour l'Europe qui, dans le nouvel environnement numérique, doit promouvoir haut et fort les valeurs sociétales qui sont les siennes et définir des actions prioritaires pour le futur. Une réponse d'ensemble à ces défis internationaux ne saurait être élaborée par des acteurs agissant en ordre dispersé. La complexité des problèmes posés demande une réflexion collective de la part de l'ensemble des parties prenantes.

La conférence du 8 décembre organisée par le G29 (groupe des autorités européennes de protection des données) et la CNIL était placée sous le patronage de l'UNESCO et de la Délégation permanente française auprès de l'UNESCO. Elle réunissait des représentants et experts d'horizons divers – institutions nationales, européennes et internationales, industrie, ONG et société civile – qui ont présenté leur point de vue sur les défis actuels de la surveillance numérique et sur la manière d'y répondre de manière adéquate dans une société démocratique.

La conférence s'est achevée par la présentation d'une Déclaration adoptée par le G29 qui était endossable par les parties prenantes qui le souhaitaient. Cette Déclaration soulignait la responsabilité collective de toutes les parties prenantes dans la définition et le respect d'un cadre éthique pour la collecte et l'utilisation de données personnelles dans l'économie numérique. Elle a défini les principes essentiels à inclure dans un tel cadre ainsi que les actions clés à entreprendre par toutes les parties prenantes, des secteurs public et privé, pour garantir le respect des règles.

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire...

Source : http://www.newspress.fr/Communique_FR_284395_1332.aspx

ESET s'engage auprès de Facebook pour protéger les utilisateurs des cyber-menaces

x	ESET s'engage auprès de Facebook pour protéger les utilisateurs des cyber-menaces
---	---

ESET protège tous les utilisateurs Facebook contre le piratage.

ESET rejoint l'initiative Anti-malware lancé par Facebook et offre « ESET Online Scanner » à tous les utilisateurs de Facebook. Cette solution permet d'identifier les posts provenant non pas des utilisateurs mais de logiciels malveillants. Ces posts sont alors retirés en toute sécurité. ESET Online Scanner pour Facebook est disponible depuis le 03 décembre 2014 et pour tous les utilisateurs de Facebook.

« Notre but est d'offrir à nos utilisateurs la meilleure technologie afin d'améliorer l'utilisation de nos services et de protéger au mieux leurs appareils connectés. ESET Online Scanner va de manière significative diminuer le nombre de clics sur des liens malicieux, effectués des milliards de fois chaque jour sur Facebook » explique Chetan Gowda, Web developer chez Facebook.

La version dédiée d'ESET Online Scanner pour Facebook, a été conçue pour détecter et nettoyer les ordinateurs infectés des utilisateurs de Facebook. « ESET est heureux d'offrir ses services aux utilisateurs de Facebook du monde entier. ESET est reconnu pour sa légèreté et sa qualité de détection, ces deux atouts se retrouvent dans cette version pour Facebook, gratuitement.», annonce Ignacio Sbampato, Directeur Commercial et Marketing chez ESET HQ.

Votre ordinateur a besoin d'être nettoyé
Suppression des logiciels malveillants
Un fonctionnement simple et ciblé

Lorsqu'un utilisateur se connecte à son compte, Facebook cherche des comportements malicieux – comme l'envoi de spams ou de liens infectés provenant d'amis Facebook. Si ce type d'activité est détecté, Facebook invite l'utilisateur à utiliser ESET Online Scanner. L'analyse s'effectue directement sur Facebook, gratuitement et en tâche de fond.

L'utilisation du scanner est sans impact sur le système de l'utilisateur, de sorte qu'il peut continuer à utiliser son appareil sans gêne. Une fois l'analyse terminée, l'utilisateur reçoit une notification de la part de Facebook; un compte rendu du scan est aussi disponible. Le nettoyage commence une fois l'analyse terminée si des malwares ont été détectés.


Ce service pour Facebook est basé sur une solution gratuite ESET Online Scanner protégeant des millions d'internautes. Sur plus de 44 millions de scans, ESET Online Scanner a détecté avec succès des malwares dans presque la moitié des analyses.

ESET est un outil de protection et de désinfection que je conseille personnellement. Vous avez envie de découvrir et de tester gratuitement ce logiciel de protection (ESET NOD32 ou ESET SMART SECURITY, je peux vous communiquer une licence sur simple demande.
Denis JACOPINI

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire...

Source : <https://mail.google.com/mail/u/0/?hl=fr&shva=1#inbox/14a2e1044c5865c4>

La justice européenne va encadrer la vidéosurveillance depuis le domicile – Next INpact

 <p>Le Net Expert INFORMATIQUE Protection des données personnelles Sécurité Informatique - Cybercriminalité</p> <p>vous informe...</p>	<p>La justice européenne va encadrer la vidéosurveillance depuis le domicile – Next INpact</p>
--	--

Jeudi, la Cour de Justice de l'Union dira si une caméra située dans une propriété privée qui surveille également une partie de l'espace public échappe ou non aux règles de protection en matière de traitement des données à caractère personnel.

Le déploiement des solutions de vidéosurveillance personnelles se démocratisant, une affaire tranchée demain par la Cour de Justice de l'Union européenne méritera une certaine attention. Le cas examiné est né en Tchécoslovaquie.

Un certain M. Ryněš, agacé que les vitres de sa maison soient brisées à maintes reprises avait installé un système de vidéosurveillance. Les flux étaient enregistrés sur disque dur à partir de caméras captant l'entrée de sa maison, celle de la maison d'en face, mais également une partie de la voie publique.

Une amende infligée par la CNIL tchèque

Dans la nuit du 6 au 7 octobre 2007, nouveau vandalisme à l'aide d'une fronde. Les enregistrements sont remis à la police qui parvient à identifier des suspects. Problème, l'un d'eux conteste la légalité des procédures auprès de l'Office tchèque pour la protection des données à caractère personnel. Et pour cause : ces enregistrements ont été effectués sans son consentement alors qu'il était sur la voie publique.

La CNIL locale lui donne raison et inflige une amende à M. Ryněš. Ce dernier attaque cependant cette décision devant la Cour suprême administrative tchèque, laquelle, prise d'un doute, a saisi la Cour de justice pour savoir si ces enregistrements constituaient ou non un traitement de données couvert par la directive 95/46 sur les données personnelles. Celle-ci en effet, ne s'applique pas quand le traitement est effectué par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques.

L'analyse de l'avocat général

Pour l'heure, l'avocat général a déjà conclu que le traitement de données à caractère personnel effectué par ce Tchéque ne relevait pas de la notion d' « exercice d'activités exclusivement personnelles ou domestiques », une des exceptions à la directive en question. Du coup, a contrario, ce système de vidéosurveillance devrait entrer dans le plein champ de ce texte européen.

Si la Cour suit cette analyse, cela ne signifiera pas nécessairement que l'amende infligée au responsable du traitement sera légitimée. Il faudra en effet déterminer si d'autres articles de cette directive ne peuvent être appelés en renfort pour légitimer cette installation effectuée sans le consentement des personnes filmées (article 7 f) de la directive).

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire...

Source

<http://www.nextinpact.com/news/91283-la-justice-europeenne-va-encadrer-videosurveillance-depuis-domicile.htm>

Fête des lumières 2014 de Lyon : les coulisses high-tech de la Place des Terreaux

!



Fête des lumières 2014 de Lyon : les coulisses high-tech de la Place des Terreaux !

Chaque année, la fête des Lumières revient illuminer la ville de Lyon. L'installation de la place des Terreaux est assurément l'une des plus impressionnantes de ce cru 2014. Dans la pratique, des vidéos haute résolution sont projetées sur les façades de la mairie de Lyon ainsi que sur le musée des beaux-arts (les deux bâtiments sont situés autour de la place des Terreaux).

La couverture de la mairie est assurée par 5 projecteurs professionnels Barco de 26 000 lumens d'une résolution de 1920 x 1200 pixels. Pour le musée, les techniciens ont dû utiliser 6 projecteurs du même type. Dans cette configuration, chaque projecteur recouvre une surface d'environ 35 m².

L'alimentation des projecteurs en image est assurée par des serveurs média de type Modulo Pi. Ces derniers sont taillés sur mesure pour délivrer des contenus audio et vidéo HD ou 4K sans le moindre accroc. Côté hardware, ils sont équipés d'un processeur de type Core i7 épaulé par 16 Go de RAM, et d'une carte graphique de type AMD Fire Pro W7000. Les fichiers vidéo sont stockés dans 8 SSD en Raid. Le serveur tourne sous Windows Embedded Standard 7, et exécute le programme serveur de modulo Pi. Une seule machine est capable de distribuer 4 flux vidéo non compressés (progressifs, sans codecs, suite d'images TGA) en 1920 x 1200 pixels, ou un seul flux 4K 120 hertz non compressé.

Les serveurs Modulo Pi sont tous mis en réseau de manière à assurer une diffusion audio / vidéo parfaitement synchronisée. Ils sont également capables de piloter les projecteurs, et corrigent la déformation lorsque l'image n'est pas projetée sur une surface plane. Détail intéressant : si les serveurs Modulo Pi sont pilotables depuis un ordinateur sous Windows ou Mac OSX, une nouvelle application Android (encore en version bêta) fait désormais son apparition.

En clair, il est possible de piloter l'ensemble de ces projections gigantesques depuis un « simple » téléphone portable !

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire...

Source : <http://www.clubic.com/video/reportages/video-fete-des-lumieres-2014-de-lyon-les-coulisses-high-tech-de-la-place-des-terreaux-458881.html>

La protection des données personnelles, « atout pour la France », selon Manuel Valls



La protection
des données
personnelles,
« atout pour
la France »
selon Manuel
Valls

« Je mesure l'audace d'inviter un ancien ministre de l'intérieur parler de protection des données, cela peut paraître risqué » : surprise, c'est le premier ministre, Manuel Valls, qui a prononcé le discours d'ouverture de l'« European data governance forum », organisé lundi 8 décembre à Paris.

Cette journée de conférence au siège de l'Unesco a été mise en place par le G29, qui rassemble les autorités européennes de protection des données, afin de réfléchir à un « cadre éthique et juridique » sur la question des données personnelles.

Le chef du gouvernement a souligné à plusieurs reprises le rôle que doivent jouer, selon lui, les autorités européennes et les Etats : « Il serait erroné de penser que toute régulation tue l'innovation. La régulation, c'est le rôle des Etats. Les valeurs de la démocratie doivent peser sur le monde numérique, la loi doit s'y appliquer. »

Projet de loi sur le numérique

« En 2015 et 2016, la loi réaffirmera de manière solennelle le droit à la vie privée et à la protection des données personnelles, ainsi que le contrôle des actes des services de renseignement », a expliqué le premier ministre. Sans préciser si cette question sera abordée dans le cadre du projet de loi numérique, en 2015, ou s'il fera l'objet d'un texte distinct.

Manuel Valls et Mme Falque-Pierrotin, la présidente de la CNIL, ont également rappelé que 2015 serait l'année du règlement sur les données personnelles, adopté au printemps par le parlement européen et qui doit désormais faire l'objet d'un accord entre les Etats membres. Sur ce sujet, le premier ministre a souligné « le soutien de la France à la réflexion sur le règlement sur les données », tandis que Mme Falque-Pierrotin a estimé qu'il y avait « urgence à nous doter de cet instrument juridique unique pour toute l'Union ».

Sur la question très sensible de l'inclusion – ou non – de la lucrative question des données personnelles dans les négociations sur les traités de libre-échange actuellement en négociation notamment entre l'UE et les Etats-Unis, M. Valls s'est voulu rassurant : « La France veillera, dans les négociations sur les traités de libre-échange, à ce que le standard européen soit préservé. »

« DÉFICIT DE CONFIANCE »

Le gouvernement français en est convaincu, a martelé Manuel Valls : la protection des données est un atout économique. « L'Europe doit faire de la protection des données personnelles un argument d'attractivité et de compétitivité. L'utilisateur doit pouvoir faire ses choix sur ses propres données en toute connaissance. Cela a un potentiel économique énorme. »

Un avis partagé par Mme Falque-Pierrotin : « Il ne faut pas que le déficit de confiance se transforme en méfiance » générale au sein de l'écosystème numérique. « Le monde a changé. Certains voudraient faire croire que la vieille histoire de la protection des données est dépassée », a conclu Manuel Valls. « Chaque époque a son combat : le droit des femmes, l'abolition de la peine de mort... La France y a tenu sa place. C'est parce que la France est le pays des droits de l'homme qu'elle doit faire de la protection des données un grand combat pour les droits humains. »

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire...

Source :

http://www.lemonde.fr/pixels/article/2014/12/08/la-protection-des-donnees-personnelles-atout-pour-la-france-selon-manuel-valls_4536408_4408996.html
par Martin Untersinger

L'intelligence artificielle, notre futur Terminator?



L'intelligence artificielle, notre futur Terminator?

L'intelligence artificielle pourrait menacer à terme l'humanité: il ne s'agit pas d'un film de science-fiction mais de la prédiction du célèbre physicien Stephen Hawking, qui relance le débat sur le risque de voir l'homme dépassé par les technologies qu'il a lui-même créées.

Interrogés par l'AFP, anthropologues, futurologues et experts en intelligence artificielle se montrent partagés sur les craintes d'Hawking. Les craintes d'un homme apprenti sorcier sont anciennes et elles ont nourri nombre de romans et des films comme « 2001: Odyssée de l'espace » avec son ordinateur meurtrier Hal 9000 et plus récemment « Terminator », le robot exterminateur. Mais aujourd'hui, c'est un astrophysicien très respecté, le Britannique Stephen Hawking, qui lance un pavé dans la mare. Atteint d'une dystrophie neuromusculaire, il s'exprime grâce à un ordinateur.

« Les formes primitives d'intelligence artificielle que nous avons déjà se sont montrées très utiles », reconnaît-il. « Mais je pense que le développement d'une intelligence artificielle complète pourrait mettre fin à la race humaine », a-t-il déclaré cette semaine à la BBC. Déjà, le milliardaire Elon Musk avait expliqué avoir investi dans des sociétés d'intelligence artificielle pour « garder un œil » sur ce qui se passe dans ce domaine. « Nous devons nous assurer que les conséquences sont bonnes et non mauvaises », selon lui.

« Cela me fait plaisir qu'un scientifique des +Sciences dures+ dise cela. Je le dis depuis des années », déclare Daniela Cerqui, anthropologue à l'université de Lausanne.

« Nous déléguons à ces machines de plus en plus de prérogatives de l'humain, afin qu'elles soient plus performantes que nous. On va finir par devenir leur esclave », selon elle.

A l'inverse, Jean-Gabriel Ganascia, philosophe et expert en intelligence artificielle, juge « excessif » le « cri d'alarme » de Hawking. « Le danger, c'est davantage l'homme qui se servirait de ces technologies pour asservir » d'autres humains, considère ce professeur à l'Université Pierre-et-Marie-Curie à Paris.

– Développer une intelligence artificielle « amicale » –

Nick Bostrom, futurologue à l'Université d'Oxford, pense que « la machine intelligente parviendra à dépasser l'intelligence biologique. Il y aura alors des risques existentiels associés à cette transition ».

« Les machines sont déjà plus fortes que nous. Je pense qu'elles finiront aussi par devenir plus intelligentes, même si ce n'est pas le cas actuellement », ajoute-t-il.

Au cours de ces dernières années, d'énormes progrès ont été réalisés dans le domaine de l'intelligence artificielle, en tant que capacité à traiter, à analyser des données et à répondre à des questions.

Mais on est « encore loin » de l'intelligence artificielle générale « complète », qui inquiète Stephen Hawking, souligne Anthony Cohn, professeur à l'université de Leeds (centre du Royaume-Uni). « Il faudra encore plusieurs décennies. »

Mathieu Lafourcade, spécialiste en intelligence artificielle et en traitement du langage à l'Université de Montpellier (sud de la France), juge « alarmiste » l'avertissement du physicien.

Mais il pense que « dans un futur hypothétique », il faudra peut être « s'en remettre » dans certains domaines aux machines car leurs capacités intellectuelles auront dépassé les nôtres. « La machine nous proposera une solution que nous ne serons pas à même de comprendre mais il faudra lui faire confiance », par exemple si elle nous recommande des mesures contre le réchauffement climatique, considère-t-il.

« Toutefois, si la machine débloque, il faudra se réserver la possibilité de la débrancher », souligne-t-il.

Stuart Armstrong, futurologue à l'université d'Oxford, relève que « les incertitudes sur le développement de l'intelligence artificielle sont extrêmes ».

« Le problème, c'est qu'il est extrêmement difficile de programmer des objectifs compatibles avec la dignité voire la survie de l'humanité », dit-il.

« Il faudrait programmer presque toutes les valeurs humaines parfaitement dans l'ordinateur afin d'éviter que l'Intelligence artificielle n'interprète +éradique la maladie+ comme +tue tout le monde+ ou bien +garde les humains sains et saufs et contents+ comme +enterre tout le monde dans des bunkers avec de l'héroïne+ ».

« Il faut que les ingénieurs prennent ces problèmes au sérieux et trouvent des solutions pour développer une intelligence artificielle +amicale+, pleinement compatible avec les valeurs humaines », considère-t-il.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire...

Source :
<http://www.leparisien.fr/sciences/l-intelligence-artificielle-notre-futur-terminator-08-12-2014-4355179.php#xtref=https%3A%2F%2Fwww.google.fr%2F>