

SECURITY NEWS N°81 – 22 février 2010
L'actualité de la privacy et de la dématérialisation
Préparée par Arnaud Belleil

Si vous estimez que cette lettre est utile, n'hésitez pas à la faire découvrir à vos amis, collègues ou relations - <http://www.cecurity.com/site/PubNews2010.php>

SOMMAIRE :

L'article : La communication du dossier médical

Economie des données personnelles

Est-il possible de vendre de la *privacy* ?
Croisement des fichiers clients dans les télécom
Bing : anonymisation de l'adresse IP après 6 mois

Administration électronique

La santé en ligne vue par les conservateurs britanniques
25 propositions pour relancer l'administration électronique

Juridique

La Cnil encadre les éthylotests antidémarrage
Parution du premier Index du droit d'accès
« *Privacy by Design* », un nouveau principe juridique ?

Archivage et dématérialisation

Le Royaume-Uni se penche sur l'archivage du web
Réutilisation des archives en ligne

Identité Numérique

Carte d'identité avec visage à 360 C°
Lancement du label IdéNum

A découvrir

Vote sur internet : sécurisation sans chiffrement
PCI DSS et la protection des données carte bancaire

Evènements

La Fédération Nationale des Tiers de Confiance à Documation

ANNONCE : Cecurity.com renforce sa position dans l'archivage électronique

Cecurity.com a procédé à l'acquisition, en date du 30 décembre 2009, de la société Micrographie Services spécialisée dans la dématérialisation et l'archivage numérique. Cette opération de croissance externe permet à Cecurity de pratiquement doubler sa taille.

■ ■ ■ En savoir plus :
http://www.cecurity.com/site/Documentation/Presse/2010/PRESSE_Communique_AcquisitionMicrographie_Cecurity_100105.pdf

L'ARTICLE : LA COMMUNICATION DU DOSSIER MEDICAL

Daphné Jayet est Correspondant Informatique et Libertés (CIL), chargée de la qualité du Système d'Information du Centre Hospitalier d'Arras. Dans le cadre du mastère spécialisé en management et protection des données à caractère personnel de l'ISEP, elle a réalisé sa thèse professionnelle sur le thème de la communication du dossier médical. Un sujet qui renvoie naturellement à la protection des données personnelles mais aussi au domaine de l'archivage électronique.

■ Lire la suite : <http://www.cecurity.com/site/PubArt201001.php>

ECONOMIE DES DONNEES PERSONNELLES

Est-il possible de vendre de la *privacy* ?

En 2000 de jeunes sociétés américaines avaient l'ambition de se développer sur le marché des technologies et services de protection des données personnelles. 10 ans plus tard, force est de constater que le succès n'est pas au rendez-vous. Pourquoi les utilisateurs ne sont-ils pas prêts à payer pour la *privacy*, s'interroge Declan McCullagh ? Une première explication résiderait dans l'évolution des normes sociales qui font que, désormais, le partage des données personnelles apparaît comme quelque chose de plus naturel. C'est globalement la thèse avancée par le patron de Facebook. En outre, on constate que les technologies de protection des données personnelles qui ont rencontré le succès reposent sur des initiatives non marchandes à l'instar du réseau de communication anonyme Tor. L'explication la plus convaincante est peut-être celle de Jim Harper du Cato Institute qui estime que la *privacy* est d'un point de vue économique un bien intermédiaire, c'est-à-dire un composant qui doit figurer par construction dans le produit fini. Pour illustrer son propos, il utilise l'image suivante : les gens qui achètent une maison ne vont pas en plus faire l'effort d'aller acheter une cheminée ; en revanche, ils peuvent considérer comme normal que la maison dispose d'une cheminée.

Source : Cnet – Date : 28 janvier 2010 – Auteur : Declan McCullagh

■ Lien de l'article (en anglais) : http://news.cnet.com/8301-13578_3-10443575-38.html

Croisement des fichiers clients dans les télécom

Free va devenir le quatrième opérateur de téléphonie mobile et l'on imagine qu'il aura tout intérêt à proposer à son importante base d'abonnés Internet des offres sur son nouveau métier. L'Arcept, que l'on a coutume de présenter comme « le gendarme des télécoms » prend les devants et indique que cette question du croisement des fichiers clients n'est pas de sa compétence mais de celle de l'Autorité de la concurrence. A ce stade, il n'est pas encore question de la Cnil.

Source : Réseaux-Télécom – Date : 3 février 2010 – Auteur : Jean Pierre Blettner

■ Lien de l'article : <http://www.reseaux-telecoms.net/actualites/lire-quadruple-play-ca-chauffe-autour-du-croisement-des-fichiers-de-clients-21533.html>

Bing : anonymisation de l'adresse IP après 6 mois

Le feuilleton de la durée de conservation des données personnelles pour les moteurs de recherche vient de connaître un nouvel épisode. Le 18 janvier 2010, Microsoft a annoncé qu'elle allait désormais procéder à l'anonymisation de l'adresse IP au bout de six mois contre dix-huit mois précédemment. Cette mesure s'appliquera dans les douze à dix-huit mois à venir et concernera les utilisateurs du moteur de recherche Bing dans le monde entier. Le communiqué officiel de la Cnil relève du bulletin scolaire pour élève moyen : en substance, en progrès mais peut mieux faire. Alex Türk, le président de la Cnil, défend naturellement cette position – « *cela ne suffit pas* » - mais ajoute une formule choc un peu moins policée : « *Microsoft a changé la donne. C'est une pierre dans le jardin de Google* ». On pourra également souligner que cette décision vient apporter de l'eau au moulin de ceux qui défendent que l'adresse IP est bien une donnée à caractère personnel. Le mot de la fin revient à la Cnil qui estime, à l'occasion de cette annonce, que « (...) *la protection des données et de la vie privée*

est devenue, sous l'impulsion des autorités de protection des données européennes, un véritable instrument concurrentiel ».

Sources : Le Point – Date : 19 janvier 2010 – Auteur : Gueric Poncet

- Lien de l'article : <http://www.lepoint.fr/actualites-technologie-internet/2010-01-19/vie-privee-alex-turk-cnill-microsoft-a-change-la-donne/1387/0/415074>
- Le communiqué de la Cnil : <http://www.cnil.fr/la-cnill/actu-cnill/article/article/2/microsoft-reduit-les-durees-de-conservation-des-adresses-ip-un-pas-en-avant-mais-peut-mieux-fai/>
- La communication de Peter Cullen de Microsoft (en anglais) : <http://microsoftontheissues.com/cs/blogs/mscorp/archive/2010/01/18/microsoft-advances-search-privacy-with-bing.aspx>

ADMINISTRATION ELECTRONIQUE

La santé en ligne vue par les conservateurs britanniques

Selon les sondages en ce début d'année 2010, David Cameron, chef du parti conservateur possède de fortes chances d'être le prochain Premier ministre britannique. Son programme est donc particulièrement pris au sérieux notamment pour ce qui concerne la e-santé. L'objectif des conservateurs est de faire en sorte que les individus puissent gérer leurs données de santé en ligne de la même façon qu'ils gèrent déjà leurs informations bancaires. Le patient serait ainsi responsable de son propre dossier de santé et il pourrait recourir à l'hébergeur (privé) de son choix. Il est également prévu que soient diffusées en ligne des informations détaillées sur le niveau de performance des hôpitaux et même des médecins.

Source : Smart Healcare.com – Date : 4 janvier 2010

- Lien de l'article (en anglais) : <http://www.smarthealthcare.com/david-cameron-online-health-records-conservatives-04jan10>

25 propositions pour relancer l'administration électronique

Le rapport « Amélioration de la relation numérique à l'utilisateur » a été rendu public le 12 février 2010. Partant d'un état des lieux mitigés sur l'administration numérique française en 2009, les 8 experts auteurs du rapport avancent 25 propositions et préconisent pour chacune d'elles un calendrier de mise en œuvre. Certaines des pistes évoquées sont particulièrement détonantes comme celle qui consisterait à diminuer par dix le nombre de sites en .gouv.fr (de 400 à 40). On y trouve également des mesures comme la proposition d'un support d'authentification et de signature électronique (proposition 5), le recours facilité aux documents numérisés (proposition 8), la généralisation du recours aux factures électroniques (proposition 11) ou encore l'adaptation des services numériques actuels aux médias mobiles (proposition 25).

Il est également intéressant de lire ce rapport en découvrant les thèmes qui y figurent peu. La question de la protection des données personnelles est abordée discrètement alors qu'il s'agissait d'un point crucial il y a dix ans lorsqu'on abordait la stratégie de la sphère publique en matière d'e-administration. Faut-il y voir une conséquence de l'évolution des normes sociales en matière de vie privée pour reprendre la thèse controversée de Mark Zuckerberg, le PDG de Facebook ?

- Lire le rapport (44 pages) : <http://www.cio-online.com/fichiers/telechargement/rapport-amelioration-de-la-relation-numerique-entre-usagers-et-administration.pdf>

JURIDIQUE

La Cnil encadre les éthylotests antidémarrage

Des éthylotests antidémarrage vont équiper progressivement la totalité du parc des bus scolaire, soit près de 61 000 véhicules concernés d'ici l'échéance du 1^{er} septembre 2015. La Cnil a souhaité encadrer la mise en œuvre du dispositif. Ainsi l'employeur des chauffeurs pourra uniquement savoir si

le résultat de l'alcotest a été positif ou négatif sans connaître le résultat exact du taux d'alcoolémie. La Cnil justifie sa position en indiquant que la solution a une finalité préventive et non disciplinaire.

Sources : Le Figaro – Date : 4 janvier 2010 – Auteur : Angélique Négroni

- Lien de l'article : <http://www.lefigaro.fr/actualite-france/2010/01/02/01016-20100102ARTFIG00608-des-ethylotests-dans-les-bus-scolaires-en-fevrier-php>
- Le communiqué de la Cnil : <http://www.cnil.fr/la-cnil/actu-cnil/article/article/2/transport-denfants-test-dalcoolemie-au-demarrage/>

Parution du premier Index du droit d'accès

Depuis 1978, la loi informatique et libertés permet à toute personne d'exercer son droit d'accès. En justifiant de son identité elle a ainsi le droit d'interroger le responsable d'un fichier ou d'un traitement de données personnelles pour savoir s'il détient des informations sur elle, et le cas échéant d'en obtenir communication. Dès 1970, une loi américaine – *Fair Credit Reporting Act* – consacrée à l'information de solvabilité des emprunteurs avait institué ce droit.

Bien des années plus tard il est intéressant de vérifier si ce droit est correctement appliqué. C'est l'objectif de l'Index du droit d'accès réalisé par l'AFDCP (Associations des Correspondants Informatiques et Libertés) en association avec le mastère spécialisé management et protection des données à caractère personnel de l'ISEP. Sur 207 organismes privés et publics sollicités, le taux de réponse atteint pratiquement les deux-tiers avec cependant de fortes disparités sectorielles. Avec 28% de réponses le secteur Internet / Réseaux sociaux fait figure de cancre. Plus inquiétant, sur le plan qualitatif de nombreuses réponses sont largement à côté de la plaque. Moins de 20% des réponses reçues ont été jugées totalement satisfaisantes. La prochaine édition annuelle de l'Index permettra de mesurer les éventuels progrès réalisés.

- En savoir plus sur l'Index AFDCP du droit d'accès : <http://www.afcdp.net/A-l-occasion-de-la-journee>

« Privacy by Design », un nouveau principe juridique ?

Les grands principes de la réglementation informatique et libertés, apparus dans les années 70, restent d'une complète actualité. Il conviendrait cependant d'introduire un nouveau principe pour tenir compte de l'évolution des technologies et des risques associés en matière d'atteinte à la vie privée. Telle est la conviction des principales autorités européennes en charge de la question. Même en France, on risque fort d'utiliser le terme anglais très concis pour parler de ce nouveau principe : *Privacy By Design*. La traduction a cependant le mérite de correspondre à une définition complète : « *prise en compte du respect de la vie privée dès la conception* ». Le G29, qui regroupe les Cnil européennes, dans un rapport adopté le 1^{er} décembre 2009, souligne que ce nouveau principe s'appliquerait non seulement aux responsables de traitements mais également aux concepteurs de technologies. Il précise que ce principe « *devrait être défini de manière neutre sur le plan technologique pour qu'il puisse durer longtemps (...)* ». Viviane Reding, commissaire européen responsable de la société de l'information, estime que la mise en œuvre du principe *Privacy By Design* serait un facteur de confiance et aurait donc un impact positif sur le plan économique.

- Le discours de Viviane Reding, le 28 janvier 2010 (en anglais) : <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/16&format=PDF&aged=0&language=EN&guiLanguage=fr>
- Le rapport conjoint du G29 et du groupe de travail police et justice (32 pages) : http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp168_fr.pdf
Le thème *Privacy by Design* y est abordé des pages 13 à 17

ARCHIVAGE ET DEMATERIALISATION

Le Royaume-Uni se penche sur l'archivage du web

The British Library, la Bibliothèque Nationale du Royaume-Uni, s'inquiète des millions de pages web perdues et de celles qui le seront à l'avenir en l'absence d'une capacité à « aspirer » ces contenus même si l'on ne prend en compte que les sites à accès gratuit. Internet devient, au détriment du papier, la forme dominante de publication au Royaume-Uni. Un tiers des travaux publiés le sont désormais exclusivement en ligne. Le ministère prévoit qu'à l'horizon de 2016 le pays hébergera 15 millions de sites et que the British Library ne pourra archiver qu' 1% d'entre eux. Une autre façon d'aborder le débat actuel sur la prétendue « fin du droit à l'oubli ».

Source : Kable (d'après The Guardian) – Date : 4 janvier 2010

■ ■ ■ Lien de l'article (en anglais) : <http://www.kable.co.uk/copyright-library-web-archiving-culture-hodge-4jan10>

Réutilisation des archives en ligne

« (...) si les archives remplissent à présent un incomparable service en ligne de diffusion du patrimoine, le tournant de la réutilisation n'est pas encore anticipé juridiquement. » écrit Lionel Maurel au terme de l'étude qu'il a menée sur les conditions de réutilisation des contenus numériques diffusés en ligne par les services d'archive. « Pourtant, poursuit-il, au regard des pratiques du web, c'est certainement le grand enjeu de la numérisation qui attend les institutions culturelles dans les prochaines années, et il ne sera bientôt plus possible de concevoir la numérisation uniquement en termes de mise en ligne des documents sur un site. »

Sources : S.I.Lex – Date : 26 janvier 2010 – Auteur : Lionel Maurel

■ ■ ■ Lien de l'article : <http://scinfolex.wordpress.com/2010/01/26/archives-en-ligne-une-etude-des-conditions-de-reutilisation/>

IDENTITÉ NUMÉRIQUE

Carte d'identité avec visage à 360 C°

Une petite vidéo étonnante sur un prototype de nouvelle carte d'identité électronique. Associant puce RFID et technologie d'affichage OLED (diode électroluminescente organique en français), elle permet de visualiser la photo du titulaire de la carte à 360 C°.

Source : filrfid.org – Date : 20 janvier 2010

■ ■ ■ Lien de l'article : <http://www.filrfid.org/article-nouvelle-carte-d-identite-oled-et-rfid-au-menu-43304562.html>

Lancement du label IdéNum

Le Secrétariat d'Etat à l'économie numérique a annoncé le lancement d'idéNum, certificat d'identification pouvant être stocké sur un support externe (clé USB, téléphone mobile, ...) afin de donner accès à de nombreux services en ligne publics ou privés. L'ambition, selon les termes de Nathalie Kosciusko-Morizet, est de mettre fin « au cauchemar des 1001 mots de passe ». Le premier prototype de cette initiative – assez curieusement présentée comme un « label » – devrait être disponible pour la fin de 2010 avant une généralisation envisagée en 2011.

Très rapidement les premières critiques ont été formulées : risque de défiance de nombreux internautes devant tout ce qui est sensé être « garanti par l'Etat », solution exclusivement franco-française, incertitude sur le modèle économique, ... Plus fondamentalement, on peut se demander si IdéNum ne remet pas en cause le projet de carte d'identité électronique annoncé de longue date et dont l'un des avantages pour l'utilisateur résidait dans sa capacité à favoriser l'authentification sécurisée en ligne.

Sources : ZDNet – Date : 2 février 2010

■ Lien de l'article : <http://www.zdnet.fr/actualites/informatique/0,39040745,39712667,00.htm>

Les Inrocks.com – Date : 3 février 2010 – Auteur : Chloé Woitier

■ Lien de l'article : <http://www.lesinrocks.com/actualite/actu-article/t/1265191921/article/carte-didentite-virtuelle-idenum-pas-nee-et-deja-decree/>

A DECOUVRIR

Vote sur internet : sécurisation sans chiffrement

L'Atelier BNP Paribas présente de façon synthétique les travaux de deux chercheurs de l'université d'Oklahoma en matière de sécurisation du vote par Internet. La méthode repose sur la partition de chaque vote sur de multiples serveurs. La solution envisagée n'implique plus de recourir au chiffrement alors que c'est aujourd'hui la méthode préconisée par la Cnil et utilisée par les plateformes de vote électronique des principaux prestataires. Le mécanisme de la partition des votes permet en outre à l'électeur de changer d'avis au cours de la période de scrutin. Cette particularité permettrait de résoudre la question jusqu'ici insoluble de l'absence d'isoloir dans le cadre du vote à distance avec la crainte associée de vote sous pression. Inversement, dans le contexte français, une telle possibilité introduirait une innovation tout à fait étrangère à notre culture démocratique : la possibilité pour l'électeur de changer d'avis en fonction du déroulement de la campagne électorale.

Source : L'Atelier – Date : 13 janvier 2010

■ Lien de l'article : <http://www.atelier.fr/securite/10/13012010/vote-internet-securiser-partition-changer-d-avis-serveurs--39215-.html>

PCI DSS et la protection des données carte bancaire

Initié par les grands acteurs internationaux de la carte bancaire (Visa, Mastercard, American Express, ...), le *Payment Card Industry Security Standards Council* (PCI DSS) est un référentiel de sécurisation de données carte bancaire applicable aux commerçants. Le PCI DSS prévoit de nombreux points de contrôle et impose notamment l'interdiction de conservation ou le chiffrement de certaines données. Thierry Autret, RSSI du GIE Carte Bancaire, indique que ce référentiel n'a pas été pensé à l'origine pour la protection des données à caractère personnel mais qu'il peut être source d'inspiration dans la mesure où le numéro de carte bancaire est une donnée indirectement nominative.

■ En savoir plus sur PCI DSS avec le dossier technique du Clusif paru en 2009 (46 pages) : <http://www.clusif.fr/fr/production/ouvrages/pdf/CLUSIF-2009-PCIDSS-Une-presentation.pdf>

■ En juin 2003, la Cnil avait rendu public une recommandation relative au même sujet : <http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/13/>

EVENEMENTS

La Fédération Nationale des Tiers de Confiance à Documentation

Dans le cadre du Salon Documentation à Paris (CNIT), la Fédération Nationale des Tiers de Confiance (FNTC) organise une conférence le 18 mars 2010 à 12h30 sur le thème « *e-archivage, coffre-fort électronique, e-paie, e-facture, les tiers de confiance en parlent* ». Alain Borghesi, vice Président de la FNTC et PDG de Cecurity.com figure parmi les intervenants.

■ En savoir plus : http://www.documentation.fr/site/FR/Zoom_Evenement,C1578,I1114,Zoom-22520716324df8a6c4300f57b4763d37,FromOut-ListGlob,TypeOut-Conf.htm?KM_Session=f8ea383613425408513e9b6538688565

Pour nous contacter, nous faire parvenir vos critiques ou suggestions, envoyez un message à :
<mailto:news@cecurity.com>

Reproduction autorisée sous réserve de mention de la source : « Cecurity.com »

Pour vous désinscrire, envoyez un message à <mailto:news@cecurity.com> en
indiquant « DESABONNEMENT » dans l'objet du message.

Newsletter Cecurity.com -
L'actualité de la privacy et de la dématérialisation
Email news@cecurity.com
Web <http://www.cecurity.com>
Tel 01 56 43 37 36
