Antiterrorisme : les Fournisseurs d'Accès à Internet devraient travailler plus étroitement avec le gouvernement

Antiterrorisme : les Fournisseurs d'Accès à Internet devraient travailler plus étroitement avec le gouvernement

Les attentats perpétrés en France, la semaine dernière contre Charlie Hebdo, et à Montrouge, pourraient poser quelques questions sur le niveau de sécurité dans l'Union européenne, ainsi que sur les moyens des services de renseignement. Les FAI pourraient prochainement devoir se rapprocher davantage des gouvernements.

« Je suis fermement convaincu que le moment est venu pour l'UE de s'unir dans une action commune et cohérente contre le terrorisme ». Tels sont les propos de Rihards Kozlovskis, ministre letton de l'Intérieur, qui a représenté la présidence du Conseil de l'Union européenne à la réunion ministérielle internationale qui s'est tenue hier.

Les ministres d'Intérieur de la France, de l'Allemagne, de l'Autriche, de la Belgique, de l'Italie, des Pays-Bas, de la Pologne, du Royaume-Uni, de la Suède, de l'Espagne et du Danemark ont publié une déclaration (PDF) conjointe condamnant les actions terroristes contre le journal français Charlie Hedbo et les assassinats commis à Montrouge et Vincennes. Ensemble, ils souhaitent également affermir leur lutte globale contre la radicalisation.

Internet jouant un rôle majeur dans le déploiement de la propagande terroriste, il s'agira de l'une des pistes de réflexion privilégiée pour renforcer les mesures de sécurité. Les ministres expliquent ainsi :

« Préoccupés par l'utilisation d'Internet à des fins de haine et de violence, nous sommes déterminés à ce que cet espace ne soit pas perverti à ces fins, tout en garantissant qu'il reste, dans le strict respect des libertés fondamentales, un lieu de libre expression, respectant pleinement la loi ».

Pour ce faire, les gouvernements entendent accroître leurs travaux avec les fournisseurs d'accès à Internet pour renforcer leurs dispositifs de surveillance :

« Dans cette perspective, le partenariat avec les grands opérateurs de l'Internet est indispensable pour créer les conditions d'un signalement rapide des contenus incitant à la haine et à la terreur, ainsi que de leur retrait, lorsque cela est approprié et/ou possible. »

Depuis des années, les grandes sociétés de la Toile française ont été sensibilisées à la lutte contre l'antisémitisme. L'on se souvient notamment que l'Amicale des déportés d'Auschwitz et des camps de Haute-Silésie, le Consistoire israélite de France, et le MRAP (Mouvement contre le racisme et pour l'amitié entre les peuples) avaient déposé une plainte contre Yahoo! en 2000 pour avoir permis la vente d'objets nazis sur ses pages Internet.

Le contenu de cette déclaration commune commence à créer une certaine polémique : plusieurs internautes sur Twitter (via le hashtag #CharlieDoesSurf) soulignent le caractère contradictoire des marches républicaines pour la liberté d'expression avec des mesures de surveillance accrues pour un meilleur contrôle du Web qui se profilent à l'horizon.

Reste à connaître la nature de ces mesures qui seront décidées entre les États membres de l'Union européenne pour renforcer la vigilance des FAI, mais également des autres acteurs majeurs de la Toile.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…
Source : http://pro.clubic.com/technologie-et-politique/actualite-749239-terrorisme-fai-devront-renforcer-vigilence-collaborer-gouvernement.html
Par Guillaume Belfiore

Enregistrement des appels téléphoniques au travail – La CNIL simplifie les règles

Enregistrement des appels téléphoniques au travail – La CNIL simplifie les règles

La CNIL a fait publier au Journal Officiel une délibération créant une norme simplifiée pour autoriser les entreprises et les administrations à enregistrer les conversations téléphoniques des employés sur le lieu de travail.

Comme l'y autorise l'article 24 de la loi du 6 janvier 1978, la CNIL a publié une « norme simplifiée » qui permet d'alléger les formalités administratives pour être autorisé à procéder à l'écoute et l'enregistrement des conversations téléphoniques du personnel sur le lieu de travail. La norme, qui vaut autorisation pour quiconque déclare s'y conformer, a été publiée ce mardi au Journal Officiel, en tant que délibération n° 2014-474 du 27 novembre 2014.
Elle autorise les entreprises et les administrations à écouter et enregistrer les conversations téléphoniques des agents et employés, avec toutefois un certain nombre de réserves. Notamment :
Les écoutes et enregistrements doivent être « ponctuels » et donc ne peuvent pas avoir de caractère « permanent ou systématique », y compris pour les salariés qui seraient en période d'essai. Toutefois la CNIL se garde de fixer un critère chiffré, que ce soit en quantité brute ou en proportion d'appels enregistrables ;

Il n'est pas autorisé de croiser les enregistrements avec des données provenant d'une capture d'écran du poste informatique de l'employé ;

Les enregistrements doivent uniquement servir à la formation des employés, leur évaluation ou « l'amélioration de la qualité du service » ;

L'enregistrement vidéo est proscrit dans le cadre de la norme simplifiée (c'est-à-dire il faut solliciter une autorisation complémentaire) ;

Les employés et leurs interlocuteurs doivent être informés de la possibilité d'enregistrement, et d'une série d'informations complémentaires (finalité, catégories de données traitées, destinataires, transfert hors UE le cas échéant, droit d'accès…).

Les enregistrements doivent être effacés au maximum 6 mois après leur collecte, et conservés avec « toutes précautions utiles pour préserver la sécurité des données », notamment d'identification des personnes autorisées à y avoir accès.

En outre, la CNIL précise que la norme simplifiée s'applique également aux « documents d'analyse, tels que les comptes-rendus ou les grilles d'analyse réalisés dans le cadre des écoutes et des enregistrements ». Elle précise que les données collectées dans ce cadre doivent être « adéquates, pertinentes et non excessives » au regard des finalités définies, et qu'elles ne peuvent porter que sur les données identifiant l'employé et l'évaluateur, les informations techniques de l'appel (date, heure, durée), et l'évaluation professionnelle correspondante.

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

Source : http://www.numerama.com/magazine/31780-la-cnil-simplifie-l-enregistrement-des-appels-telephoniques-au-travail.html
Par Guillaume Champeau

Vie privée, vie professionnelle, sommes-nous

tous espionnés ? Reportage Zone Interdite

Vie privée, vie professionnelle, sommes-nous tous espionnés ? Reportage Zone Interdite

Avec le développement de la technologie, le monopole de la surveillance électronique n'est plus réservé à l'Etat : surveiller ses proches ou ses employés est devenu un jeu d'enfant.
Paul et Nicolas, deux maris, se livrent à l'espionnage conjugal. Ils ont installé des logiciels sur les téléphones portables de leurs épouses afin de suivre leurs conversations. Mais le danger vient aussi d'Internet, où les traces laissées sont très difficiles à contrôler. Des salariés ont ainsi été licenciés pour avoir critiqué leur patron sur Facebook. Cette tendance a parfois des conséquences tragiques. Aux Etats-Unis, Tyler Clementi, 18 ans, s'est donné la mort après avoir été filmé par ses colocataires. Au Royaume-Uni, des volontaires scrutent les images des caméras de surveillance pour dénoncer les infractions. Ils sont payés pour chaque alerte donnée.

Vie privée vie professionnelle sommes nous tous espionnés 1/7.
Reportage diffusé sur M6 dans l'émission Zone Interdite le 10/04/2011
Disponible sur YouTube en 7 parties.

Vie privée vie professionnelle sommes nous tous espionnés 2/7.
Reportage diffusé sur M6 dans l'émission Zone Interdite le 10/04/2011.
Disponible sur YouTube en 7 parties.

Vie privée vie professionnelle sommes nous tous espionnés 3/7.
Reportage diffusé sur M6 dans l'émission Zone Interdite le 10/04/2011.
Disponible sur YouTube en 7 parties.

Vie privée vie professionnelle sommes nous tous espionnés 4/7.
Reportage diffusé sur M6 dans l'émission Zone Interdite le 10/04/2011.
Disponible sur YouTube en 7 parties.

Vie privée vie professionnelle sommes nous tous espionnés 5/7.
Reportage diffusé sur M6 dans l'émission Zone Interdite le 10/04/2011.
Disponible sur YouTube en 7 parties.

Vie privée vie professionnelle sommes nous tous espionnés 6/7.
Reportage diffusé sur M6 dans l'émission Zone Interdite le 10/04/2011.
Disponible sur YouTube en 7 parties.

Vie privée vie professionnelle sommes nous tous espionnés 7/7.
Reportage diffusé sur M6 dans l'émission Zone Interdite le 10/04/2011.
Disponible sur YouTube en 7 parties.

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

Source :
http://www.programme-tv.net/programme/culture-infos/r8841-zone-interdite/2703356-vie-privee-vie-professionnelle-sommes-nous-tous-espionnes/

Surveillance des internautes – La loi valse sous haute discrétion

	Surveillance des internautes – La loi valse sous haute discrétion

Le 24 décembre, Matignon a publié un décret sur une mesure très contestée permettant aux agents de l'État de surveiller le Net français. Habile !C'est un cadeau de Noël dont les internautes et les opérateurs français se seraient bien passés. Le gouvernement a publié mercredi 24 décembre, à la faveur des fêtes de Noël, le décret d'application du très contesté article 20 de la loi de programmation militaire (LPM). Ce texte prévoit un accès très vaste des services de l'État aux télécommunications (téléphone, SMS, Internet, etc.) des Français, et à toutes les informations qui transitent par les réseaux nationaux.
La mesure de surveillance, pudiquement nommée « accès administratif aux données de connexion », avait été votée fin 2013 et entrera en vigueur le 1er janvier 2015. Dénichées par notre excellent confrère Next INpact (http://www.nextinpact.com/news/91534-le-decret-l-article-20-lpm-publie-on-fait-point.htm), qui évoque « un décret qui sent le sapin », ce sont les modalités de sa mise en oeuvre, tout aussi importantes, qui ont été dévoilées pour Noël.
Comme dans de nombreuses démocraties, le spectre terroriste permet au gouvernement de faire passer des mesures très floues et de tirer pleinement parti des systèmes d'information de plus en plus performants afin de surveiller la population.

Qui chapeaute le système ?
Le décret du 24 décembre présente « le groupement interministériel de contrôle […], un service du Premier ministre chargé des interceptions de sécurité et de l'accès administratif aux données de connexion ». Ce groupement est chargé de centraliser les demandes des agents et de les transmettre aux opérateurs concernés, en les épurant de toute information sensible.
En effet, si les services de l'État doivent justifier leurs requêtes auprès du Premier ministre (qui nomme une « personnalité qualifiée »), il est hors de question de transmettre ces explications aux opérateurs. Les fournisseurs d'accès ne sauront même pas de quel service ou ministère émane une demande, ni à quelle date elle a été formulée.

Quelles données sont concernées ?
Sans surprise, le décret se réfère à l'article 20 de la LPM, sans vraiment le préciser. Peuvent donc être interceptés les « informations ou documents traités ou conservés par les réseaux ou services de communications électroniques, y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications ».
On notera l'utilisation de la formule « y compris », qui n'est aucunement exhaustive : difficile de faire plus vaste.

Un contrôle démocratique insignifiant
Face aux critiques sur l'intrusion dans la vie privée, le gouvernement invoque la Commission nationale de contrôle des interceptions de sécurité (CNCIS), un organe très joli sur le papier mais qui n'a jusqu'à présent pas été doté d'un réel pouvoir. Cette commission « dispose d'un accès permanent aux traitements automatisés », et « l'autorité ayant approuvé une demande de recueil d'informations ou de documents fournit à la commission tous les éclaircissements que celle-ci sollicite », promet le décret, plein de bons sentiments.

Néanmoins, la CNCIS **n'a toujours pas le pouvoir de sanction et ne peut même pas alerter la justice en cas de manquement sur un dossier couvert par le secret de la défense nationale**. Habile…

Par ailleurs, le gouvernement se protège en supprimant ses archives en un temps record. Si l'on peut saluer la suppression des informations et des fichiers recueillis au bout de trois ans, on ne peut être que surpris par le fait que les registres mentionnant qui a autorisé telle ou telle surveillance soient eux aussi « automatiquement effacés » après trois ans. Le seul contrôle démocratique possible lorsqu'on jongle avec le secret défense, celui qui s'effectue a posteriori, est donc rendu impossible, pour la CNCIS comme pour la justice.

À quel prix ?
« Les coûts supportés par les opérateurs pour la transmission des informations ou des documents font l'objet d'un remboursement par l'État », précise le décret. Pas un mot sur la grille tarifaire qui sera appliquée, car ils seront définis par les ministères concernés.

Qui peut demander les informations ?
Trois ministères sont habilités à émettre des demandes. Le décret détaille le nombre impressionnant de services pour lesquels les vannes du Web français sont ouvertes :

– Au ministère de l'Intérieur : la Direction générale de la sécurité intérieure (DGSI), la Direction générale de la police nationale (unité de coordination de la lutte antiterroriste, Direction centrale de la police judiciaire, Direction centrale de la sécurité publique, Direction centrale de la police aux frontières), la Direction générale de la gendarmerie nationale (sous-direction de la police judiciaire ; sous-direction de l'anticipation opérationnelle ; service technique de recherches judiciaires et de documentation ; sections de recherches), la préfecture de police (Direction du renseignement ; direction régionale de la police judiciaire ; service transversal d'agglomération des événements ; cellule de suivi du plan de lutte contre les bandes ; sûreté régionale des transports ; sûretés territoriales).

– Au ministère de la Défense : la Direction générale de la sécurité extérieure (DGSE), la Direction de la protection et de la sécurité de la défense, la Direction du renseignement militaire.

– Au ministère des Finances et des Comptes publics : la Direction nationale du renseignement et des enquêtes douanières, le service de traitement du renseignement et d'action contre les circuits financiers clandestins.

Dans tous ces services, seuls les agents et officiers « dûment habilités » par leur directeur pourront réclamer des informations, assure le décret.

Des perspectives inquiétantes
La loi de programmation militaire a mis en place un outil de surveillance de la population française qui aurait fait pâlir d'envie les pires dictateurs de l'histoire. Si nous sommes très loin d'un régime totalitaire en France, il n'est pas exclu que des leaders extrémistes disent demain merci au gouvernement Valls pour leur avoir fourni un tel outil clé en main.

Pour info :
Décret n° 2014-1576 du 24 décembre 2014 relatif à l'accès administratif aux données de connexion
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000029958091&dateTexte&categorieLien=id

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

Source :
http://www.lepoint.fr/chroniqueurs-du-point/guerric-poncet/le-cadeau-de-noel-du-gouvernement-aux-internautes-la-surveillance-26-12-2014-1892495_506.php
Par GUERRIC PONCET

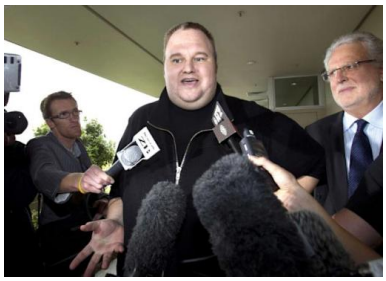
La NSA pourrait avoir eut accès aux appels, messages, fichiers, vidéos échangés sur Skype, d'aprè

La NSA pourrait avoir eut accès aux appels, messages, fichiers, vidéos échangés sur Skype, d'après de récents documents

Newly published NSA documents show agency could grab all Skype traffic

A National Security Agency document published this week by the German news magazine Der Spiegel from the trove provided by former NSA contractor Edward Snowden shows that the agency had full access to voice, video, text messaging, and file sharing from targeted individuals over Microsoft's Skype service. The access, mandated by a Foreign Intelligence Surveillance Court warrant, was part of the NSA's PRISM program and allowed "sustained Skype collection" in real time from specific users identified by their Skype user names. The nature of the Skype data collection was spelled out in an NSA document dated August 2012 entitled "User's Guide for PRISM Skype Collection." The document details how to "task" the capture of voice communications from Skype by NSA's NUCLEON system, which allows for text searches against captured voice communications. It also discusses how to find text chat and other data sent between clients in NSA's PINWALE "digital network intelligence" database. The full capture of voice traffic began in February of 2011 for "Skype in" and "Skype out" calls—calls between a Skype user and a land line or cellphone through a gateway to the public switched telephone network (PSTN), captured through warranted taps into Microsoft's gateways. But in July of 2011, the NSA added the capability of capturing peer-to-peer Skype communications—meaning that the NSA gained the ability to capture peer-to-peer traffic and decrypt it using keys provided by Microsoft through the PRISM warrant request. The NSA was then able to "task" any Skype traffic that passed over networks it monitored or by exploitation of a targeted user's system. "NSA receives Skype collection via prism when one of the peers is a (FISA Amendments Act Section 702) tasked target," the Skype collection guide stated. Because Skype has no central servers, the guide explained, for multiparty calls, "Skype creates a mesh-network, where users are connected together through multiple peer-to-peer links. Instant Messages sent to this group of meshed participants can be routed through any participant." If any participant in a chat was monitored, the NSA could capture all of the IM traffic in the shared chat. Initially, NSA analysts had to piece together voice communications between peers because they were carried over separate streams, but a service added by August of 2012 by the NSA's Cryptanalysis and Exploitation Services (CES) automatically stitched both audio streams of a conversation together. As of 2012, however, analysts still had to search for associated video from a call session to match it up with audio in a tool called the Digital Network Intelligence Presenter (DNIP).
Après cette lecture, quel est votre avis ? Cliquez et laissez-nous un commentaire… Source : http://arstechnica.com/tech-policy/2014/12/newly-published-nsa-documents-show-agency-could-grab-all-skype-traffic/

MegaChat : la messagerie anti-NSA signée Kim Dotcom

	**MegaChat : la messagerie anti-NSA signée Kim Dotcom**

Le sulfureux fondateur du défunt MegaUpload annonce le lancement d'une messagerie chiffrée capable d'échapper à la curiosité des services de renseignement, NSA en tête.

Kim DotCom signe son retour. Après avoir – en apparence du moins – négocié l'arrêt des attaques par déni de service contre les réseaux Sony PlayStation et Xbox Live avec les hackers de la Lizard Squad, le sulfureux fondateur du défunt site de téléchargement MegaUpload promet l'arrivée imminente d'un nouveau service de messagerie électronique et de discussion instantanée sécurisé par chiffrement. Un service baptisé MegaChat qui entre dans la croisade de Kim Dotcom visant à garantir aux internautes une confidentialité totale de leurs échanges numérique. Rappelons que ce dernier a déjà lancé un service de stockage chiffré, Mega.
Pour passer à travers les mailles du filet de la NSA et d'autres services de renseignement, cette alternative cryptée à Skype permettra aux internautes, dès début 2015, d'utiliser cette messagerie ultra-sécurisée dotée de fonctionnalités d'appels audio et de visioconférence.
Elle autorisa également « le transfert de fichiers à haute vitesse via un navigateur Web », a promis Kim Dotcom, dans un message publié sur Twitter. Pas besoin donc d'installer un logiciel spécifique sur son ordinateur ou sa tablette, notent nos confrères d'ITespresso. De manière sécurisée, les utilisateurs pourront, grâce au chiffrement intégral des données, envoyer, lire et partager des fichiers (audio, vidéos,…).

« Skype est obligé de fournir des backdoors »
« Vous ne pouvez faire confiance à aucun fournisseur de services en ligne installé aux Etats-Unis pour [garantir la confidentialité] de vos données », a souligné Kim Dotcom. « Skype n'a pas le choix. Ils sont obligés de fournir des backdoors au gouvernement américain ». A en croire l'homme d'affaires d'origine allemande, MegaChat serait donc un des seuls services Internet capables de garantir l'intégrité des données de ses membres, et de les préserver des manœuvres d'espionnage des autorités gouvernementales, Etats-Unis en tête.
Rappelons que selon des informations relayées par Der Spiegel et issues des documents confidentiels dévoilés par Edward Snowden, la NSA a réussi à contourner, dès la fin 2011, la sécurité de Skype pour permettre à l'agence américaine de mettre en place une collecte de données à grande échelle sur le système de communications, propriété de Microsoft.

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

Source : http://www.silicon.fr/megachat-messagerie-anti-nsa-kim-dotcom-104829.html

---

Accès administratif aux données de connexion: rassuré

avec le décret ?

	Accès administratif aux données de connexion: rassuré avec le décret ?

Le décret sur l'accès administratif aux données de connexion, en lien avec l'article 20 de la LPM, a été publié le 24 décembre. La cyber-surveillance tend à se généraliser malgré la vigilance de la CNIL.

C'est un grand classique quel que soit le gouvernement : la tentation de faire passer des décrets juste avant Noël pour éviter de faire trop de bruit. Mais le tour de passe-passe n'a pas échappé à des médias vigilants sur la protection de la vie privée comme NextInpact.

Dans le JORF en date du 26 décembre, on découvre le décret 2014-1576 « relatif à l'accès administratif aux données de connexion » (qui avait été approuvé le 24 décembre).
Une belle tentative de mettre en œuvre en catimini d'ici le premier janvier 2015 ce qui avait provoqué une polémique sur la protection des droits civils à l'ère numérique dans le cadre de l'examen du projet de loi sur la programmation militaire (LPM).
Adopté en décembre 2013, le texte dense intègre un article 20 au contour flou qui a des répercussions sur la vie civile : l'accès par les autorités – sans décision judiciaire – aux données de connexion des internautes.
Une approche qui suscitait des craintes sur l'encadrement de l'accès aux données à caractère personnel. Gare à la dérive cyber-sécuritaire, estimait des associations professionnelles du secteur IT comme Renaissance Numérique ou l'ASIC à l'époque.
Ainsi, la loi prévoit initialement l'accès par l'administration aux « informations ou documents traités ou conservés par leurs réseaux ou services de communications électroniques ». Le champ des données surveillées n'était pas limité aux seules données de connexion, mais pouvait concerner l'ensemble des données stockées par l'utilisateur : documents sur le cloud, mails, échanges sur les réseaux sociaux, pseudos, mots de passé, etc.

L'élargissement de la cyber-surveillance reste d'actualité avec la publication du décret associé à l'article 20 de la LPM. Le régime d'exception de l'accès administratif aux données de connexion – jusqu'ici associé principalement à la lutte antiterroriste – est généralisé : « Les données détenues par les opérateurs qui peuvent être demandées sont de plus en plus nombreuses et sont accessibles à un nombre de plus en plus important d'organismes. »
Et ce, pour des finalités très différentes » au nom de divers intérêts nationaux : « sauvegarde des éléments essentiels du potentiel scientifique et économique de la France », « prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous ».

Le spectre du Big Brother serait écarté partiellement avec les nouveaux éléments fournis dans le décret du 24 décembre sur « l'accès administratif aux données de connexion ». Celui-ci limite la collecte d'information aux données de connexion (identité de la personne, date et heure de communication, etc.) mais il reste néanmoins à préciser l'exact périmètre des données recueillies.

Bonne nouvelle : le décret semble écarter les risques de droit de regard sur les contenus.
De même, la DGSE, la DGSI ou tout autre service de police judiciaire ne pourront pas directement installer des logiciels d'espionnage (« mouchards ») de manière intensive sur les réseaux des opérateurs.
Selon l'avis de la CNIL rendu le 4 décembre (sur ce qui était à l'époque un projet de décret) mais qui vient juste d'être publié dans le prolongement de la promulgation du décret, il en résulte que « cette formulation interdit toute possibilité d'aspiration massive et directe des données par les services concernés et, plus généralement, tout accès direct des agents des services de renseignement aux réseaux des opérateurs, dans la mesure où l'intervention sur les réseaux concernés est réalisée par les opérateurs de communication eux-mêmes ».
L'autorité française en charge de la protection des données personnelles reste vigilante. « Elle appelle l'attention du gouvernement sur les risques qui en résultent pour la vie privée et la protection des données à caractère personnel et sur la nécessité d'adapter le régime juridique national en matière de conservation et d'accès aux données personnelles des utilisateurs de services de communications électroniques. »
L'année 2015 va mal démarrer alors que le gouvernement prépare une loi sur le numérique. L'occasion d'éclaircir le débat ? Dans le cadre de la consultation gouvernementale ouverte au grand public pour élaborer cette loi, on espère un peu plus de transparence à propos de cette extension de la cyber-surveillance.

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

Source : http://www.itespresso.fr/acces-administratif-donnees-connexion-rassure-publication-decret-85710.html

Au Japon, une banque de visages de clients suspectés de vols à l’étalage

	Au Japon, une banque de visages de clients suspectés de vols à l’étalage

Reconnaissance faciale des boutiques en réseau
Au Japon, un réseau de magasins se partagent une banque de visages de clients suspectés de vols à l'étalage ou de ceux qui « créent » des problèmes. Ceci sans que les personnes concernées en aient connaissance.

Automatically recorded images of shoppers' faces taken by security cameras have been shared among 115 Japanese supermarkets and convenience stores as an anti-shoplifting measure, without customers' knowledge.

Although the images are used mainly to prevent shoplifting, experts and industry bodies say it is necessary to make clear rules because providing people's facial data to a third party could constitute an invasion of privacy.
The facial data in question was shared by 115 stores of 50 separate operators that have installed a shoplifting prevention system that a Nagoya-based software development company had started marketing in October of last year.
The stores include major convenience stores operated by individuals under franchise contracts. At these shops, security cameras film all customers' faces. If a person shoplifts or makes an unreasonable complaint at one of the stores, security camera footage of the person is processed into facial data with the recognition system and classified into categories such as « shoplifter » and « complainer ».
They are then sent to the software firm's server to be recorded. The facial images themselves, however, cannot be browsed from other stores.
Once registered on the digital blacklist, however, a warning is issued to the staff of other stores – in a way only the staff can notice – when the face-recognition system installed at these stores detects the blacklisted person visiting their stores. At these stores, stickers are placed within the stores to inform customers that « face recognition security cameras are installed ». But customers are not informed that the stores are sharing the facial data.
Under Japanese law, facial images that are filmed by security cameras are considered personal information. The law allows such images to be filmed when it is used for crime prevention.
But sharing the facial data could be a violation of a law that bans providing personal information to a third party without the person's consent.
Lawyer Yoichiro Itakura said the data could be used in a way disadvantageous to customers as « stores can arbitrarily register specific shoppers as suspicious people, and they may then suffer unjust treatment at stores they have never visited before ».
An official of the Nagoya software development firm said: « The system has no problems. We just responded to the needs of the stores, which is their need to prevent shoplifting. »

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

Source : http://www.scmp.com/news/asia/article/1466536/115-japanese-stores-sharing-customers-facial-data
Par Yomiuri Shimbun

Système d’appel d’urgence (eCall) obligatoire à partir d’octobre 2015

Système d’appel d’urgence (eCall) obligatoire à partir d’octobre 2015

A partir d’octobre 2015, tous les nouveaux véhicules vendus dans l’Union européenne seront équipés d’un service permettant de composer un numéro d’urgence en cas d’accident grave: le système eCall. C’est ce que prévoient les nouvelles règles qui seront votées par la commission du marché intérieur le 11 février 2014.

« eCall »: c’est le nom de ce système qui devrait sauver de nombreuses vies. En cas d’accident, le système eCall compose automatiquement le 112, et ce dès que ses capteurs (situés par exemple sur les airbags) enregistrent un choc. Le numéro pourrait également être activé manuellement, grâce à un bouton spécial. Le système est censé transmettre ensuite le lieu et l’heure de l’accident au centre de secours le plus proche.

« Le système eCall pourrait sauver jusqu’à 2500 vies par an, ce qui est selon moi un argument décisif pour l’introduction de ce service public d’appel d’urgence dans toute l’Union européenne », a déclaré le rapporteur Olga Sehnalová, députée démocrate socialiste tchèque.

D’ici là, les Etats membres devront améliorer leur infrastructure de manière à ce que les eCalls aboutissement directement aux services d’urgence.

Aujourd’hui, seuls 0,7 % de tous les passagers dans l’Union européenne sont équipés de systèmes automatiques d’appels d’urgence. Le coût d’une installation de l’outil eCall est estimé à moins de 100 euros par véhicule.

Voir aussi sur le même sujet « Installation obligatoire d’eCall dans les véhicules à partir de 2015 »
http://www.techno-science.net/?onglet=news&news=11767

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

Source : http://www.techno-science.net/?onglet=news&news=12481

Edward Snowden pour la première fois en France s’est exprimé. Il est confiant sur la « prise de conscience » du grand public

	Edward Snowden pour la première fois en France s’est exprimé. Il est confiant sur la « prise de conscience » du grand public

Pour la première fois, Edward Snowden s'est exprimé en France dans le cadre d'une conférence organisée par la branche française d'Amnesty International. L'ex sous-traitant de la NSA n'a pas fait de révélations sur le cas français, mais s'inquiete d'une situation « qui a empiré ».

Pour ceux qui espéraient des déclarations fracassantes d'Edward Snowden sur les moyens d'espionnage mis en œuvre par le renseignement français, c'est un peu raté. L'ancien sous-traitant de la NSA s'exprimait hier à l'occasion de la conférence organisée par Amnesty International. Toujours bloqué en Russie, il a communiqué par vidéoconférence (Via Google Hangouts) et a répondu aux questions du journaliste Nicolas Demorand.
Interrogé sur les changements qu'il a perçu depuis ses révélations en 2013, Snowden semble globalement satisfait de la prise de conscience qu'il a provoqué mais reste lucide « Dans beaucoup de pays occidentaux la situation a empiré. Mais on voit aussi des critiques et dans la décennie à venir, celles-ci vont continuer » a-t-il expliqué. Conscient que « rien ne va changer en un mois ou en un an», il cite notamment des études qui montrent qu'un tiers de la population sondée a entendu parler des révélations et que 40% des concernés a pris des mesures spécifiques pour protéger sa vie privée.
Il rappelle également les différentes initiatives juridiques et politiques qui ont émergées à la suite de ces révélations : « Des choses bougent en Europe sur la protection des données. Mais l'important est d'avoir des standards internationaux sur ce qui est autorisé ou pas. »

Rien à dire sur la France
« Le problème n'est pas que le gouvernement veuille combattre le terrorisme, mais c'est d'inventer des systèmes d'espionnage pour toute la population et non pas pour des individus en particulier » a rappelé Edward Snowden. Et en France alors ? « Je n'ai pas de scoop sur la France » a-t-il confessé, rappelant néanmoins que la surveillance de masse était une réalité pour tous les pays développés. Snowden s'appuie notamment sur l'enquête du Monde ayant révélé les relations entre la DGSE et l'opérateur historique Orange pour étayer ses propos mais n'a pas apporté de nouveaux éléments sur le cas français.

Actualité oblige, Snowden a également évoqué la récente publication du rapport faisant état des pratiques de tortures utilisées par les États Unis dans la lutte contre le terrorisme. Un rapport qui « l'attriste et le révolte ». Snowden explique avoir travaillé à la CIA mais n'avoir entendu que des rumeurs sur les programmes évoqués par le rapport. Et il s'inquiète des conséquences d'un tel laxisme : « si les Etats Unis s'autorisent à torturer, quel signal cela va-t-il envoyer aux pays moins démocratiques ? »

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

Source : http://www.zdnet.fr/actualites/snowden-confiant-sur-la-prise-de-conscience-du-grand-public-39811211.htm