Principauté de Monaco

DROIT D'@CCÈS

Le courrier de la Commission de Contrôle des Informations Nominatives - N° 7

28 JANVIER 2011

JOURNÉE EUROPÉENNE DE LA PROTECTION DES DONNÉES

ÉDITO

Avec l'explosion des smartphones et l'engouement pour les nouvelles technologies, l'intérêt de protéger notre vie privée doit désormais être pris au sérieux. Tout simplement, parce que **des personnes peuvent être valablement licenciées pour s'être exprimées sur leur employeur par le biais d'un réseau social :**

- les mails peuvent être lus et interprétés,
- nos téléphones en disent plus sur nous qu'une simple autobiographie,
- nos voitures retiennent nos incivilités...

La CCIN, autorité de protection des informations nominatives, travaille pour faire en sorte que nouvelles technologies ne riment pas avec surveillance, harcèlement, contrôle des individus. Le meilleur allié de la vie privée et de la protection des informations nominatives demeure toutefois la personne concernée, qui doit veiller à l'utilisation de ses données personnelles.

SOMMAIRE

STREET-VIEW **EN PRINCIPAUTÉ : DES PRISES DE VUE EN NOVEMBRE 2010** p.2

MAÎTRISE DES ÉNERGIES ET PROTECTION DES INFORMATIONS NOMINATIVES p.3

RÉSEAUX SOCIAUX ET PROTECTION DES INFORMATIONS NOMINATIVES p.4

L'INFORMATIQUE, LA TÊTE DANS LES NUAGES DES DONNÉES PERSONNELLES À BALISER p.6

L'INVASION DES PUCES p.7

CE QU'ILS DISENT DE NOS VIES PRIVÉES p.8

À Cagnes-sur-Mer : souriez... vous êtes vidéo-verbalisés !

"Constater par caméra interposée un stationnement irrégulier est désormais possible et parfaitement légal (...) **les PV multimédia vont pouvoir fleurir virtuellement** (...) sur les pare-brises des véhicules garés en double file, sur un passage piéton..."

Monaco-Matin **– 9 mars 2010**

Les cartes bancaires piratées vendues 2,30 euros sur le Web.

"Le marché des cartes piratées a son argus. Le centre anti-fraude RSA vient d'en publier quelques prix : (...) il faut compter entre **1,15 et 2,30 euros pour obtenir les informations d'une carte bancaire volée.** Pour ce prix, le pirate fournit le numéro d'identification à 16 chiffres, le cryptogramme à 3 chiffres qui figure au dos de la carte, sa date d'expiration ainsi que l'adresse et le nom de son véritable propriétaire (...). Avec ces informations, il est alors facile de réaliser un achat sur presque n'importe quel site."

Monaco-Matin **– 9 mars 2010**

Dans le Monde, nos lectures suivies à la page.

"Pour rester maîtres de nos lectures, il va falloir le demander." "Apple, Google et Amazon - ainsi que la Fnac bientôt avec son fnacbook, Chapitre.com (...) savent très bien ce que vous lisez. Ils savent qui vous êtes (...). Ils connaissent tous les livres que vous consultez en ligne ou achetez (...). Ils connaissent le nom des fichiers contenus dans vos machines. Ils savent quand vous achetez un titre. Comment vous l'achetez. Où vous en êtes dans votre lecture". Grâce aux outils de géolocalisation "transmis via les applications de nos outils mobiles qui se moquent ouvertement de notre vie privée" ils savent "où vous l'avez lu. Ils peuvent donc savoir si vous lisez chez vous, dans les transports, au bureau, ailleurs, mais ils peuvent aussi le déduire de vos horaires de consultations (...)." "Tout cela n'a qu'une finalité marketing. Mais ces données ne servent pas qu'aux enseignes auxquelles vous achetez ces produits. Rien ne les empêche de revendre ces données, notamment aux éditeurs, mais également à d'autres bases marketing".

> « ILS SAVENT QUI VOUS ÊTES. »

Le Monde technologique **- 5 novembre 2010**

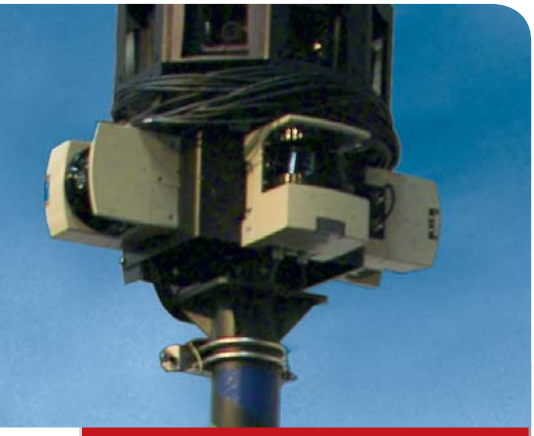
USA : les autorités assurant la sécurité nationale américaine souhaitent pouvoir mettre sur écoute les messages électroniques.

"La sécurité nationale américaine voudrait imposer de nouvelles règles en matière de communication sur Internet. Selon le New York Times, **les autorités souhaitent pouvoir mettre sur écoute les messages envoyés avec un BlackBerry, sur Skype ou sur Facebook,** qu'ils soient ou non chiffrés. Un projet de loi pourrait être examiné par le Congrès dès l'année prochaine (...). Nous parlons d'écoutes autorisées légalement", a indiqué au quotidien américain Valérie Caproni, conseillère générale du FBI. Quant aux défenseurs des libertés individuelles, ils craignent un verrouillage d'Internet".

01net **– 28 septembre 2010**

STREET-VIEW EN PRINCIPAUTÉ

Des prises de vue en novembre 2010.



Les clichés de la Principauté pris par les voitures Google en novembre 2010 ne sont pas en ligne. Si la CCIN reste vigilante, il vous appartiendra néanmoins de vérifier les images diffusées.

Street-View à Monaco... c'était en novembre 2010 !

Google Street-View est un service lancé en mai 2007 qui permet aux internautes de naviguer virtuellement dans les rues de grandes villes, avec une vue à 360 degrés. Une voiture équipée de caméras circule en prenant des images. Un logiciel de Google les assemble pour donner une impression de continuité.

À l'origine, seules quelques villes américaines étaient accessibles, puis rapidement, le service s'est étendu à d'autres pays de l'U.E., de l'Asie, et de l'Océanie. Ce service permet à une personne de se rendre virtuellement dans les lieux les plus reculés depuis son salon, mais aussi de s'orienter plus rapidement dans un endroit donné.

> « *GOOGLE STREET-VIEW* S'EST RÉVÉLÉ ÊTRE PORTEUR DE TROUBLES À LA VIE PRIVÉE. »

Présenté à l'origine comme une avancée technologique, *Google Street-View* s'est révélé être porteur de troubles à la vie privée au regard, par exemple, des prises de clichés, de la nature des informations réellement collectées lors du passage des "voitures Google", ou encore de la conservation des données personnelles.

Souriez, vous êtes googlés !

Il arrive que les clichés de *Google Street-View* dévoilent le visage des personnes photographiées, ainsi que des plaques d'immatriculation de voiture et ce malgré les "floutages" mis en place. En 2008, un couple de Pennsylvanie a porté plainte contre Google après avoir trouvé des images de son foyer prises dans une voie clairement marquée comme "propriété privée". Ils ont été indemnisés ... 1 $ symbolique. Début 2010, un Finlandais a été photographié par surprise, le pantalon baissé, assis sur une balancelle dans son jardin. Sans parler des enfants qui jouent devant leur maison ou dans les jardins publics, etc.

Pour s'opposer : écrire à Google.

En cas de défaillance du système de floutage, l'internaute qui constate que des informations permettant de l'identifier directement ou indirectement ont été publiées peut faire flouter le cliché.

Il lui appartient de le signaler en cliquant sur **"signaler un problème"** dans le coin inférieur gauche de l'image *Street-View*, et en remplissant le formulaire qui apparaît.

Dès que la demande est contrôlée, l'image est normalement floutée... mais pas supprimée. L'image restera telle quelle dans la base de données car son utilisation première est d'être un élément de cartographie.

L'Allemagne est le seul pays où les habitants ont eu la possibilité de demander le floutage de leur domicile avant le lancement du programme.

La collecte parallèle de données Wi-Fi... qui fâche.

En France, au Royaume-Uni, en Espagne (...), les voitures *Street-View* ont collecté, via des antennes radio, des données Wi-Fi lors du passage des voitures. Parmi ces données figurent le nom d'identification des réseaux Wi-Fi rencontrés et les MAC adresses des routeurs, mais aussi des échantillons de données qui circulaient sur le réseau Wi-Fi ouvert, comme des mots de passe et des extraits de courriels...

En novembre 2010, après la déclaration fracassante de son PDG invitant les personnes qui n'apprécient pas que leur domicile ou leur entreprise figure sur *Street-View* à "déménager", la société américaine s'engageait à désactiver les antennes, à flouter les visages et plaques d'immatriculation des personnes et à retirer les clichés d'habitations à la demande de leur propriétaire.

MAÎTRISE DES ÉNERGIES ET PROTECTION DES INFORMATIONS NOMINATIVES

La rencontre de la protection de l'environnement et de la protection de la vie privée.

Le compteur électrique "intelligent" : technologie écolo ou mouchard social ?

A l'occasion de la 32ème Conférence Internationale des Commissaires à la Protection des Données Personnelles qui s'est déroulée en novembre 2010 en Israël, Michiel KARSKENS a rappelé les dangers que les compteurs intelligents peuvent présenter pour la vie privée.

Ces compteurs intelligents permettent de surveiller avec une grande précision la consommation électrique d'un foyer, ou bien sa consommation en gaz ou en eau. Ils permettent de connaître précisément quels sont les appareils les plus gourmands, et ce presque en temps réel, souvent de demi-heure en demi-heure. Ils peuvent ainsi nous permettre de faire à la fois des économies et d'adopter des habitudes de consommation plus écologiques.

Toutefois, le compteur intelligent représente un nouveau danger pour la vie privée des consommateurs. Le fournisseur d'énergie pourrait déduire, à partir des informations précises sur la consommation d'un ménage, des informations d'ordre privé comme : le nombre d'habitants au foyer, leurs âges, leurs habitudes (habitudes hygiéniques, heures des repas, heures du coucher, etc).

Déjà, lors de la 31ème Conférence Internationale des Commissaires à la Protection des Données Personnelles qui s'était tenue à Madrid en 2009, Elias QUINN, du Centre pour la Sécurité Energétique et Environnementale de l'Université du Colorado, avait pointé le risque que les compagnies électriques vendent les données collectées par les compteurs intelligents.

> "LE COMPTEUR INTELLIGENT REPRÉSENTE UN NOUVEAU DANGER POUR LA VIE PRIVÉE DES CONSOMMATEURS."

Le 14 octobre 2010, la CNIL a émis des recommandations afin de limiter les atteintes à la vie privée et aux libertés par ces dispositifs innovants en France. Consciente de ces risques, la Commission de Contrôle des Informations Nominatives demeure vigilante à la mise en place de ces compteurs à Monaco.

Aux États-Unis, Intelligrid offre une gestion personnelle des consommations.

"Dans l'État de Washington, un réseau électrique, [appelé Intelligrid], propose à quelques 300 foyers une alimentation énergétique intelligente. Le principe : **le prix du courant n'est plus fixe, mais varie en fonction de l'offre et de la demande** et l'usager, informé de ces variations, peut désormais décider à quel moment il souhaite faire fonctionner son lave-linge, par exemple. Ayant la main sur le système, il peut à tout moment modifier ses préférences"*... pourrait-on vérifier et contrôler par ce biais le comportement éco-citoyen du consommateur ?

***Source : 26 août 2008 (www.goodplanet.info)**

RÉSEAUX SOCIAUX ET PROTECTION DES INFORMATIONS NOMINATIVES

Lorsque nos propos, nos comportements échangés avec "nos amis" se retrouvent sur la place publique, jugés, déformés, sortis de leur contexte, sortis de la sphère qui aurait dû être la leur...

Un réseau social est fondé sur l'échange, voire sur la confiance.

Un réseau social peut être défini comme "une communauté d'individus ou d'organisations en relation directe ou indirecte, rassemblée en fonction de centres d'intérêts communs, comme par exemple les goûts musicaux, les passions ou encore la vie professionnelle. Sur Internet, de nombreux sites sont à la source de la création de ces réseaux, à l'image de LinkedIn et 6nergies dans le monde professionnel, ou encore MySpace, Copains d'avant ou Flickr dans le grand public".

Journaldunet.com

La force du réseau social : la liberté d'expression.

La liberté d'expression est un droit consacré. Ainsi, dans la Constitution monégasque, l'article 23 dispose que *"la liberté des cultes, celle de leur exercice public, ainsi que la liberté de manifester ses opinions en toutes matières sont garanties, sauf la répression des délits commis à l'occasion de l'usage de ces libertés"*. La Convention de Sauvegarde des Droits de l'Homme et des Libertés Fondamentales du Conseil de l'Europe lui consacre son article 10. Ainsi *"Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontière (...)"*.

> « CE DROIT À LA LIBERTÉ D'EXPRESSION EST UN DROIT FONDAMENTAL, CE QUI NE SIGNIFIE PAS QUE CE DROIT EST SANS LIMITE. »

Ce droit à la liberté d'expression est un droit fondamental, ce qui ne signifie pas que ce droit est sans limite. Dans ce sens *"l'exercice de cette liberté ne peut être limité que dans la mesure requise par le respect de la dignité de la personne humaine, de la vie privée et familiale, de la liberté et de la propriété d'autrui, du caractère pluraliste de l'expression des courants de pensée et d'opinion ainsi que par la sauvegarde de l'ordre public"* (article 1er de Loi n° 1.299 du 15 juillet 2005 sur la liberté d'expression publique).

Retour d'expérience de ceux qui y ont cru : licenciés pour des propos échangés sur Facebook.

Plusieurs salariés d'une entreprise de consultants avaient, sur leur page privée Facebook critiqué leur hiérarchie depuis leur domicile. Les propos publiés sur leur "***mur***" n'étaient pas accessibles à l'ensemble des utilisateurs mais seulement à leurs ***amis*** et ***aux amis des amis***, dont certains collègues.

L'un d'entre eux a fait une capture écran de la page et l'a transmise à leur employeur commun. Les salariés ont été licenciés pour *"faute grave"* sur le fondement de *"l'incitation à la rébellion et du dénigrement de l'entreprise"*.

Il avait été plaidé par les salariés qu'une discussion sur le ***"mur"*** Facebook relevait de la vie privée. Mais dans un jugement du 19 novembre 2010, le conseil des Prud'hommes de Boulogne-Billancourt a considéré que l'employeur n'avait pas *"violé la vie privée de ses salariés"*, les propos ayant été échangés *"sur un site social ouvert"*, et *"la page mentionnant les propos incriminés constitue un moyen de preuve licite du caractère bien-fondé du licenciement"*. Prenons acte et attendons que l'appel de cette décision nous en apprenne davantage...

Moralité : les amis de mes amis ne sont pas toujours mes amis, ou est-ce la définition du mot ***"ami"*** qu'il faudrait revoir dans sa version virtuelle.

...D'ici là, notons qu'il s'agit d'un "site social ouvert".

Les réseaux sociaux, de type "Facebook", ne sont pas des boîtes mail. **Lorsque l'on publie des propos sur un site social ouvert, ils appartiennent à la sphère publique.** Dans l'attente de l'arrêt de la Cour d'appel, il n'est pas inutile de vérifier le paramétrage de son compte Facebook, mais aussi des autres comptes d'autres réseaux. Il est possible de n'autoriser l'accès à ses données (ou certaines d'entre elles) qu'à ses "amis" ou un certain "groupe d'amis".

Candidat à un emploi ?

Une nouvelle tendance fait actuellement débat, celle des Directions des Ressources Humaines de percevoir les réseaux sociaux (Facebook, Twitter, LinkedIn, Viadéo...) aux fins de recueillir des informations sur les candidats à un emploi.
Le paramétrage du compte présente un intérêt notable, notamment lorsqu'il est mis en partage avec ses "amis". Cette précaution s'avère être primordiale lorsque le Directeur des Ressources Humaines qui examine le candidat, ne partage pas sa conception selon laquelle "Casimir" participe à la biodiversité. Il faut être prudent sur les contenus et les images partagés sur le net.

Les "murs" ont des oreilles.

Facebook a révolutionné l'univers des réseaux sociaux, voire la notion "d'ami". "L'ami Facebook" était jusqu'à présent bien pratique, se "cliquant", "s'invitant" se "supprimant" au gré de l'humeur du moment. Même dématérialisé, il peut être nuisible. La "demande d'amitié" sur Facebook est un art subtil et délicat pour qui veut accéder aux données personnelles de sa "cible".

Maman, j'ai reçu une invitation d'Harry Potter !

Pour qui en doute encore, Harry Potter n'est qu'un personnage de fiction. Il n'invite pas les enfants à faire des stages de magie après l'école. Les réseaux sociaux sont aussi ludiques pour les enfants que pour les parents. Il faut donc faire preuve de discernement.

À l'instar de Monsieur qui ignore toujours que la blonde incendiaire aux courbes ravageuses qui veut l'ajouter à sa liste d'amis s'appelle en réalité Gaston, hacker de profession, les enfants n'ont pas le recul nécessaire pour vérifier l'identité de leur interlocuteur. La charte Facebook dans sa version du 4 octobre 2010 dispose : "Vous n'utiliserez pas Facebook si vous avez moins de 13 ans". Dans la pratique de nombreux enfants utilisent Facebook, parfois sans l'encadrement nécessaire des parents.

> « IL EST NÉCESSAIRE DE PARAMÉTRER L'ACCÈS À L'INTERNET ET AUX SITES FRÉQUENTÉS PAR LES ENFANTS, DE POSER DES FILTRES, DE DIALOGUER AVEC EUX POUR LES INFORMER DES DANGERS DU NET. »

L'article 16 de la Convention internationale relative aux droits de l'enfant énonce que "l'enfant a le droit d'être protégé contre toute immixtion dans sa vie privée, sa famille, son domicile et sa correspondance, et contre les atteintes illégales à son honneur". La protection de l'enfant commence à la maison. Comme il faut faire attention lorsque l'enfant va jouer dehors, il faut être vigilant sur son utilisation des sites sociaux et plus généralement de l'Internet.

Il est nécessaire de paramétrer l'accès à l'Internet et aux sites fréquentés par les enfants, de poser des filtres, de dialoguer avec eux pour les informer des dangers du net.

Facebook ne vous oubliera jamais...

En 2009, Mark ZUCKERBERG, dirigeant du réseau social Facebook, avait tenté le passage en force d'une modification des conditions générales d'utilisation en introduisant un ovni juridique dans le ciel Internet : "La licence perpétuelle et mondiale". L'idée : Facebook disposait d'un droit de propriété sur l'ensemble des contenus (photos, messages, vidéos) publié sur le réseau social. Ce qui est à vous est à lui et ce qui est à lui est à lui, normal entre amis. **Facebook s'autorisait ainsi à maintenir les contenus même si l'expéditeur (donc le propriétaire des contenus) se désinscrivait.**

Devant les réactions hostiles des utilisateurs, le réseau social est revenu aux conditions initiales : "Nous avons reçu de nombreux commentaires relatifs à ces changements et à ce qu'ils signifient pour les gens et pour leurs informations. Sur la base de ces réactions, nous avons décidé de revenir à nos précédentes conditions d'utilisation".

Lorsqu'un réseau social modifie ses conditions générales, il en informe l'utilisateur. Avant de cliquer sur "oui" pour marquer son acceptation, il conviendrait de lire le texte. Même s'il s'agit d'Internet, c'est un contrat.

L'INFORMATIQUE, LA TÊTE DANS LES NUAGES...

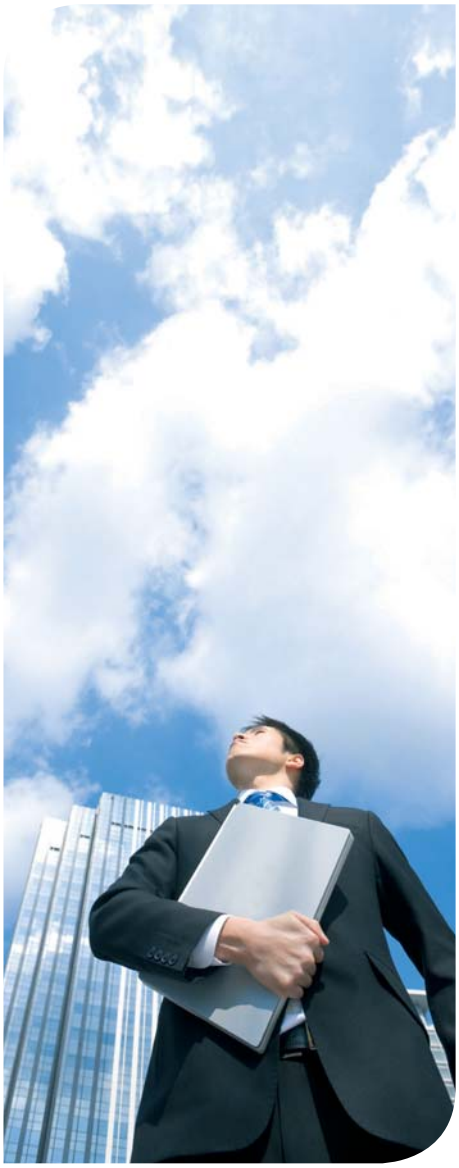
Des données personnelles à baliser.

Le Cloud Computing : le village dans les nuages.

Cloud Computing, "informatique dans les nuages", "informagique", ces expressions, hier énigmatiques, nous sont de plus en plus familières. Pour cause, Microsoft fait les louanges de ses derniers logiciels à grand renfort de slogans : "Destination le Cloud".

Le *Cloud Computing* consiste à externaliser sur des serveurs distants des traitements informatiques jusqu'ici localisés sur le poste utilisateur. Les utilisateurs ou les entreprises ne gèreront plus leurs serveurs informatiques, voire même les licences, mais accéderont à des services en ligne "à la carte" sans avoir à gérer l'infrastructure. Cela signifie que les applications et les données ne seront plus sur l'ordinateur local mais dans le Cloud, lui-même composé de serveurs distants tous interconnectés. L'accès au service s'effectue au moyen d'une application simple, comme le navigateur internet.

> “LE CLOUD COMPUTING CONSISTE À EXTERNALISER SUR DES SERVEURS DISTANTS DES TRAITEMENTS INFORMATIQUES JUSQU'ICI LOCALISÉS SUR LE POSTE UTILISATEUR.”



Le Green-Cloud : l'argument vert pour une version Green-IT.

Microsoft a publié un rapport très sérieux aux termes duquel il est expliqué l'impact particulièrement favorable du *Cloud Computing* sur l'environnement.

Le *Cloud Computing* permettrait de réduire l'empreinte carbone jusqu'à 90% par rapport à l'utilisation de serveurs internes. Le *Cloud Computing* au service de l'environnement, ce n'est plus le village dans les nuages... mais les Jardins de Babylone.

L'ONG Greenpeace dénonce toutefois les impacts négatifs de l'informatique en nuage dans son rapport 2010 : l'impact climatique du nuage de données (le "Cloud Computing") composé de fermes de serveurs et d'équipements télécom.

Ces conclusions sont à rapprocher d'un rapport intitulé "TIC et développement durable", publié par les Ministères de l'Industrie et de l'Environnement français en octobre 2008, qui met en lumière les préoccupations environnementales, notamment de ces centres de données : 40% de leurs consommations énergétiques sont liées à la climatisation des salles de serveurs. A surface identique, ils consomment 100 fois plus d'énergie au m^2 qu'un immeuble de bureaux. Selon ce rapport "si rien n'est fait, dans 25 ans, Internet consommera autant d'énergie que l'humanité toute entière en 2008".

Le droit à l'oubli, ou droit à une seconde chance : un mythe sur le Web ?

Le droit à l'oubli, droit de faire supprimer les informations qui portent sur vous, est l'enjeu de demain dans le "Cloud" : chacun y aura des milliers d'informations nominatives en transit. Chacune de ces informations sera dupliquée dans des milliers de fichiers, certains parfois oubliés de tous, non supprimés, non actualisés, errants dans des limbes numériques. La photo ridicule de ce fameux premier de l'an restera ancrée à jamais dans l'histoire numérique sans espoir de rédemption.

Le Cloud soulève des problématiques de sécurité générale des données et du réseau de l'entreprise.

Sans *Cloud Computing*, une entreprise peut mettre une partie de son réseau en local sans aucune connexion à internet pour des raisons de haute confidentialité, par exemple. Dans un schéma de *Cloud Computing*, elle devra toujours se connecter à Internet a minima pour accéder à ses applications.

Si l'entreprise perd le contrôle de l'implantation de ces données, elle perdra également la maîtrise de leur cycle de vie. En effet, où seront-elles physiquement hébergées ? Dans quel pays ? Quelles sont les garanties de récupération des données si elles se trouvent dans des pays non respectueux de la protection des données personnelles ?

Qu'en sera-t-il de la sécurité juridique ? Dans l'affaire Yahoo en 2000, Yahoo Inc. avait été attaqué et condamné en France par le TGI de Paris pour avoir hébergé une vente aux enchères d'objets du III[ème] Reich. L'exequatur de la décision n'a jamais été validée aux États-Unis pour des raisons de non conformité au premier amendement garantissant la liberté d'expression. La complexité du Cloud fera que la responsabilité et la question de la territorialité des tribunaux compétents ne pourront être véritablement définies que par la voie contractuelle. Entre impunité et forum shopping, le droit de la protection des données personnelles trouvera-t-il des îlots d'effectivité ?

Faudra-t-il se contenter de la seule promesse de responsabilisation des acteurs du Cloud ?

> « SI L'ENTREPRISE PERD LE CONTRÔLE DE L'IMPLANTATION DE CES DONNÉES, ELLE PERDRA ÉGALEMENT LA MAÎTRISE DE LEUR CYCLE DE VIE. »

La prolifération des puces RFID.

On en parle de plus en plus mais personne ne la connaît vraiment. Révolution technologique, cette puce correspond à une petite balise électronique insérée dans des objets ou des marchandises pour envoyer tous types de renseignements à travers des ondes radio à un lecteur. Cette collecte d'informations permet aux entreprises de gérer leurs stocks de marchandises, mais également de suivre les habitudes de consommation de leurs acheteurs.

Depuis 2007, on assiste à une prolifération inquiétante de cette puce qui a soulevé questionnements et inquiétudes des consommateurs. Les questions les plus récurrentes concernent le respect des données à caractère privé :

- À partir de croisements de données entre fournisseurs ou encore avec d'autres informations disponibles par la géolocalisation de nos téléphones portables, les puces de nos cartes bancaires pourraient permettre l'établissement de profils de consommation très détaillés ;
- Les puces RFID sont illisibles, pour ne pas dire invisibles au consommateur. On ne sait rien, non seulement des informations contenues dans la puce, mais aussi de l'exploitation qui en sera faite ultérieurement ;
- Pourra-t-on désactiver ces puces après un passage en caisse ?

Sans bruit, la puce RFID s'est d'ores et déjà infiltrée dans notre quotidien : sur notre carte de transport, sur l'autoroute, à la bibliothèque, sur nos vêtements, sur nos animaux... Elle nous suit ... elle nous connaît ... elle nous surveille.

Invasion de puces en cours : les puces RFID sont dans vos poches... Comment sont-elles ? Qui sont-elles et que disent-elles de vous ?

NeoWare... trace les étudiants !

En janvier 2010, l'université de Toulon a testé auprès de 200 étudiants volontaires un produit multipass, dénommé *NeoWare* et présenté lors des Assises de la Sécurité à Monaco en octobre 2010. Il permet de pointer à l'entrée des salles de cours, de télécharger les cours, de payer à la cantine avec un système Monéo, de gérer les livres empruntés à la bibliothèque, de disposer de sa carte de transport... un support de la taille d'un porte-clés pour plusieurs utilisations. Une réussite auprès des étudiants... Mais serait-il possible de savoir qui est allé en cours, à quelle heure l'étudiant est arrivé, s'il a pris connaissance des cours, s'il a pu plagier des documents ?

Sera-t-il finalement possible de surveiller une personne dans ses moindres faits et gestes, dans ses moindres déplacements, dans ses lectures, dans ses habitudes de vie ? Est-il acceptable de permettre ce genre d'utilisation... de laisser faire ?

CES PERSONNALITÉS DE RENOMS OBSERVENT ET APPELLENT À LA VIGILANCE.

Chaque jour, dans le domaine des nouvelles technologies et de leurs utilisateurs, nous utilisons les applications que leurs sociétés ont développé. Elles sont devenues des incontournables dans notre vie professionnelle et quotidienne. Elles sont "nos amies". Mais que disent leurs créateurs de nous ?

"Si je regarde suffisamment vos messages et votre localisation, et que j'utilise une intelligence artificielle, je peux prévoir où vous allez vous rendre. Montrez-nous quatorze photos de vous et nous pourrons vous identifier. Vous pensez qu'il n'y a pas quatorze photos différentes de vous sur Internet ? Il y en a plein sur Facebook !"

"La seule manière de gérer ce problème est une vraie transparence, et la fin de l'anonymat. **Dans un monde où les menaces sont asynchrones, il est trop dangereux qu'on ne puisse pas vous identifier d'une manière ou d'une autre.** Nous avons besoin d'un service d'identification personnel. Les gouvernements le demanderont".

***PDG de Google, M . SCHMIDT* – Conférence techonomy le 4 août 2010.**

Un doute, une question : "Google mon ami" me donne la réponse ! ...En échange, il sait tout de moi.

"Le web est essentiel, non pas seulement pour la révolution numérique, mais aussi pour la continuation de notre prospérité et même pour notre liberté. Comme la démocratie, il doit être défendu". Surveillance de l'Internet, censure d'informations, restriction d'accès aux sites sont autant de pratiques non conformes avec l'esprit du Web.

Quant aux sites de réseautage, "**plus vous entrez d'informations, plus vous vous verrouillez sur le site de réseau social que vous utilisez.** Votre site de réseautage social devient une plate-forme centrale, un silo de contenu fermé, qui ne vous donne pas le plein contrôle des informations que vous stockez en son sein".

Tim BERNERS-LEE
créateur du concept du web en 1990, observe son évolution.

"**Nous risquons d'entrer dans une société où il ne serait jamais plus possible de cacher aux autres où et avec qui nous nous trouvons.** Ce serait une société invivable". "Mais le plus grave est que la population, les individus, ne se sentent pas en danger et trouvent [les nouvelles technologies] intéressantes".

***Alex TURK* – Président de la CNIL, les Assises de la Sécurité, Monaco, octobre 2010.**

"Les gens sont désormais à l'aise avec **l'idée de partager plus d'informations différentes, de manière plus ouverte et avec plus d'internautes** (...). La norme sociale a évolué. Les 350 millions d'utilisateurs du site n'attachent plus autant d'importance à la protection de leur données personnelles".

PDG de Facebook, Mark ZUCKERBERG
San Francisco, janvier 2010, à propos de la modification des paramètres de vie privée de son réseau social.

« NOUS RISQUONS D'ENTRER DANS UNE SOCIÉTÉ OÙ IL NE SERAIT JAMAIS PLUS POSSIBLE DE CACHER AUX AUTRES OÙ ET AVEC QUI NOUS NOUS TROUVONS. »

Papier issu de bois provenant de forêts gérées durablement - WWW.GROUPECOMPLUS.COM - 1210422-03

COMPOSITION DE LA COMMISSION :

Président : Michel SOSSO

Vice-Président : Me Jacques SBARRATO

Commissaires : Daniel BOERI, Patrick MEDECIN, Jacques ORECCHIA, Stéphanie VIKSTRÖM

SECRÉTARIAT GÉNÉRAL :

Secrétaire Général : Caroline PORASSO

Division Juridique : Céline ANSQUER, Benjamin AOUIZERAT, Anne-Fleur GRILLOT

Division Administrative : Emilie CAMPILLO, Isabelle GERTALDI

Division Informatique : Jean SISTI

Secrétariat : Aurélie CIAIS

COMMISSION DE CONTRÔLE DES INFORMATIONS NOMINATIVES

Bureau 409 – Bloc B – "Gildo Pastor Center" - 7 rue du Gabian – MC 98000 MONACO
Téléphone : (+ 377) 97 70 22 44 - Fax : (+ 377) 97 70 22 45
E-mail : ccin@ccin.mc - Site Internet : www.ccin.mc
Les bureaux sont ouverts du lundi au vendredi de 9h00 à 12h30 et l'après-midi sur rendez-vous.