Districts français
Rotary international

Concours national 2012-2013

Promotion de l'éthique professionnelle

Conférence des grandes écoles

TIC et vie privée :

vers une révision de la valeur de l'information

Mot de passe : Ch0cO

Auteurs : Kevin Bourgeois et Barthélémy Cabouat, élèves ingénieurs en 1ère année

Relecteur : Cendrine LE LOCAT, responsable développement durable et solidaire

Télécom Bretagne

Technopôle Brest-Iroise
CS 83818
29238 Brest Cedex 3
France

TIC et vie privée :

vers une révision de la valeur de l'information

Mot de passe : Ch0cO

Angle d'approche

Après s'être plongé deux ans dans l'étude des sciences exactes, nous intégrons une école d'ingénieur. Nous y découvrons un monde complexe et passionnant qui suscite mille et une questions. Au terme de notre formation, nous serons immergés dans un monde multiforme. Or pour rester à la surface, nous devrons nous adapter aux demandes de notre employeur et du marché. Pris par la fièvre de l'enthousiasme, il n'en faudra pas moins garder en tête nos valeurs éthiques. Nous avons donc décidé de nous pencher dès aujourd'hui sur ces sujets capitaux, qui façonneront la société de demain. Nous avons grandi avec Internet et l'explosion des TIC. Certains de leurs formidables possibilités et de leur utilité, nous nous questionnons tout de même sur les implications des échanges de l'information dans un monde si différent de celui de nos parents. A l'heure où les cartes postales se sont virtualisées et les signatures numérisées, il est grand temps de s'interroger sur les répercussions des nouvelles technologies sur notre vie privée.

Résumé

L'usage presque systématique des TIC dans un cadre professionnel n'est pas sans risques. Afin de limiter les menaces qui peuvent se créer pour la vie privée des employés, il faut cadrer leur utilisation et prévenir les dérives potentielles. C'est dans ce contexte que l'éthique se place comme garde-fou contre la collecte et l'exploitation de données personnelles, que ce soit à des fins commerciales ou bien frauduleuses. Cet essai se penche sur les deux moyens d'action principaux qui sont à mettre en œuvre pour maintenir ces valeurs : la législation et la sécurisation des données face aux intrusions dans les systèmes d'informations. Il sera également question d'étudier les valeurs économique et éthique de l'information personnelle, et de confronter ces deux points de vue pour faire émerger les problématiques qui les opposent.

Bibliographie

- **[Cisco]** CISCO. « The economic impact of cyber-attacks ». *Congressional Research Service The Library of Congress* [en ligne]. 2004, p10 [consulté le 09-02-2013]. Disponible sur : http://www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf

- **[SECJ]** Information Security Policy Council from Japan. « Secure Japan ». June 22, 2009 [consulté le 09-02-2013]. Disponible sur : *www.nisc.go.jp/eng/pdf/sj2009_eng.pdf*

- **[FB]** Le Monde. *Facebook franchit la barre du milliard d'utilisateurs [en ligne]. Disponible sur : http://www.lemonde.fr/technologies/article/2012/10/04/facebook-franchit-la-barre-du-milliard-d-utilisateurs_1770255_651865.html [consulté le 05-02-2013].*

- **[TW]** Libération. *Un demi-milliard d'utilisateurs pour twitter* [en ligne]. Disponible sur : *http://www.liberation.fr/ecrans/2012/07/30/un-demi-milliard-d-utilisateurs-pour-twitter_836560 [consulté le 05-02-2013].*

- **[WKL]** Wikipedia. *LulzSec* [en ligne]. Disponible sur : http://en.wikipedia.org/wiki/LulzSec [*consulté le 05-02-2013]*

- **[ZDN]** Zdnet. *The consortium hacks porn site* [en ligne]. Disponible sur : *http://www.zdnet.com/blog/security/the-consortium-hacks-porn-site/10690 [consulté le 05-02-2013]*

- **[HP]** HP. « *Cost of Cyber Crime Study* ». Août 2011. Disponible sur : *www.hpenterprisesecurity.com/collateral/report/2011_Cost_of_Cyber_Crime_Study_August.pdf [consulté le 05-02-2013]*

- **[SMARTV]** The Register. *Smart Tv Pwned. 12 décembre, 2012. Disponible sur :* http://www.theregister.co.uk/2012/12/12/smart_tv_pwned/ [*consulté le 05-02-2013]*

- **[CAM]** The Wired. *School District Allegedly Snapped Thousands of Student Webcam Spy Pics* [en ligne]. Disponible sur : http://www.wired.com/threatlevel/2010/04/webcamscanda/ *[consulté le 06-02-2013]*.

- **[GIZ]** Gizmodo. Watch the World's Highest Resolution Drone-Mounted Camera in Action [en ligne]. Disponible sur : http://gizmodo.com/5979372/watch-the-worlds-highest-resolution-drone+mounted-camera-in-action *[consulté le 06-02-2013]*

- **[SAT]** ADAM LAURIE. « *Satellite Hacking For Fun and Profit* ». Blackhat presentation. Disponible sur : http://www.blackhat.com/presentations/bh-dc-09/Laurie/BlackHat-DC-09-Laurie-Satellite-Hacking.pdf *[consulté le 07-02-2013]*

- **[DV]** DANIEL VENTRE, *Cyber Conflict. Competing National Perspectives,* Editions Wiley-ISTE.

- **[LAT]** Latimes. 100 million tvs will be internet connected by 2016 [en ligne]. Disponible sur : http://latimesblogs.latimes.com/entertainmentnewsbuzz/2012/03/100-million-tvs-will-be-internet-connected-by-2016.html [*consulté le 08-02-2013*]

- **[GO]** GEORG ORWELL, *1984*, p.2, Secker and Warburg, 1949, Londres. ISBN 0452284236.

- **[IL]** : Loi Informatique et Libertés du 6 janvier 1978

- **[DIR] :** directives de la CNIL. Disponible sur : http://www.cnil.fr/vos-responsabilites/vos-obligations/ [*consulté le 06-02-2013*]

- **[LCEN]** : Loi pour la confiance dans l'économie numérique du 21 juin 2004. Disponible sur : http://fr.wikipedia.org/wiki/LCEN [*consulté le 06-02-2013*]

- **[ARR1]** : Arrêt de la Cour de Cassation du 10 mai 2012. Disponible sur : http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000025861623&fastReqId=1316191160&fastPos=1GlossaireD%C3%A9f [*consulté le 06-02-2013*]
- **[FB2] :** Le Monde, *Vie privée sur Internet : la polémique Facebook*, http://www.lemonde.fr/technologies/article/2009/02/19/vie-privee-sur-internet-la-polemique-facebook_1157484_651865.html, *[consulté le 08-02-2013]*

Glossaire

(**N**)**TIC** : (**N**ouvelles) **T**echnologies de l'**I**nformation et de la **C**ommunication

Cybersécurité : *«On entend par cybersécurité l'ensemble des outils, politiques, concepts de sécurité, mécanismes de sécurité […] qui peuvent être utilisés pour protéger le cyberenvironnement et les actifs des organisations et des utilisateurs. [...]. Les objectifs généraux en matière de sécurité sont les suivants:*

- *Disponibilité;*
- *Intégrité, qui peut englober l'authenticité et la non-répudiation;*
- *Confidentialité.»*

Source : Union Internationale des Télécommunications. Disponible sur : http://www.itu.int/net/itunews/issues/2010/09/20-fr.aspx

Cyberdéfense : *« Ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les systèmes d'information jugés essentiels. »*

Source : Ministère de la défense. Disponible sur : www.defense.gouv.fr/content/download/149570/1496328/

Introduction

La phrase culte « Big Brother is watching you » **[GO]** n'a jamais été autant au goût du jour. Avec l'aide de la technologie et de ses progrès fulgurants, les citoyens du monde décrit par George Orwell dans *1984* sont surveillés en permanence, chez eux, dans la rue, au travail. Leur vie est entièrement enregistrée sur des bandes magnétiques et ils semblent prisonniers de leur quotidien. Cet ouvrage de science-fiction suscite chez le lecteur une vive interrogation au sujet des limites du progrès : jusqu'où ira-t-on ? jusqu'où a-t-on le droit d'aller ?

Tandis que l'enthousiasme pour le développement des NTIC bat son plein, on ne peut s'empêcher de se remémorer les interrogations soulevées par ce roman publié il y a plus d'un demi-siècle. Une certaine réticence vis-à-vis de l'accélération de l'avancée technologique dans ce domaine nous amène à nous demander si cette recherche ne se fait pas au dépit de l'éthique, du respect de l'autre en particulier. Et lorsque l'interaction n'est plus entre personnes physiques, mais entre une personne physique et une personne morale telle qu'une entreprise, ce danger se fait de plus en plus menaçant.

Bien que nous sommes encore loin de la société de *1984* abolissant la plus importante des libertés, la liberté d'opinion, il est légitime de se poser la question suivante, afin de mettre en place les garde-fous nécessaires aux prochaines générations de scientifiques, d'entrepreneurs et de législateurs français: les TIC peuvent ils nuire à la vie privée?

Afin d'esquisser une réponse à cette question, nous avons envisagé plusieurs points de vue pour une bonne compréhension des enjeux éthiques constitués par l'utilisation grandissante qui est faite des TIC dans l'entreprise vis-à-vis de la vie privée. Tout d'abord, il nous a semblé juste de poser le cadre légal dans lequel cet essor prend place. Celui-ci est susceptible d'évoluer, et il est important de définir son rôle et ses priorités. Par la suite, nous étudierons le rôle des mesures techniques de sécurité internes à l'entreprise, pour protéger des données sensibles concernant notamment ses employés. Celles-ci constituent une protection supplémentaire en relais de la loi dans tous les cas où elle est enfreinte ou bien ne s'applique pas : il est donc vital de la développer au même rythme que l'évolution des TIC. Enfin, nous poserons quelques éléments de réflexion au sujet de la valeur de l'information dans un tel contexte, tant dans sa dimension morale qu'économique, en explorant des possibilités et des dérives qu'offre la collecte d'informations privées dans un cadre professionnel. Tout au long de l'étude, il sera donc question de replacer la protection des valeurs de l'éthique au centre des problématiques du monde du travail.

I / Le cadre légal

Les textes de loi

L'émergence de nouvelles TIC a accéléré la croissance du partage d'informations, qu'elles appartiennent à la sphère publique ou bien à la sphère privée. Ceci peut donner lieu à des dérives au départ minimes, mais amplifiées sans limites par des publications, mémorisations, transferts, traitements des informations qui ont « glissé » d'une sphère à l'autre. Le but de cette partie est de décrire, dans le cadre professionnel, les acteurs responsables pénalement de cette diffusion et les dispositifs mis en place pour éviter les fuites menaçant l'intimité des citoyens, ainsi que les limites de l'action de la loi.

Dans un premier temps, afin d'apporter quelques éléments précisant quels sont les acteurs concernés par les régulations légales et dans quelle mesure, voici quelques notions juridiques concernant des situations courantes d'usage des TIC dans l'entreprise.

En ce qui concerne l'hébergement de fichiers, toute information sur le Web engage la responsabilité de celui qui l'a publiée, notamment en ce qui concerne le droit à l'image, les droits d'auteur, les injures, la diffamation, etc **[IL]**. En plus de cela, la CNIL (Commission nationale de l'informatique et des libertés) a mis en place un certain nombre de directives **[DIR]** qui doivent être

suivies lors de la mise en ligne d'informations personnelles, ainsi que lors de leur recueil.
Il est à noter que la responsabilité de l'hébergeur n'est pas mise en jeu pour ce qui concerne les contenus de ses serveurs, mais il a l'obligation de retirer toutes données illicites à partir du moment où il en est informé, conformément à l'article 6-I, 2 de la loi LCEN **[LCEN]**.

Pour les fichiers d'un salarié stockés sur un poste de travail, il faut d'abord pouvoir différencier les fichiers personnels. Ceci peut dépendre par exemple de l'emplacement du fichier et des mentions ajoutées par le salarié. On retiendra que l'employeur est libre de consulter tous les fichiers professionnels hors des horaires de travail de l'employé, et peut consulter les fichiers personnels s'il en informe à l'avance le salarié ou bien en présence de ce dernier. **[ARR1]**

Dans la perspective d'associer normes éthiques et normes juridiques, la constitution d'une législation rigoureusement protectrice des données personnelles semble de mise ; cependant, des mesures trop extrêmes pourraient être perçues par les entreprise comme de l'interventionnisme. Nous sommes amenés à penser qu'on trouve là une problématique complexe pour la mise en place d'un compromis législatif éthiquement acceptable, mais également ancré dans la réalité d'un monde marqué par la nécessité pour les entreprises d'être compétitives.

Limites d'application

En raison de la difficulté technique de garder le contrôle sur la circulation de données mises en ligne par un employé, la loi ne peut garantir des procédures rigoureuses que dans le cadre d'une interaction entre un salarié et son employeur tous deux français. Cependant, afin de surveiller la circulation des données via Internet, la CNIL a été instituée en 1978. Son rôle est notamment de garantir un contrôle des sources d'informations, comme le signifie cet extrait d'une fiche informative C2i :
« En France, tout fichier (sauf exception) contenant des données personnelles doit faire l'objet d'une déclaration à la CNIL. Le citoyen a le droit d'accès, de rectification et d'opposition sur les informations de ces fichiers. » **[IL]**

Cependant, il est utopique de penser que ces fichiers pourront être effacés de tout réseau de données ; ils sont en effet bien souvent transférés vers des serveurs situés hors de la juridiction française. Ces échanges sont parfois difficiles à tracer, et l'utilisateur tout comme la CNIL perdent rapidement le contrôle de la circulation des fichiers contenant des informations personnelles.

De plus, il est souvent possible de combiner des données ordinaires pour en déduire des informations non publiées et parfois sensibles, ce qui peut mettre en jeu la sécurité nationale. Prenons l'exemple d'une personne indiquant travailler dans la marine sur Facebook. Elle précise également habiter à Brest (seul port accueillant des sous-marins lanceurs d'engin (SNLE) en France) sur LinkedIn. Finalement, elle publie sur son blog un billet expliquant qu'elle sera indisponible pendant les deux mois à venir, durée typique d'une patrouille d'un SNLE. Cela est suffisant pour en déduire qu'il est probable qu'un SNLE s'apprête à partir en patrouille, afin de remplacer un autre qui rentre au port, laissant éventuellement un intervalle de temps avec moins de sous-marins disponibles en cas de danger imminent.

Grâce à une collection systématique de ce type d'informations, anodines en apparence, n'importe quelle personne ou organisme peut donc aboutir après un traitement suffisamment efficace à des conclusions qui n'ont pas pas forcément vocation à leur être divulguées.

Néanmoins, la fuite d'informations ne vient pas toujours de l'employé. Malgré le fait qu'un utilisateur soit consciencieux, il n'est pas à l'abri d'une faille de sécurité dans le système d'informations de son entreprise. Ceci relève alors du domaine de la vigilance et de la protection face aux intrusions, bien souvent intraçables et ainsi particulièrement dangereuses.

II / La sécurité

La sécurité des données, un enjeu majeur

La numérisation des données a ouvert la voie à un monde plus connecté, où l'échange y est désormais instantané. Or, en élargissant le périmètre d'accès aux informations, la menace de fuite s'en trouve amplifiée. Contrôler les accès aux documents nécessite parfois la mise en place de systèmes d'authentification lourds et complexes qui sont souvent négligés, par soucis pratiques ou économiques.

La cybersécurité est une composante à prendre en compte dans toutes les instances de la société. Que cela soit au niveau individuel ou au niveau étatique, elle représente un maillon critique du partage d'informations.

Si les agressions informatiques ne sont pas nouvelles, leur fréquence ne cesse d'augmenter ces dernières années. Les sondages effectués par le FBI (Federal Bureau of Investigation) en 2002 auprès de 530 entreprises américaines montrent que 90 % des entreprises et des organismes gouvernementaux ont constaté des infractions à la sécurité informatique en 2002. Parmi ces entreprises, 80 % ont reconnu avoir subi des pertes financières.**[CISCO]**

Malgré tout, la mise en place de politiques de cyberdéfense n'est que récente dans nombre de pays. Le Japon ne considère par exemple comme un délit la création et la diffusion d'un virus informatique que depuis 2010.**[SECJ]** Souvent considérée comme la première cyberattaque de grande ampleur, le cas de l'Estonie en 2007 est assez évocateur de l'importance d'un système d'information robuste. L'ensemble de l'économie estonienne s'est vue paralysée pendant des heures par une attaque informatique. L'OTAN ne disposait pas alors de cadre juridique prenant en compte ce type d'attaque non physique.

Suite à cette agression, de nombreux pays réalisèrent la faisabilité de telles attaques, et leur potentiel dévastateur. Des politiques de réponses aux intrusions furent ainsi étudiées et votées par une grande partie des économies dominantes (Etats-Unis, Europe, Chine...) **[DV]**

La sécurité garante de la confidentialité des données utilisateurs

De nombreux sites disposent d'une base de données de plusieurs millions d'utilisateurs **[FB] [TW]**. Quelque soit la charte d'utilisation acceptée par les usagers, leurs informations doivent être utilisées dans un cadre légal défini en amont. Rendre ces données publiques, même malgré soi, est pénalement condamnable.[1]
Certains sites, par faiblesse de conception, ont révélé l'identité de leurs clients malgré l'anonymat garanti à ses utilisateurs. C'est l'embarrassante histoire qui est arrivée à plusieurs des plus grands sites pornographiques. Or, la simple mise à disposition d'emails peut avoir de fâcheuses conséquences : parmi celles-ci se trouvaient du personnel de la Maison blanche, des généraux de l'armée (Etats-Unis, Chine, etc.), des diplomates ainsi que des représentants de pays où la pornographique est un délit. **[WKL]**

Plus dangereux encore, l'accès à des données permettant d'usurper l'identité des clients. Digitalplayground est un exemple parlant. Les attaquants ont réussi à dérober toutes les informations de 72000 utilisateurs. Outre mot de passe et adresse email, leurs données bancaires figuraient également dans les bases de données **[ZDN]**. La faute de la compagnie fut double. D'une part, celle-ci a permis un accès non autorisé à des assaillants extérieurs par négligence. D'autre part, aucune donnée n'a été chiffrée. La diffusion des informations a ainsi put être quasiment immédiate. Nous voyons bien les méfaits que peuvent causer une politique de sécurité trop légère. Les données sensibles devraient être systématiquement chiffrées par un algorithme

1 - http://fr.wikipedia.org/wiki/Fuite_d%27information

robuste.[2]
Ces attaques ciblent différents secteurs. Le nombre de clients représente la principale motivation des pirates. Ainsi Sony perdit les données de 77 millions d'utilisateurs du PlayStation Network, et de 25 millions de clients PC Network en 2010. Précédemment, NTT et KDDI perdaient les informations de 6 millions d'usagers. Ces intrusions ont un lourd impact sur l'économie des entreprises. Le rapport 2011 Second Annual Cost of Cyber Crime Study par le Ponemon Institute **[HP]** étudie 50 compagnies de différents secteurs d'activités. Bien que toutes situées aux Etats-Unis, elles sont ouvertes sur l'international. Les chiffres sont équivoques : « Le coût médian par an relatif au cybercrime est de 5.9 millions de dollars par compagnie […] et plus d'une attaque par semaine aboutit ». Il semble ainsi évident que quelle que soit son coût, une politique de sécurité solide est indispensable.

De l'atteinte à l'intimité physique

Outre l'acquisition de données sociales (opinions politiques/religieuses, numéros de téléphone, etc.), une utilisation pernicieuse des TIC peut porter atteinte à l'image physique d'une personne. Il est nécessaire de traiter tout dispositif de capture d'image avec le plus grand soin. L'attention doit être double. D'une part, la technologie doit être parfaitement maîtrisée, au risque d'être compromise et utilisée à des fins douteuses. D'autre part, il est important de surveiller les contrôleurs de ces équipements « *sed quis custodiet ipsos custodes* » (Qui gardera ces gardiens) ?
Prenons l'exemple des télévisions nouvelles générations. Celles-ci sont équipées d'une webcam permettant de faciliter l'interaction entre écran et utilisateur. Elles offrent également un accès internet. Il a récemment été découvert qu'un attaquant pouvait prendre le contrôle de la caméra via une simple page malicieuse **[SMARTV]**. A lui votre canapé, votre salon et le loisir d'espionner tous vos faits et gestes. Le télécran d'Orwell en rugirait de jalousie. Les chercheurs estiment que 100 millions de télévisions nord-américaines et européennes seront connectées d'ici 2016. **[LAT]** Les téléviseurs, bien qu'objets du quotidien, sont désormais un élément critique vis à vis de la vie privée.
Autre fait prouvant la nécessité d'un contrôle des utilisations : la distribution d'ordinateurs aux élèves d'une école de Philadelphie. Ceux-ci disposaient de webcams activées en cas de vol. Or de nombreuses images d'étudiant(e)s peu vêtu(e)s furent dérobées. Des membres du personnel de l'école ont été inculpés dans cette fuite. **[CAM]**
Mais l'espionnage physique ne se limite pas qu'à ce vecteur d'intrusion. Les avancées technologiques dans le domaine du spatial et de la miniaturisation permettent de créer de véritables yeux omniscients. Il est désormais possible d'obtenir des vidéos nettes d'objets de 15 cm avec des drones placés à plus de 5000 mètres. **[GIZ]** Or un satellite se pirate de la même façon qu'un simple ordinateur. **[SAT]**

Les entreprises doivent donc être rapidement soumises à une réglementation concernant leur politique de sécurité. Les attaquants faisant fi de toutes frontières, ces normes doivent être définies mondialement. La formation des futurs ingénieurs devrait comporter une formation à la sécurité. Sans cela, tout comme Winston Smith[3], nous en viendrons à craindre Internet, nos appareils et même nos rues.

III / La valeur de l'information

Valeur morale vs valeur économique : les conflits d'intérêts entre la loi et les entreprises

Les TIC sont versatiles. Ils changent d'application, de domaine, d'enjeux. Ce cycle de métamorphose est aujourd'hui principalement guidé par l'appel du profit. Or, à force de transformations, la valeur morale des innovations se dilue dans le torrent de l'appât du gain. Sans jalon éthique, la science ne sera que l'esclave de l'intérêt financier et non plus du progrès de la

2 - C'est d'ailleurs ce que recommande la CNIL.
3 Personnage principal du roman 1984.

société.

Ce combat constant entre rentabilité et morale est représenté par le bras de fer entre législation et entreprise. De par la malléabilité des TIC, la loi peine à suivre la témérité des affaires. Ainsi, c'est aux entreprises que le rôle incombe de respecter une déontologie saine.

Ainsi, le droit à l'oubli numérique a fait débat ces dernières années.[4] Ce texte a subi une forte opposition de la part des juristes des plus grands groupes Internet : Google, Facebook, etc. Outre la mise en avant de « l'impossibilité de sa mise en application », les géants du web ont invoqué le droit à la liberté d'expression. Malheureux ouroboros, la problème reste en suspend. Entre souhait politique et réalité d'entreprise, le fossé se creuse et responsabiliser les futurs décideurs lors de leur formation semble le seul échappatoire à cette lutte perpétuelle.

Malgré tout, un climat de méfiance tend à s'installer parmi les utilisateurs.[5]

Que penser alors de la double authentification Google, qui permet de renforcer la sécurité de nos comptes à condition de fournir un numéro de téléphone ? Ou de la localisation Facebook, qui détecte tout changement de machine ? Si en apparence la démarche semble louable, on ne peut que s'interroger quant aux réelles motivations derrières ces fonctionnalités. Reste que la transparence et la protection des données reste un modèle économique lucratif et émergeant.

Traitement de l'information : la vraie valeur ajoutée

Comme vu précédemment, l'information peut avoir une valeur économique réelle lorsqu'elle permet de faire des statistiques, et donne de nouveaux outils pour développer une stratégie de marketing de masse plus efficace. Cependant, il est également possible de combiner des données au niveau de l'individu. Ceci a par exemple bouleversé les techniques publicitaires modernes : si vous cherchez des billets de train à prix réduits, Google s'en souviendra et vous aiguillera dans vos recherches futures vers des sites de covoiturage. Si vous montrez de l'intérêt pour la 1ere classe, quelle que soit le prix, pourquoi ne pas prendre l'avion à la place ?

Ce marketing personnalisé n'est pas forcément dérangeant lorsque ce phénomène reste circonscrit à des utilisations bien particulières : après tout, si vous avez accepté de donner des informations personnelles à Facebook, il a bien le droit de les utiliser pour en faire des publicités plus intéressantes. Le véritable problème vient du fait que Facebook soit en droit de « revendre » ces informations tant qu'elles sont en ligne. Un projet de garder une licence sur tout le contenu déposé, y compris celui ensuite supprimé, a provoqué un tel tollé que la firme a rapidement fait marche arrière en février 2009. **[FB2]**
En dehors du domaine publicitaire, le traitement de l'information est un processus à très haute valeur ajoutée, et donc un enjeu considérable pour les entreprises. La compétition économique devenant de plus en plus pressante dans un contexte de globalisation, la course à la collecte d'informations est devenue une véritable guerre économique dans laquelle dérober des informations personnelles est seulement un moyen de pression,un levier permettant de faire chanter des dirigeants, les poussant à lâcher prise sur des données sensibles de l'entreprise.

Dans ces deux types de cas, le salarié en tant que personne est traité comme un produit, ou bien comme un simple moyen dans une lutte entre deux entreprises. Ses données personnelles sont extraites de gré ou de force, analysées, raffinées, et utilisées dans des buts sur lequel il n'a plus aucun contrôle. C'est ici que doit intervenir l'action des dirigeants, en protégeant l'intégrité de l'intimité : empêcher la fuite de l'information et faire de la confidentialité des données personnelles une priorité dans son entreprise.

4 http://fr.wikipedia.org/wiki/Chartes_du_droit_à_l'oubli_numérique

5 Ainsi, un américain sur deux possesseurs d'un smartphone android a déjà supprimé une application par méfiance à l'égard de sa vie privée selon Isabelle Falque-Pierrotin, présidente de la CNIL lors de son investiture.

Conclusion

Ainsi, il semble clair que dans un monde de l'information en pleine explosion, il nous faut canaliser cette brutale expansion. Si des efforts sont fait pour encadrer juridiquement l'utilisation des données personnelles, la rapidité d'évolution des TIC les rend vite obsolètes. Le cadre légal est sans cesse en retard vis-à-vis de nouvelles prouesses technologiques. Le changement doit donc s'opérer au sein même des entreprises. A travers de nombreux exemples, nous constatons l'impérative nécessité d'une politique de sécurité forte. Ignorer les risques revient à exposer à nus ses clients, moralement et physiquement. Mettre en place un standard de fiabilité permet donc de palier partiellement aux manquements des lois. Mais si la sécurité a un coût, qu'en est-il du prix de l'information ? Les données personnelles sont convoitées par les plus grandes entreprises, qui défendent une utilisation des informations sans limite. Or si la récupération de données est une aubaine vénale, leur traitement est le véritable dessein. Grâce à des analyses statistiques, les entreprises se font omniscientes.
Cet essai, loin d'être exhaustif, a tenté d'exposer les principaux problèmes auxquels sont et seront confrontés les décideurs de demain. Les TIC et Internet ne doivent pas devenir une toile reliant des araignées emprisonnant notre intimité. Ce n'est que par l'éducation des utilisateurs et la formation des futurs ingénieurs que peut naitre un traitement des données parcimonieux. Attachons-nous plutôt à exploiter aux mieux les phénoménales capacités mémorielles de TIC pour en faire des éponges à savoir, et non à personne.

19930 mots (essai)