

Licencié pour un abus d'utilisation de l'email perso en entreprise ? Voici un levier de contestation !

 Denis JACOBINI vous informe	Licencié pour un abus d'utilisation de l'email perso en entreprise ? Voici un levier de contestation !
L'employeur qui n'a pas déclaré préalablement à la CNIL son système de surveillance des salariés ne peut pas en utiliser les données récoltées pour sanctionner ou licencier un salarié pourtant fautif. Dans un arrêt en date du 8 octobre 2014, n° 13-14991, la Cour de cassation a jugé que des informations collectées via un système de traitement automatisé de données personnelles ne pouvaient être utilisées par l'employeur à l'appui d'un licenciement dès lors que le dispositif n'avait pas encore été déclaré à la Cnil. En l'espèce, l'employeur n'avait pas omis de déclarer le système de surveillance à la Cnil, mais l'avait déclaré tardivement, à savoir près de 2 mois et demi après sa mise en place. Ce dispositif avait toutefois servi dès son installation à mettre en lumière l'utilisation excessive par une salariée de sa messagerie professionnelle à des fins personnelles. Si » le système de surveillance permettait de prendre connaissance non pas du contenu des messages mais de la date et de l'heure d'envoi ou de réception, de leur destinataire ou expéditeur et de leur objet. Il avait ainsi comptabilisé, sur une période de 2 mois, un peu plus de 1200 messages personnels envoyés et reçus par la salariée via sa messagerie professionnelle » rappelle un auteur. La Cour de cassation invalide le licenciement de la salariée fondé sur une utilisation abusive de la messagerie électronique durant les 2 mois ayant précédé la déclaration du dispositif de surveillance à la Cnil, considérant que « constituent un moyen de preuve illicite les informations collectées par un système de traitement automatisé de données personnelles avant sa déclaration à la Cnil ». Par Me Grégoire HERVET Et vous ? Vous en pensez quoi ? Cliquez et laissez-nous votre avis... Source : http://www.juritravail.com/Actualite/obtenir-des-dommages-et-interets-pour-licenciement-pour-faute-grave-ou-lourde-injustifie/Id/170721	

Technologie: Le numérique a la mort aux trousses



Technologie: Le numérique a la mort aux trousses

Aurore est décédée. C'était il y a cinq ans. Pourtant, son profil Facebook, lui, vit toujours. Ses proches l'ont transformé en mausolée. Untel poste une photo, un autre se fend d'un mot souvenir. Le tout ne serait pas choquant si le réseau social n'envoyait pas chaque année une alerte anniversaire à ses «amis». L'internaute ne meurt-il donc jamais?

Avec le développement des technologies digitales, la question de la mort numérique s'invite dans le débat, entraînant avec elle une foule de questions: que deviennent nos données numériques (mails, réseaux sociaux, photos...) lorsque l'on passe de vie à trépas? Peut-on hériter d'une bibliothèque iTunes comme on récupérerait les vinyles de grand-père? Les morts du Web ont-ils le droit de reposer en paix? «Le sujet reste encore très peu encadré par la loi, souligne le conseiller national Jean Christophe Schwaab, c'est pourquoi j'ai décidé de déposer un objet parlementaire en septembre dernier, afin que le droit de succession s'intéresse enfin aux données numériques.» L'enjeu est de taille. Selon la Commission nationale de l'informatique et des libertés (Cnil), un profil Facebook sur cent – soit 130 millions de pages – appartiendrait à un mort.

Et vous ? Vous en pensez quoi ?

Cliquez et laissez-nous votre avis...

Une députée propose que la famille puisse supprimer les données d'un proche décédé

	Identité numérique : des défunts : Une députée propose que la famille puisse supprimer les données d'un proche décédé
La suppression des données personnelles présentes en ligne, même après le décès d'une personne, reste actuellement dans le flou. Une députée demande à ce que les proches puissent faire retirer ces informations. Afin d'aider les familles à gérer la mort d'un proche, des procédures permettant de supprimer les comptes en ligne existent. Parfois complexes, elles autorisent toutefois à ce que des membres d'une même famille puissent empêcher que les informations soient utilisées ou que le compte subsiste. Lorsqu'un tel événement survient, la personne qui se charge de cette tâche doit donc généralement passer par des formulaires en ligne, tous différents, en fonction du service ciblé. Une tâche qui peut donc s'avérer fastidieuse, lorsque plusieurs plateformes (ou ensemble tels que la constellation Gmail, YouTube, Drive...) sont pris en compte. Face à cette complexité, la députée socialiste Edith Gueugneau demande à ce que les règles en la matière soient plus précises. Dans une question adressée à Axelle Lemaire, secrétaire d'Etat chargée du numérique, l'élue estime que la loi est à ce jour « imprécise sur le devenir de ces données après le décès de l'utilisateur » et considère qu'il est : « particulièrement difficile pour les proches du défunt d'obtenir l'effacement de ces données. La loi ne prévoit pas non plus de délai d'exécution de la demande ». C'est pourquoi elle demande que la loi puisse donner aux proches d'une personne décédée un droit, afin qu'ils puissent faire effacer ces données personnelles. La députée PS souhaite pour cela associer FAI, moteurs de recherche ainsi que les services de l'état civil. Si l'idée d'un effacement complet du Web ne paraît pas réaliste, certaines pistes pourraient conduire à cette finalité. La procédure de « droit à l'oubli » mise en place par les moteurs de recherche pouvant par exemple être étendue à cet effet. Toujours est-il qu'il revient désormais à Axelle Lemaire de se pencher sur cette question. Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès) Source : http://pro.clubic.com/legislation-loi-internet/donnees-personnelles/actualite-739481-donnees-mort-flou.html?&svc_mode=M&svc_campaign=NL_ClubicPro_New_18/11/2014 par Olivier Robillart	

Airbus Helicopters a-t-il été victime d'un piratage

informatique américain?



Airbus
Helicopters
a-t-il été
victime d'un
piratage
informatique
américain?

Selon des sources concordantes, Airbus Helicopters a été victime d'une attaque informatique. Le constructeur a de « fortes suspicions » d'une attaque venant des États-Unis.

C'est peut-être une affaire d'État. Certes ce qui s'est passé chez Airbus Helicopters n'est pas réellement surprenant mais si l'enquête des autorités françaises en cours confirme les « fortes suspicions » du constructeur de Marignane, selon des sources concordantes, elle mettrait une nouvelle fois en lumière les pratiques détestables d'espionnage des États-Unis à l'égard de leurs alliés malgré toutes les conséquences néfastes sur le plan diplomatique de l'affaire Snowden. Ce qui est sûr, selon ces mêmes sources, c'est que Airbus Helicopters a bien été victime d'une attaque informatique, dont l'ampleur reste encore à déterminer.

Le constructeur de Marignane s'est récemment aperçu d'une intrusion ou d'une tentative d'intrusion dans ses réseaux de communications. Alerté par Airbus Helicopters, l'Agence nationale de la sécurité des systèmes d'information (ANSSI), l'autorité nationale en matière de sécurité et de défense des systèmes d'information, a lancé une enquête pour savoir si les intrusions ont réussi et, si c'est le cas, pour déterminer l'ampleur des dommages. Contacté par La Tribune, Airbus Helicopters affirme qu'« aucune information classifiée » n'a été dérobée. Mais, selon des sources concordantes interrogées par La Tribune, le constructeur nourrit de « fortes suspicions » vis-à-vis des États-Unis. « Mais nous n'avons pas encore d'éléments pour le démontrer », explique-t-on chez le constructeur à La Tribune.

En jeu, un important appel d'offre en Pologne

Pourquoi les États-Unis ? Selon ces mêmes sources, le constructeur suspecte s'être fait « piraté » dans le cadre de l'appel d'offres international lancé par la Pologne, qui veut acheter 70 hélicoptères de transport pour un montant estimé à 2,5 milliards d'euros environ. Les trois compétiteurs – l'italien AgustaWestland (AW149), Airbus Helicopters (Caracal ou EC725) et l'américain Sikorsky (S-70) attendent une décision de Varsovie fin 2014, voire début 2015. Les candidats ont jusqu'au 28 novembre pour déposer leurs offres. Jusqu'ici la compétition entre Airbus Helicopters et Sikorsky était très, très chaude.

Depuis plusieurs jours, Sikorsky joue d'ailleurs un drôle de jeu en Pologne. Les Américains veulent vendre des hélicoptères dont les performances ne correspondent pas au cahier de charge établi par Varsovie. Ce sont des appareils d'ancienne génération qu'ils ont en stock. Le ministère polonais de la Défense a répliqué fin octobre sur un ton extrêmement ferme à un courrier du président du consortium Sikorsky Aircraft Corporation (SAC) Mick Maurer, en affirmant que c'est à lui qu'appartient de « définir les besoins des forces armées et non au soumissionnaire de lui indiquer ce qu'il a à vendre ».

Que va faire Sikorsky ?

« Les exigences concernant l'hélicoptère multitâche étaient connues depuis mai dernier et la société SAC dispose d'appareils qui y répondent », a relevé le ministère polonais, avant de noter que « les autres candidats ont annoncé qu'ils présenteraient des offres correspondant aux exigences de l'Inspection de l'Armement ». Le ministère « ne prévoit pas d'annuler l'appel d'offres ou d'en modifier les termes au détriment de la Pologne », a assuré Varsovie, laissant entendre que tel était le sens de la lettre de Sikorsky. Il « reste ouvert à un dialogue équitable avec tous les candidats, mais ne cède pas aux pressions de contractants potentiels concernant les termes de la commande ».

Du coup, le 30 octobre, Sikorsky Aircraft a annoncé qu'elle ne participerait pas à l'appel d'offres pour la fourniture de 70 hélicoptères à la Pologne si les termes n'en sont pas modifiés. Le constructeur a précisé qu'il ne présenterait pas de proposition avec son partenaire polonais PZL Mielec car il lui semble impossible de livrer ses hélicoptères Black Hawk dans les conditions définies par l'appel d'offres. Dans un communiqué, le ministère polonais de la Défense a qualifié cette attitude de tactique de négociation, ce qu'a démenti Sikorsky. Le ministère a confirmé qu'il n'envisageait pas de modifier les termes de l'appel d'offres.

Cet article vous a plu ? Laissez-nous un commentaire (Source de progrès)

Source :

<http://www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/20141113trib0392bd0ed/airbus-helicopters-a-t-il-ete-victime-d-un-piratage-informatique-americain.html>

Données c'est donner...



Données
c'est
donner...

Fondateurs de réseaux sociaux ou de sites de rencontre, tous tentent d'exploiter les data des internautes. Des manipulations s'opèrent, à l'insu des utilisateurs... Les questions d'éthique et de droit restent posées.

En juin, Facebook révélait avoir mené une expérience psychologique sur près de 700 000 utilisateurs à leur insu.

L'idée: tester une potentielle «contagion émotionnelle».

Dans la foulée, le site de rencontre OKCupid affichait des «manipulations de profils» de ses internautes.

Christian Rudder, cofondateur du site, postait récemment un billet intitulé «Nous réalisons des expériences sur les êtres humains», affirmant : «si vous utilisez Internet, vous êtes l'objet de centaines d'expériences, à tout moment quel que soit le site.» De quoi faire frissonner.

OKCupid est un site basé sur des questions auxquelles l'on répond en tant qu'utilisateur, sur tous sujets – de la propreté du bac à douche, à la fellation ou encore à l'usage du LSD. Plus l'internaute répond, plus l'Algorithme Magique est susceptible de lui proposer l'âme sœur. Soit. Et de fait, sur une base aussi riche, il est possible d'envisager une pertinence ethno-sociologique à ces expériences in vivo qui posent bien entendu des questions éthiques. Peut-on utiliser les données d'innocents internautes qui viennent chercher une cour de récréation / une rencontre sur les réseaux sociaux ?

Ces thèmes ont été largement discutés. Ce qui choque, c'est la position «de plein droit» que s'accordent les géants du Net, s'affichant dans une normalité sur le thème: «Oui, nous utilisons vos données, et alors ?» Et alors... ? Bizarrement, c'est aussi ce que répondent nombre d'internautes quand ont les avertis de l'impact de leurs clics. Faites le test. Expliquez à une personne non avertie que ses données sont transmises à l'annonceur quand il en like la pub. Réponse probable : «Qu'est-ce qu'on s'en fout ?»

Pourtant quand le juriste-activiste autrichien Max Schrems a demandé à Facebook de lui envoyer une compilation de ses données, **il a reçu un fichier de plus de mille pages** contenant ses informations présentes sur le site, y compris celles qu'il pensait avoir supprimées. Il a déposé une plainte cet été, rappelant que les questions éthiques posées par ces intrusions impliquent d'abord une prise de conscience de l'individualité et du droit des internautes.

DATA EN MASSE

Avec respectivement 1,2 milliard et 4 millions d'utilisateurs, les américains Facebook et OKCupid bénéficient d'un corpus qui combinent âge, sexe, CSP, habitat (urbain, rural), habitudes de consommation, et même religion. Autant de données croisées qui feraient rêver n'importe quel statisticien.

Stéphanie ESTOURNET

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :

http://ecrans.liberation.fr/ecrans/2014/10/17/donnees-c-est-donner_1115973?xtor=rss-450

La Cnil met en demeure Apple France, accusé de surveiller en permanence ses salariés...

	La Cnil met en demeure Apple France, accusé de surveiller en permanence ses salariés...
La firme à la pomme a été épinglée plusieurs fois par la Commission pour sa pratique abusive des caméras de surveillance, même dans les espaces de repos des salariés.	
Il fut un temps où Apple dénonçait à grands coups de publicités la surveillance généralisée d'une société, comme dans 1984. La firme à la pomme semble aujourd'hui avoir zappé ces beaux principes...	
La Cnil annonce en effet avoir mis en demeure Apple Retail France pour sa pratique abusive des caméras de surveillance dans ses boutiques et pour le manque d'information des salariés. Les caméras « ne sont pas orientées uniquement vers les zones sensibles (apporte d'accès ou coffre-fort) mais filment de manière directe et constante les postes de travail » mais aussi la salle de repos d'une des boutiques.	
Cette surveillance, « est disproportionnée au regard de la finalité de prévention des atteintes aux personnes et aux biens. Si la surveillance de zones sensibles est justifiée par des impératifs de sécurité, le placement sous surveillance permanente de salariés, attentatoire à leur vie privée, ne peut intervenir que dans des circonstances exceptionnelles », assène la Commission.	
Surveillance disproportionnée Ce n'est en fait pas la première fois que la firme est épinglée par la Commission informatique et Libertés. En décembre 2013, elle faisait déjà l'objet d'une mise en demeure portant sur le dispositif de vidéosurveillance des salariés installé au sein de l'Apple Store d'Opéra à Paris. « Il était notamment demandé à la société de réorienter certaines caméras qui filmaient en permanence des salariés et de leur délivrer une information complète », explique la Cnil. En février 2014, la société a justifié s'être mise en conformité avec ses obligations pour le magasin, entraînant la clôture de la mise en demeure. Mais des contrôles menés en mai et juin derniers dans d'autres magasins français du géant « ont révélé que la société n'avait pas adopté des mesures de conformité similaires à l'ensemble de ses magasins. L'information des salariés sur le dispositif demeurait lacunaire et certaines caméras continuaient à filmer des salariés à leur poste de travail sans justification particulière ». « La persistance de ces manquements » a conduit la Commission à mettre à nouveau en demeure la société « de modifier l'intégralité des dispositifs de vidéosurveillance de ses 16 magasins sur le territoire national ». « Aucune suite ne sera donnée à cette procédure si Apple France se conforme à la loi dans le délai de deux mois qui lui est imparti », ajoute la Cnil. Dans le cas contraire, la firme pourrait écoper de sanctions financières. Voilà de quoi tendre encore un peu plus les relations entre Apple et ses salariés français. En 2012 déjà, ces derniers s'étaient mis en grève. En cause, des revendications sur les salaires et les conditions de travail. Les syndicats négociaient avec la direction la mise en place de différents dispositifs, dont l'attribution de tickets restaurant et d'un 13e mois. Les salariés ont finalement obtenu une concession : des tickets restaurant d'un montant de 8,50 euros... Par Olivier Chicheportiche	
Cet article vous a plu ? Laissez-nous un commentaire (Source de progrès)	
Source : http://www.zdnet.fr/actualites/la-cnil-met-en-demeure-apple-france-accuse-de-surveiller-en-permanence-ses-salaries-39808739.htm	

Est-ce que votre site Internet est en règle avec la CNIL ?

Est-ce que votre site Internet est en règle avec la CNIL ?

Est-ce que votre site Internet est en règle vis à vis de la loi informatique et libertés ?

Des grands changements ont eu lieu ces derniers mois.

Déclaration à la Cnil d'un dispositif de contrôle et moyen de preuve

	Déclaration à la Cnil d'un dispositif de contrôle et moyen de preuve
Les informations collectées par un système automatisé de contrôle des données à caractère personnel avant sa déclaration à la Cnil constituent un moyen de preuve illicite. Une salariée engagée en tant qu'assistante chargée de l'analyse financière des dossiers ayant fait un usage excessif de sa messagerie électronique à des fins personnelles, son employeur l'a licenciée pour cause réelle et sérieuse. La cour d'appel a rejeté les demandes de dommages et intérêts de la salariée pour licenciement sans cause réelle et sérieuse et pour licenciement vexatoire, au motif que la déclaration tardive à la Cnil de la mise en place d'un dispositif de contrôle individuel des flux de la messagerie électronique ne rend pas ce système de contrôle illicite, alors que la salariée ne faisait pas un usage raisonnable de cet outil à des fins privées, durant son temps de travail. La Cour de cassation censure cette position, dans un arrêt du 8 octobre 2014, et considère que les informations collectées par un système de traitement automatisé des données personnelles avant sa déclaration à la Cnil, constituent un moyen de preuve illicite. Les éléments de preuve obtenus à l'aide d'un tel système avant sa déclaration à la Cnil ne sont donc pas licites. Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès) Source : http://actualitesdudroit.lamy.fr/Accueil/Articles/tabid/88/articleType/ArticleView/articleId/125297/Declaration-a-la-Cnil-dun-dispositif-de-controle-et-moyen-de-preuve.aspx	

Une bague connectée pour mieux nous contrôler ?



Une bague
connectée pour
mieux
nous contrôler
?

Un anneau pour les contrôler tous ? Au Japon, plusieurs sociétés planchent sur le concept de bague connectée, avec l'ambition de proposer reconnaissance de mouvements, clé sans contact, porte-monnaie électronique et système d'alerte au sein d'un seul et même petit appareil en forme de bijou.

Lunettes, montres ou vêtements, la tentation est grande de conférer des capacités informatiques à tous les objets du quotidien et beaucoup d'acteurs courent après la vision d'un accessoire à tout faire, fonctionnant en adéquation avec un smartphone. Parmi les différentes intégrations possibles, plusieurs se sont déjà intéressés à la bague. Un anneau se fait aisément oublier tout en restant accessible, et le doigt reste encore l'un des meilleurs moyens qu'a trouvés l'homme pour interagir avec son environnement. Jusqu'ici, les premières tentatives en matière d'anneaux connectés se sont toutefois révélées décevantes, en grande partie parce que les interactions proposées étaient à trop faible valeur ajoutée...

La donne va-t-elle changer ? La miniaturisation des composants permet désormais d'aller plus loin, comme en témoigne le projet développé par la start-up japonaise 16Lab. Celle-ci planche sur un anneau de titane qui, à terme, servirait aussi bien à la saisie de texte et de messages qu'à ouvrir la porte de sa voiture, payer ses courses ou alerter lors de la réception d'un message. Dans sa version actuelle, encore en cours de développement, la bague embarque deux petites surfaces tactiles qu'il suffit d'actionner du pouce pour « réveiller » l'appareil, qui émet alors une vibration de confirmation. Au centre de l'anneau, on trouve un composant développé par ALPS, qui propose, au sein d'une enveloppe de seulement 6 mm² une liaison Bluetooth 4.0, un accéléromètre et une boussole. Cette puce permet donc d'assurer la liaison avec le smartphone de l'utilisateur, mais aussi de mesurer la position de sa main dans l'espace ainsi que les mouvements de cette dernière.

D'après son concepteur, le dispositif est suffisamment précis pour envisager sérieusement d'écrire à main levée, en traçant simplement dans les airs les caractères. ALPS propose d'ailleurs des scénarios dans lesquels un démonstrateur contrôle une interface de télévision ou de téléphone grâce à des gestes capturés non pas par une caméra, mais par ce sensor network module.

16Lab admet toutefois sans ambages que la simple reconnaissance de mouvements ne justifierait sans doute pas l'achat et le port d'une telle bague. Il fallait donc chercher à enrichir cette dernière, ce qui passe par l'ajout de composants supplémentaires. Rapidement, le NFC s'est imposé comme une piste à étudier : les communications en champ proche, en plein essor, permettent en effet d'utiliser l'anneau comme une clé, capable d'actionner une serrure compatible, mais aussi comme un porte-monnaie électronique, à l'instar des déploiements en cours dans l'univers de la téléphonie mobile. Plutôt que de sortir son téléphone de sa poche, on n'aurait donc qu'à poser la main sur une surface dédiée au paiement. Dans tous ces scénarios, la bague fonctionne comme une interface rapprochée de la main, l'intelligence et la communication restant gérés au niveau du téléphone.

Alors, la bague sera-t-elle le parfait « raccourci » ? En attendant que le marché en décide, une autre start-up japonaise a justement fait de cette notion son slogan. Logbar Inc. développe également une bague à tout faire, avec une proposition de valeur similaire à celle qu'avance 16Lab. Sa bague s'appelle pour l'instant simplement Ring, et les développements reposent sur des fonds levés grâce au financement participatif. Bouclée en début d'année, la campagne Kickstarter de Logbar a débouché sur une enveloppe globale de 880 000 dollars, alors que la société avait fixé son objectif à 250 000 dollars. Le concept de bague connectée semble donc ne pas laisser indifférent. Reste à voir dans quelle mesure ces premiers essais seront transformés.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :

<http://www.clubic.com/technologies-d-avenir/ceatec/actu-une-bague-connectee-pour-les-controler-tous-731899.html>

France Connect, pour simplifier l'administration

numérique



France Connect,
pour simplifier
l'administration
numérique

Les administrations et les collectivités locales qui bénéficieront à court terme d'un support d'identification unifié.

Thierry Mandon, le secrétaire d'Etat chargé de la réforme de l'Etat et de la simplification, s'est rendu le 2 octobre dans les locaux de la Dila pour visiter le plateau de développement du projet « France Connect ». France Connect est la « marque de fabrique » du futur système numérique national d'identification et d'authentification des usagers des services de l'administration.

Le dispositif, développé par le Secrétariat général pour la modernisation de l'action publique (SGMAP), cible les services publics de l'Etat, les administrations et les collectivités locales qui bénéficieront à court terme d'un support d'identification unifié, bon marché et relativement facile à implémenter dans leur propre système d'information.

Ce programme, qui sera déployé dès 2015 avec la bascule sur France Connect des trois millions de comptes du site portail « mon.service-public.fr », doit permettre à l'utilisateur de fédérer tous ses comptes publics existants, puis d'établir ensuite de nouvelles connexions avec des administrations non encore dotées de leur propre système d'authentification, à condition d'adopter directement celui de France Connect.

La solution annule et remplace la carte d'identité électronique

La procédure qui s'apparente à celle déjà pratiquée par les réseaux sociaux comme « Facebook Connect » ou « Google+ Sign in » restera relativement simple à déployer. L'utilisateur n'ayant pas encore de compte pourra s'enregistrer à partir d'une administration reconnue par le label et à laquelle il est numériquement affilié. Après avoir saisi ses identifiants d'origine, le site lui proposera en retour de fédérer son compte avec France Connect.

Après avoir donné son consentement, il disposera d'un compte national réutilisable sur de nombreux sites. Cette simplicité dans le mode d'enregistrement a d'ailleurs incité la DGFIP à proposer aux contribuables, dès la campagne 2016 de déclaration de revenus en ligne, de fédérer leur compte « impôts.gouv.fr » avec France Connect afin d'étendre rapidement le dispositif aux 10 millions d'utilisateurs dotés d'un compte fiscal.

France Connect ne se limite pas au seul composant unifié d'identification. A terme, il devrait permettre aux administrations et notamment aux collectivités d'effectuer des requêtes sur le niveau d'imposition ou sur la domiciliation de l'utilisateur afin d'éviter l'étape coûteuse des demandes de justificatifs. Selon un expert ayant participé à la définition du projet, la nouvelle solution répondrait à 95% des besoins justifiant la création d'une carte d'identité électronique (CNIE) et l'économie réalisée sur la « non création » de cette carte avoisinerait le milliard d'euros.

France Connect devrait ainsi accélérer le développement de portails de téléservices couvrant la totalité des besoins transactionnels des collectivités avec les usagers et constituer également une brique essentielle de la mise en œuvre du programme « dites-le nous une fois » dans toutes les administrations. Autant dire qu'il constitue déjà à lui seul un levier essentiel pour les prochaines conquêtes de l'administration numérique.

Philippe Parmantier / EVS

Cet article vous a plu ? Laissez-nous un commentaire (Source de progrès)

Source :

<http://www.localtis.info/cs/ContentServer?pagename=Localtis/LOCActu/ArticleActualite&cid=1250267813817>