



## CASES articles

Série d'articles CASES : À poil sur la toile ? – Protégez vos données !

### Les traces numériques que nous laissons derrière nous

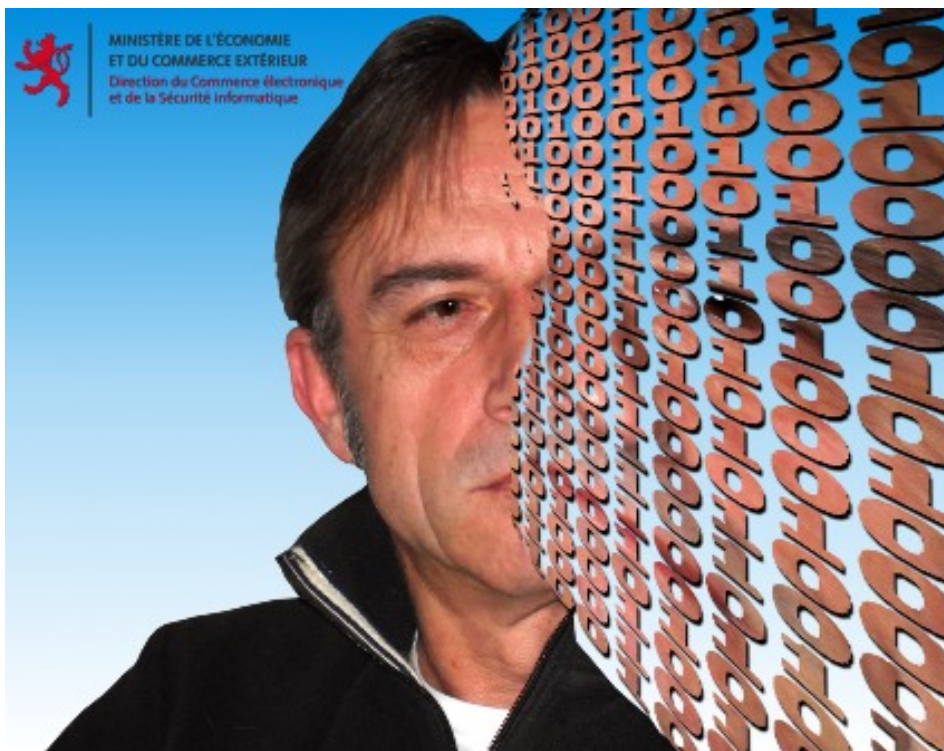
**Pour plus de sécurité, adoptez les réflexes CASES !**

**Vos données numériques peuvent être utilisées de manière abusive à des fins de surveillance et de manipulation**

Les technologies de l'information permettent la création d'une société de la connaissance. Les informations peuvent être consultées et combinées entre elles avec une rapidité fulgurante, au grand bénéfice de la société. Dans le même temps, NTIC peuvent créer une véritable cartographie numérique de leurs utilisateurs. Chaque individu est concerné, en fonction de son mode d'utilisation des technologies de l'information. Afin d'éviter l'exploitation abusive de ces données par des tiers, les utilisateurs devraient, dans la mesure du possible, veiller à protéger leurs données privées et à limiter leurs traces numériques.

L'utilisation des technologies de l'information et des médias numériques « oblige » à laisser de nombreuses traces. Un exemple va nous permettre de les identifier : nous allons suivre deux personnes – nommons-les Lisa et Paul – tout au long d'une journée ordinaire.

Lisa et Paul disposent chacun d'un téléphone mobile, d'un ordinateur et de nombreux autres acquis de la société de l'information moderne. Sur leur lieu de travail, tous deux utilisent des ordinateurs en réseau et des périphériques, tels que des imprimantes par exemple. Ils se servent également de moyens de télécommunications modernes. Toutes ces activités génèrent des traces numériques, aussi bien géographiques que dans le



temps. Les tâches professionnelles ou autres activités qu'ils ont effectuées peuvent ainsi être reconstituées.

La piste commence dès le matin chez Lisa et Paul, peu après leur lever : ils sont par exemple filmés par le système de vidéosurveillance dans le parking souterrain.

Lorsque Lisa et Paul activent leurs téléphones mobiles pour la nouvelle journée, il est possible de les localiser géographiquement. L'opérateur d'un réseau mobile est ainsi tout à fait en mesure de déterminer où ils se trouvent. Cet état de fait devient d'ailleurs évident à chaque fois que l'utilisateur d'un téléphone mobile franchit une frontière européenne : un SMS lui

indiquant les tarifs téléphoniques à l'intérieur de l'Union européenne lui est transmis quelques instants plus tard. À des fins de facturation, les opérateurs de réseaux mobiles enregistrent les données de communication des quelque 450 millions d'utilisateurs de leurs réseaux au sein de l'UE, pour une durée d'au moins 6 mois. Les services de renseignement et organismes judiciaires peuvent consulter et exploiter ces données dans le cadre de la lutte contre la criminalité et le terrorisme. Tous les appels effectués, ainsi que leurs durées sont ainsi répertoriés.

## **La piste se poursuit jusqu'au lieu de travail**

Lisa se rend à son travail en utilisant les transports en commun et elle règle le prix du voyage à l'aide d'une Smartcard. Celle-ci est comparable à une carte de sécurité sociale ou à une carte bancaire : elle est dotée d'une puce sur laquelle sont stockées des données personnelles, telles que le nom et l'adresse. Il est ainsi possible de reconstituer où se trouvait Lisa et à quel moment.

Il en va de même pour Paul : sa voiture est équipée d'un système de télémétrie, dont font également partie les appareils de navigation. La télémétrie fournit constamment des informations quant à la localisation du véhicule. Des indications sur le kilométrage parcouru ainsi que sur la vitesse peuvent également être transmises. Il est tout à fait envisageable que ces informations soient par exemple un jour exploitées par les compagnies d'assurance, afin de déterminer le style de conduite de Paul. Elles seraient ainsi en mesure d'adapter le montant de la cotisation au style de conduite. Ces informations permettraient également à l'administration fiscale de vérifier le nombre de kilomètres parcourus par rapport à ceux indiqués par Paul dans sa déclaration d'impôts.

Arrivés sur leurs lieux de travail, Lisa et Paul continuent à laisser des traces numériques, cette fois sur leurs postes de travail informatiques. Un logiciel spécifique permet par exemple de contrôler l'activité de nos deux protagonistes sur leurs ordinateurs respectifs. Peuvent alors être enregistrés, entre autres : les pages Internet visitées, les e-mails reçus et envoyés, la durée d'utilisation de telle ou telle application ou le nombre de frappes de clavier par heure. Dans certains pays, plus de la moitié des employeurs recueillent d'ores et déjà ce genre de données.

Il est même possible d'identifier l'imprimante laser couleur qui a été utilisée pour une impression grâce à un code dissimulé sur celle-ci, com-

portant le numéro de série de l'appareil, l'heure et la date d'impression.

## **Des traces numériques même pendant les loisirs**

Pendant leurs loisirs, Lisa et Paul règlent souvent leurs dépenses à l'aide de leur carte de crédit ou carte eurochèque. L'établissement de crédit ou la banque peuvent ainsi très aisément déterminer où Lisa et Paul ont fait leurs emplettes, dans quels restaurants ils ont mangé, dans quels hôtels ils ont passé la nuit, s'ils ont loué une voiture et où ils sont partis en vacances. Les autorités peuvent consulter et exploiter ces données dans le cadre de la lutte contre la criminalité. Il est ainsi également possible d'établir un profil de consommateur, permettant d'estimer le pouvoir d'achat respectif de Lisa et de Paul, de déterminer s'ils vivent seuls ou en couple et s'ils ont des enfants, ou encore de connaître leurs habitudes alimentaires et leurs passe-temps favoris. En outre, ces données permettent par exemple d'établir quel type de publicité sera le mieux perçue par les 2 protagonistes.

À l'avenir, il est envisagé de remplacer les codes-barres figurant sur les produits achetés par une puce pouvant être lue sans contact, par radio. Un appareil de lecture correspondant serait alors par exemple en mesure d'identifier les vêtements que portent Lisa et Paul. Si les billets de banque venaient à être dotés de ce genre de puce, il serait même possible de déterminer la somme d'argent que ces deux personnes ont sur elles.

En soirée, de retour à la maison, Lisa et Paul utilisent leur ordinateur privé pour envoyer des e-mails, chatter, faire des achats ou encore réserver un voyage. Une fois encore, ils laissent des traces. La Directive européenne 2006/24/CE du 15 mars 2006, exige des prestataires de services Internet l'enregistrement pour une durée de 6 à 24 mois des données de connexion. Les données relatives à la

connexion, à la durée de la session en ligne, à l'identifiant, au nom et à l'adresse de la personne, aux pages Internet consultées ainsi que de nombreuses autres informations sont stockées, en vue de leur exploitation au cours d'éventuelles enquêtes.

Si Lisa et Paul n'ont pas pris les mesures adéquates de protection, leur ordinateur peut en outre être espionné par toute une série de programmes malveillants. À ceux-ci viennent souvent s'ajouter des applications tout à fait normales, mais disposant de « portes dérobées » permettant de transmettre discrètement des données au sujet de l'utilisateur et de son système informatique.

Même lorsqu'ils regardent la télévision numérique, Lisa et Paul laissent des traces : il est ainsi possible de connaître leurs émissions préférées et de déterminer les produits qu'ils ont commandés sur les chaînes de téléachat.

Les congés de carnaval ne sont plus très loin et Lisa et Paul envisagent de partir en vacances. Ils souhaitent rendre visite à des amis à New York. Lors de la réservation de leur vol, la compagnie aérienne ne transmet pas moins de 40 champs de données aux autorités américaines. Ces données seront ensuite stockées durant 15 années. Parmi les informations ainsi transmises figurent les noms de Lisa et Paul, leurs dates de naissance, leurs adresses e-mail, les données relatives à leur carte bancaire, les noms des autres voyageurs ainsi que le nom de l'agence de voyages auprès de laquelle ils ont réservé leur voyage. Ces données sont analysées sur la base de critères précis. De plus, à leur arrivée, leurs empreintes digitales seront relevées. Celles-ci demeureront dans les bases de données américaines pour une durée de 50 ans.

## Maîtriser les dangers

De nombreuses données numériques sont stockées dans des banques de données, par exemple celles relatives à la réservation en ligne d'un voyage. De nos jours, les banques de données peuvent toutefois être compressées et copiées sans que d'importantes connaissances spécifiques soient requises. C'est l'une des raisons pour lesquelles les données ne demeurent pas seulement là où elles ont été enregistrées initialement, mais apparaissent subitement aux endroits les plus divers.

Les informations concernant Lisa et Paul sont de ce fait, enregistrées un peu partout... L'utilisation d'ordinateurs toujours plus rapides et de programmes spécifiques permet aujourd'hui de combiner toutes ces données et d'effectuer des recherches instantanées sur des informations particulières ou des catégories d'informations. Ces informations peuvent ensuite être exploitées par des tiers à des fins criminelles. Les utilisateurs devraient donc veiller à ne pas divulguer trop facilement des données personnelles. Ils devraient réfléchir avec attention aux données qu'ils souhaitent communiquer à une entreprise ou à une organisation en vue d'une prestation de service. Ils devraient insister pour que leurs données ne soient pas exploitées en dehors du cadre de leur utilisation prévue initialement et qu'elles ne soient pas communiquées à des tiers.

Lorsque les conventions régissant une société se modifient lentement et

### Conseils de sécurité : manifestations autour du thème de la sécurité de l'information

Vendredi 13.02.2009 a eu lieu une soirée d'information sur le thème de la sécurité de l'information dans le Centre Martialis à Ellange. Organisée par l'Amicale Ellange, elle était animée par François Thill, responsable du portail de la sécurité de l'information CASES du Ministère de l'Économie et du Commerce extérieur. Ont figuré parmi les thèmes principaux de cette soirée: la détection des risques sur l'Internet et comment se protéger, ainsi que la thématique de la sécurité de l'information auprès des enfants et des adolescents.

Dans les locaux de la Cité Bibliothèque de la Ville de Luxembourg, LUSi – portail luxembourgeois de la sécurité de l'information pour les enfants et les adolescents – a organisé, du 10.02 au 14.02.2009, en collaboration avec d'autres partenaires, une exposition interactive, des démonstrations et des conférences autour du thème de la sécurité de l'information. Chaque jour, à 17h30, a eu lieu une conférence, suivie d'une discussion, relative à l'un des thèmes de la sécurité de l'information suivants : sécurité du commerce électronique ; protection des données privées sur l'Internet ; la sécurité en ligne ; l'Internet – terrain de jeu de la jeunesse. De plus amples informations à ce sujet peuvent être consultées sur [www.lusi.lu](http://www.lusi.lu).

La Commune de Schengen a organisé les 11.02 (en langue allemande) et 18.02.2009 (en langue française), en collaboration avec le portail de la sécurité de l'information CASES, des soirées de formation continue au profit des adultes. Ces soirées ont eu lieu à l'Auberge de jeunesse de Remerschen. Outre la description des modes de fonctionnement des virus, vers et autres chevaux de Troie, a également été abordé le thème du comportement des utilisateurs. Les participants ont ainsi eu la possibilité d'acquérir des compétences dans le domaine de la sécurité de l'information ou d'améliorer celles dont ils disposaient déjà.

presque imperceptiblement, l'être humain s'habitue graduellement aux nouvelles normes et règles. Outre les transformations positives que peut apporter une telle évolution, il convient toutefois de ne pas perdre de vue les dangers potentiels qui peuvent en découler, en particulier dans la société de l'information. Les traces numériques peuvent être utilisées à des fins de surveillance, et

donc mener à la restriction de la sphère privée, voire à la manipulation de personne. Toute exploitation abusive des données visant à léser la personne est également envisageable. Les utilisateurs devraient veiller à ce que les services et les applications qu'ils utilisent offrent une sécurité de l'information suffisante et s'ils sont à même d'exclure tout risque d'utilisation abusive de leurs données.

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

[www.cases.lu](http://www.cases.lu)