Informatique : comment protéger notre vie privée ?

Rencontre du Café des techniques du jeudi 15 janvier 2004 au musée des Arts et Métiers
A l'initiative de l'AFAS, en collaboration avec l'Association des amis du musée des Arts et Métiers
Avec le soutien de la délégation à la Recherche et à la Technologie d'Ile-de-France

avec la participation de

Pascal Lointier, président du Club de la sécurité des systèmes d'information français (CLUSIF)

Robert Longeon, chargé de mission à la sécurité des systèmes d'information, direction générale du CNRS, fonctionnaire de défense

Christophe Pallez, secrétaire général, chargé des affaires juridiques de la Commission nationale de l'informatique et des libertés (CNIL)

Jacques Stern, professeur à l'Ecole normale supérieure, directeur du département informatique

Rencontre animée par **Paul de Brem**, journaliste scientifique

Pourquoi cette rencontre ?

Que sait-on de nous ?
Où se situe la frontière entre libre circulation de l'information et protection de la vie privée ? Internet, messagerie électronique, carte à puce, badge d'accès, téléphone portable… L'évolution des technologies nous offre chaque jour de nouveaux services pour faciliter notre quotidien. Sommes-nous toujours conscients qu'en les utilisant, nous dévoilons aussi une partie de notre vie privée ?
Les multiples données informatisées ainsi mises en circulation ouvrent des possibilités de surveillance par des acteurs ayant des motivations très diverses. La protection des informations devient alors une véritable course contre la montre rythmée par les innovations technologiques.
Comment préserver la confidentialité des données personnelles, mais aussi leur intégrité et leur authenticité ? Quelles sont les perspectives d'application de la cryptographie ? Est-il possible de garantir le respect de l'anonymat lors d'échanges d'informations ? Comment encadrer la finalité et l'usage des différentes données collectées sur chacun de nous ?
Dans un contexte où le facteur humain reste un élément central, découvrez quels sont les moyens mis en œuvre pour assurer la sécurité des systèmes d'information.

R. Klapisch :

Je vous souhaite la bienvenue à cette Rencontre du Café des techniques, organisée conjointement par l'Association française pour l'avancement des sciences (AFAS) et le musée des Arts et Métiers.

La séance d'aujourd'hui marque le troisième anniversaire de ces Rencontres, et je vous remercie d'être venus si nombreux.

Le thème de ce soir, l'informatique et la vie privée, touche à la fois à la technologie et à la société. Cette rencontre sera animée par Paul de Brem, à qui je passe la parole.

P. de Brem

Merci et bonsoir à tous.

La prise de conscience a eu lieu sans doute aux alentours de 1993. Cette année-là, vous vous en souvenez peut-être, pour couvrir son ami Bernard Tapie dans l'affaire OM-VA, le député-maire de Béthune, Jacques Mellick, déclare qu'il se trouvait avec lui dans son bureau de Paris, le 17 juin. Mal lui en prend, car l'enquête révèle rapidement qu'à l'heure dite, il se trouvait en réalité à un péage autoroutier. La preuve est une trace de son passage laissée dans la mémoire d'un ordinateur au moment du paiement. Il sera condamné à un an d'emprisonnement avec sursis, cinq ans d'inéligibilité et 30 000 F d'amende pour témoignage mensonger.

Depuis cette époque, nous avons tous pris conscience que nous laissons un peu partout, le plus souvent à notre insu, des traces informatiques de notre passage et de nos activités. Pour le monde marchand, ces données sont de véritables mines d'information sur nos comportements,

nos habitudes de consommation, et elles ouvrent la voie à un nouveau marketing dit «ciblé», avec des offres publicitaires spécifiques à chacun. Pour l'avenir, certains craignent également le pouvoir gigantesque qu'offriraient à un état policier répressif ces nouveaux moyens de surveillance.

Les objets technologiques et de communication qui nous entourent et dont nous dépendons de plus en plus peuvent donc nous piéger et nous trahir. La société de l'information se déploie-t-elle aux dépens de notre vie privée ? Quelle est la réelle nature du danger, son étendue ? Quelles sont les mesures et les moyens mis en place actuellement pour nous préserver ? Ces moyens suffisent-ils ? Face à des réseaux mondialisés, comment faire respecter des règles communes ? Ce sont quelques-unes des questions que, tous ensemble, nous allons poser. Vous connaissez le principe du Café des techniques : vous êtes là pour poser des questions à nos invités, des scientifiques avec qui nous évoquerons des mots récemment apparus comme *spam*, *phishing*, *spyware*, *skimming*, *yescarding*, qui recouvrent des moyens d'entrer dans notre vie privée et de nous jouer de vilains tours.

Le Café des techniques d'aujourd'hui s'intitule : «Informatique : comment protéger notre vie privée ?». J'ai le plaisir d'accueillir quatre invités, qui vont chacun se présenter et préciser le type de questions auxquelles ils peuvent répondre.

P. Lointier :

Je suis le président du CLUSIF (Club de la sécurité des systèmes d'information français), association sans but lucratif qui regroupe 600 membres, pour moitié des responsables ou des fonctionnaires de sécurité et pour l'autre moitié des fournisseurs de services de sécurité. Nous échangeons des informations sur les problèmes types de sécurité de l'information.

Je suis président de cette association à titre bénévole, et je travaille par ailleurs dans une compagnie d'assurance spécialisée dans l'assurance des systèmes d'information contre les virus, les fraudes financières, les extorsions, etc.

J'ai également d'autres casquettes, qui me permettent d'apporter une précision quant à l'affaire de Béthune que vous venez d'évoquer : la preuve était en fait irrecevable, car l'appareil n'était pas passé aux bancs et mesures !

R. Longeon :

Je suis chargé de mission à la sécurité des systèmes d'information au CNRS et j'édite la revue *Sécurité des systèmes d'information*. Je fais également un peu de formation sur la sécurité des systèmes d'information.

Je peux répondre à des questions concernant la protection des systèmes.

P. de Brem :

Pascal Lointier, vous êtes davantage spécialiste des questions de malveillance, en particulier sur l'Internet.

P. Lointier :

Tout à fait. Je travaille dans une compagnie d'assurance, mais j'ai un profil de consultant en sécurité, et mon domaine de spécialisation est surtout les atteintes, donc la malveillance.

C. Pallez :

Je suis le secrétaire général de la Commission nationale de l'informatique et des libertés, la CNIL, dont le sigle, je l'espère, vous est familier. La CNIL est l'autorité administrative indépendante chargée de veiller à ce que les traitements informatiques ne mettent pas en péril la vie privée. Elle reçoit les déclarations des traitements, vérifie leur conformité à la loi, et recherche les aberrations dans la mise en œuvre de ces traitements par rapport à la protection de la vie privée.

Le champ des questions auxquelles je peux répondre est donc juridique puisque la CNIL est une autorité qui vérifie la conformité à la loi, qui édicte des textes juridiques permettant de mieux garantir les droits des personnes, et qui a une certaine expérience de la façon dont l'informatique et le développement des techniques d'information peuvent mettre en péril certains éléments de la vie privée.

P. de Brem :

Nous verrons avec vous toutes les questions juridiques relatives à la protection de la vie privée, et à la façon dont ces dispositions sont actuellement mises en œuvre.

J. Stern :

Je suis directeur du département d'informatique de l'Ecole normale supérieure. Je suis présent ce soir au titre de ma spécialité, la cryptologie, qui est la science des messages secrets. Son but est d'assurer l'authenticité, l'intégrité et surtout la confidentialité des données échangées sur les réseaux. Vous voyez que nous sommes au cœur de la protection de la vie privée.

Je suis prêt à répondre à toute question, mais plus particulièrement aux questions un peu techniques sur la manière dont on procède pour protéger ces données et pour se défendre contre les attaques éventuelles de ceux qui cherchent à contourner les protections.

P. de Brem :

Avant d'entamer notre débat, j'aimerais poser une question à chacun de nos invités.

Ma première question s'adresse à Pascal Lointier. Il y a deux jours, vous avez organisé une conférence qui a réuni une soixantaine de personnes, dont des journalistes, sur le thème : «Le panorama de la cybercriminalité». Vous organisez cette conférence chaque année en essayant de décrire les innovations des «cybercriminels» au cours de l'année écoulée. L'une des innovations concernant la vie privée a attiré mon attention, à savoir celle des virus.

Jusqu'alors, les virus informatiques étaient le fait de personnes qui s'amusaient - le virus arrivait sur votre

ordinateur et vous aviez un message vous disant : «Je vous ai bien eu !» - ou alors plus malveillantes avec des virus qui détruisent les données. Or, cette année nous avons eu deux virus, et non des moindres, qui ont eu notamment pour fonction de récupérer des données personnelles sur l'ordinateur et de les envoyer on ne sait où.

P. Lointier :

L'objet de ce panorama, qui est en libre téléchargement sur le site du CLUSIF, consiste à remettre en perspective les grands événements de l'année : soit des événements qui sont symptomatiques d'un volume important d'affaires, soit des événements qui sont des cas d'école et auxquels, parfois, on ne pense pas en tant que responsable sécurité, soit encore des événements qui sont des émergences de nouvelles tendances.

Les virus, depuis déjà quelques années, parvenaient parfois à récupérer les mots de passe ou des fichiers, à les prendre sur la machine et à les envoyer. 2003 aura été une année très forte parce qu'on a vu deux développements majeurs dans les fonctionnalités des virus.

D'abord, un groupe de nouveaux virus spécialisés dans l'installation des logiciels de *spams*, ces courriers non sollicités, qu'on appelle aussi des «pourriels» par référence aux «courriels». Dans la mesure où les *spamers* commencent à être condamnés au niveau international, ils ont voulu rendre leur action plus anonyme. C'est ainsi que nous avons vu un certain nombre de virus qui n'avaient pas pour fonction de détruire vos données, de vous jouer une musique ou de faire un affichage sur votre écran, mais d'exploiter votre machine, que ce soit un PC, un Mac ou un serveur, pour propager leurs messages illicites.

La seconde évolution majeure, concernant toujours cette capture des informations confidentielles, est la volonté de cibler des institutions financières, des banques, pour récupérer des mots de passe de connexion ou des informations. Nous avons eu, en début d'année, un virus qui avait dans son code 1 300 institutions financières comme cibles d'activation de ses effets.

Donc, manifestement, nous quittons le domaine ludique, amateur, individuel ou collectif - les auteurs de virus sont parfois des groupes, comme le groupe 29A qui est un très «bon» groupe d'auteurs hispaniques.

Là, nous sommes face à des professionnels, à une délinquance organisée, qui exploite cet outil - le virus est une ressource informatique -, dans un but professionnel, marchand, avec recherche de gains. Ils ne sont pas parvenus, semble-t-il, à pénétrer les 1 300 banques, dont certaines françaises. Mais, en tout état de cause, il y a une volonté manifeste et affichée, sur l'année 2003, d'exploiter les virus dans un but professionnel.

P. de Brem :

L'un de ces virus s'activait lorsqu'on tapait sur le clavier «compte» ou «banque», et restait éveillé pendant quelques secondes en espérant récupérer le mot de passe qui permet d'entrer sur le site de votre banque.

P. Lointier :

Tout à fait. Ce n'est pas difficile sur le plan informatique. Le logiciel va «écouter» le clavier, et lorsque vous tapez votre nom ou une requête de connexion, il va mémoriser les caractères que vous tapez juste après l'identifiant et qui comprennent, bien sûr, votre mot de passe. Votre mot de passe est en clair puisque c'est du clavier qu'est prise l'information. Il le récupère donc, ainsi que votre nom de compte, et l'envoie soit sur un canal IRC, qui est une ressource Internet pour communiquer, soit sur un site Web, soit sur un e-mail «anonyme».

Nous voyons donc bien qu'il ne s'agit plus de jeu, mais d'une volonté manifeste d'exploiter ces informations.

P. de Brem :

Je précise qu'il ne s'agit pas de n'importe quel virus : Bugbear est un énorme virus. Au cours de ce panorama de la cybercriminalité, il n'a pas été démontré que ces virus avaient donné lieu effectivement à des retraits d'argent par l'utilisation de ces mots de passe.

P. Lointier :

Non, effectivement, aucun événement ne s'est réalisé. Dans le panorama 2002, en revanche, un précédent virus récupérait des mots de passe, et le FBI avait voulu forcer un fournisseur d'accès à récupérer tous les mots de passe que le virus pouvait collecter et faire transiter via ce fournisseur d'accès. Le fournisseur d'accès a été contraint de s'exécuter, mais, pour rétablir l'équilibre, il a ouvert une page spéciale où l'on pouvait taper un identifiant et vérifier si le virus en avait récupéré le mot de passe.

Sur 2003, c'est un événement de plus en plus fréquent, et le reproche que je pourrais faire à la médiatisation autour de ce genre de virus est celui-ci : je n'ai pas vu un seul message indiquant aux personnes contaminées par un tel virus de changer leur mot de passe. L'avez-vous fait ?

P. de Brem :

Non, pas depuis deux jours !

Robert Longeon, vous vous occupez beaucoup de sécurité informatique au CNRS. Nous quittons un instant le domaine de la vie privée. Le CNRS, en tant qu'institution qui possède des secrets, qui fait des recherches sur lesquelles beaucoup de personnes aimeraient pouvoir mettre la main, a-t-il déjà fait l'objet d'attaques directes pour essayer de récupérer des données scientifiques que vous auriez découvertes ?

R. Longeon :

Nous faisons des statistiques sur les attaques que nous subissons, et c'est de l'ordre de mille attaques par semaine. Il s'agit d'attaques graves mettant en jeu des valeurs parfois considérables. Ce peut être par exemple une intrusion dans le système d'information ou une mise en indisponibilité d'une machine par l'extérieur, causant un arrêt de la production ou du moins une gêne, ou encore une com-

munication qui a été écoutée, c'est-à-dire la sécurité sous l'aspect intégrité, disponibilité et confidentialité.

Sur ces mille attaques, à peu près quatre-vingt sont identifiées, et pour la moitié d'entre elles, on peut empêcher la malveillance de se poursuivre.

P. de Brem :

Cela signifie qu'il y en a 920 qui réussissent à passer.

R. Longeon :

Nous faisons ces mesures par statistiques en simulant des attaques, et nous regardons les réactions.

P. de Brem :

Vous vous attaquez vous-mêmes ?

R. Longeon :

Oui. Afin de vous donner une idée de l'ampleur du problème, nous nous sommes fait voler un logiciel de reconnaissance vocale que nous avons retrouvé sur le marché à 42 millions de dollars. Cela vous donne une idée de ce que représente une attaque informatique pour la société, car, quelque part, c'est nous tous qui payons.

C'est parfois assez sournois. Je citerais l'exemple d'un directeur qui m'a appelé un soir pour me dire : «Je crois que j'ai quelqu'un dans ma machine en ce moment». Je lui demande sur quelle machine il travaille. Il m'indique qu'il travaille sur un Macintosh®. Je lui réponds : «Alors, ce n'est pas grave puisque vous ne devez pas avoir grand-chose sur votre Macintosh®». Effectivement, il s'en servait seulement pour faire du traitement de texte. Mais au cours de la discussion, je lui pose la question de savoir s'il a des contrats industriels et il me répond que justement il négocie un contrat industriel avec un grand de la pharmacie, contrat de 2 millions de dollars qu'il était en train de taper sur son ordinateur. Il était donc en train de se faire espionner en direct. Voilà l'univers dans lequel nous rentrons.

Cet exemple n'est pas directement lié à la vie privée de chacun, mais il montre que la menace est immanente c'est-à-dire qu'elle plane sur le réseau, et lorsque vous vous branchez sur le réseau, vous invitez en fait 600 millions d'internautes à venir dans votre salle à manger.

P. de Brem :

Je vais passer la parole à M. Pallez, à qui j'avais envie de demander si l'arsenal juridique actuel de la France pour protéger nos vies privées des attaques dues au développement des nouvelles technologies de l'information et de la communication est suffisant ou s'il est perfectible ?

C. Pallez :

Il est certainement perfectible, mais je pense qu'il est relativement suffisant. Il apparaît que la loi de 1978 a pris le tournant de l'Internet sans trop de difficultés. Elle s'est adaptée à l'évolution des technologies, même si, parfois, nous constatons que ce n'est pas totalement le cas comme avec l'exemple du *spam* que notre loi ne permet pas vraiment de traiter. C'est la raison pour laquelle une disposition législative est en cours de discussion pour l'interdire de manière très claire.

A l'inverse, je peux citer des exemples pour lesquels il apparaît que la législation répond bien. Avec la loi de 1978, nous avons les éléments pour traiter les problèmes liés aux techniques qui présentent des risques importants pour la vie privée, comme la géolocalisation.

Nous pouvons toujours aller plus loin ; c'est pourquoi cette loi est en cours de modification et elle va apporter quelques outils supplémentaires à la CNIL.

P. de Brem :

M. Stern, vous êtes spécialiste de la cryptographie. Jusqu'en 1999, celle-ci était légalement prohibée, ou plus exactement, réservée aux usages militaires et diplomatiques. Or, aujourd'hui, elle est autorisée, pour partie un peu grâce à vous puisque vous avez rédigé un rapport qui, dans un premier temps, était secret. Ce rapport conseillait au Gouvernement d'ouvrir cette cryptographie. C'est, d'une certaine façon, un plus pour les sociétés et pour les particuliers, qui peuvent protéger leurs correspondances, même s'ils ne le font pas encore beaucoup. Pourquoi a-t-il fallu attendre 1999 pour ouvrir l'utilisation de la cryptographie ?

J. Stern :

On ne peut pas dire que la cryptographie était interdite en 1999. On peut dire qu'il n'était pas facile de l'utiliser, surtout la cryptographie forte. Pourquoi ? La cryptographie était considérée comme une spécialité principalement diplomatique et militaire, donnant un avantage au pays qui la maîtrisait, et donc comme une activité régalienne. Je pourrais relater nombre d'histoires de défenses et d'attaques, de codes brisés, etc, durant les première et seconde guerres mondiales. Puis on sort de la seconde guerre mondiale et, doucement, on passe de la cryptographie, arme de guerre, à la situation actuelle où nous utilisons tous en permanence de la cryptographie sans le savoir. Presque tout le monde a aujourd'hui deux processeurs cryptographiques sur lui, l'un dans la carte bancaire et l'autre dans le téléphone GSM. Cela s'est donc fait petit à petit.

En 1999, on était déjà assez avancé puisqu'il existait des usages de la cryptographie, ne serait-ce que dans les cartes bancaires. Néanmoins pour les télécommunications, la logique d'un certain nombre de gouvernements était une logique de limitation, qui se traduisait, en France, par l'idée qu'on allait donner de la cryptographie «douce» aux gens comme vous et moi, et de la cryptographie forte à ceux qui en avaient vraiment besoin. Or, on développait, hors de notre «village gaulois», des produits simples d'emploi, y compris dans les navigateurs Internet, et l'on devait, lorsqu'on arrivait en France, troquer la cryptographie forte contre la cryptographie faible ! C'était devenu intenable, et beaucoup de personnes allant dans le même sens, il n'a pas été trop compliqué de faire comprendre qu'il fallait changer. Ces techniques utiles pour la protec-

tion de la confidentialité et de la vie privée se devaient d'être au service de tout le monde.

P. de Brem :

Je vous invite à poser vos questions.

Question :

En réaction aux propos de M. Longeon : n'importe qui peut installer très facilement sur son poste un pare-feu, un antivirus, voire même des logiciels de protection. Comment se fait-il qu'au CNRS, où les secrets valent plusieurs millions de dollars, ces outils ne soient pas suffisamment efficaces pour parer à toutes les attaques ?

R. Longeon :

Dans la sécurité, il y a des aspects techniques et des facteurs humains, et c'est toujours avec les facteurs humains que les choses se compliquent. Dans le cas, par exemple, du logiciel de reconnaissance vocale, les personnes en cause ont fait une démonstration d'utilisation du logiciel dans une université à l'étranger, et se sont fait «sniffer» leur mot de passe, c'est-à-dire que, sur le réseau, quelqu'un a capté le mot de passe de connexion sur leur système. La défaillance humaine se retrouve dans cet exemple car si l'on n'utilise pas de procédure sécurisée, on circule en clair sur le réseau, et la tentation est grande de capter le mot de passe. Ils auraient dû prendre un certain nombre de précautions, d'autant plus que c'étaient des informaticiens.

P. Lointier :

Je vais vous indiquer comment pénétrer sur un site avec un téléphone. Vous appelez disons le CNRS à midi moins cinq et vous vous présentez comme le nouvel adjoint de M. Longeon, qui est en congés en ce moment - bien sûr, vous aurez appelé quelques heures auparavant pour le savoir -, et vous dites que M. Untel, qui est un grand chef de l'entité, a un problème pour se connecter à tel serveur. Vous commencez à parler technique et vous pressez la personne de vous donner son mot de passe et son identifiant pour reconstruire la table d'adressage. Qu'avez-vous donné ? Vous avez donné l'information comme quoi vous faites partie de la maison puisque vous connaissez M. Longeon et que vous savez qu'il est absent ; vous avez menacé votre interlocuteur d'une gêne pour un grand chef s'il ne coopère pas à une demande aussi simple que donner un mot de passe. A votre avis, que fera la personne si elle n'a pas été sensibilisée ? Au regard de l'heure, elle sera d'autant plus pressée de régler ce type de cette situation. On appelle cela l'ingénierie sociale, qui est extrêmement utilisée pour obtenir un premier accès à un réseau d'entreprise ou d'administration.

R. Klapisch :

Je peux concevoir la malveillance car après tout, on sait que des gens dévalisent les banques, et il est clair et net que c'est un crime, dont on comprend la motivation, qui est de gagner de l'argent malhonnêtement. Ce qui me pose problème, c'est cette espèce de sport de gens qui, au début pour s'amuser, embêtent le monde, font du *spam*, etc.

Pour résoudre un problème, il faut d'abord le comprendre. Je veux bien qu'au début, ces gens voulaient prouver qu'ils étaient capables, mais tout le monde sait maintenant qu'on peut faire énormément de choses. Des études psychologiques ont-elles été faites pour permettre de cibler le profil de ces individus, de comprendre leurs motivations, et, éventuellement, de pouvoir y répondre, indépendamment de la technologie ?

P. Lointier :

Il n'existe aucune étude valable à ce jour. On entre dans le domaine de l'analyse comportementale ou du profilage, et tous les ressorts psychologiques, toutes les motivations humaines sont possibles pour la réalisation d'un virus ou pour s'introduire sur un réseau. Tous les cas de figure ont été rencontrés et il serait extrêmement dangereux de se dire qu'un pirate informatique est un gamin de 13 ans avec des boutons, des lunettes et qui a des problèmes avec le sexe opposé ! On trouve tous les profils. Certains auteurs de virus ont 40 ou 50 ans. L'année dernière, un pirate allemand très célèbre est décédé, et, depuis, reste dans la mémoire des pirates allemands. Il n'y a pas d'âge ni de profil psychologique ou sociétal, tout comme pour le terrorisme.

Question :

Je voudrais poser une question d'ordre éthique parce que, lorsque j'essaye d'introduire auprès des jeunes étudiants, la notion d'éthique dans l'éthique, je suis confronté à un problème qu'on pourrait nommer NSA (National Security Agency), Echelon, et autres activités peut-être illégales. Quand les Etats deviennent voyous et délinquants, que pouvons-nous faire ?

P. de Brem :

La NSA est un vaste système d'espionnage à l'usage des Américains et des Britanniques, et peut-être d'autres pays, la France n'en faisant pas partie. Que peut-on dire à des étudiants en informatique à qui l'on recommande de ne pas faire de piratage et qui s'aperçoivent que des Etats le font et le cachent ?

R. Longeon :

Il y a beaucoup de choses que les Etats font et que le particulier n'a pas le droit de faire, tuer son voisin par exemple. Cela étant, je suis persuadé qu'il y a, d'une manière ou d'une autre, des services secrets derrière toutes les malveillances qu'on repère actuellement, que ce soient les *spams*, les virus ou les intrusions. Des gens peuvent être manipulés à leur insu, d'autres tirant les ficelles par derrière.

Certaines observations vont dans ce sens. En observant la répartition de la contamination virale dans le

monde jusqu'en 1992-1993, on s'est aperçu que les virus étaient très présents en Europe de l'Est et en Union soviétique alors qu'il y avait très peu de machines et surtout très peu de MS-DOS. On pouvait donc imaginer qu'il y avait, malgré tout, des petits échanges d'«amitié» entre les blocs, qui se passaient sous forme de virus.

P. de Brem :

Parlons clair : il y avait très peu de PC et pourtant, c'était la région du monde la plus contaminée. Qu'est ce que cela signifiait ?

P. Lointier :

Que c'était la région du monde où l'on fabriquait le plus de virus. En 1990, j'avais été invité à Sofia par un collègue des services secrets pour parler de virologie, et effectivement, c'était un pays où l'on trouvait très peu de PC et encore moins de logiciels. Il existait donc deux sports nationaux en Bulgarie, le pays technologique des pays de l'Est : craquer les logiciels donc les contrefaire, ou faire sauter les sécurités qui existaient à l'époque et étudier la virologie informatique. Il est clair que les Bulgares ont beaucoup fait pour l'évolution technique des virus informatiques. L'exploitation qui en a été faite par ailleurs est un autre débat.

R. Longeon :

Au moment de la chute du mur de Berlin, on a vu des personnes, issues des services secrets, monter des sociétés d'antivirus.

P. de Brem :

Vous voulez dire que les services secrets bulgares, russes, est-allemands, produisaient des virus et les envoyaient là où ils voulaient nuire. J'imagine que tout le monde fait la même chose.

R. Longeon :

Bien sûr. C'est tout simplement une nouvelle dimension de la guerre.

Quand on regarde les *spams*, quelque chose semble bizarre : une personne qui veut vendre du Viagra®, on comprend bien que c'est pour faire de l'argent, mais à quoi sert-il d'envoyer mille fois le même message à la même personne ? Si elle n'en veut pas, c'est que vraiment, elle n'en a pas besoin. Donc il y a autre chose derrière.

On peut bien sûr penser que certaines personnes ont l'esprit un peu tordu et que cela les amuse d'empoisonner leur voisin, mais dans un pays, il n'y a quand même pas des milliers de gens tordus. Il y a donc probablement autre chose derrière.

Si l'on associe tout cela à d'autres faits : par exemple que l'armée chinoise a monté une brigade d'informaticiens de combat ; que les équipements d'extrémité fabriqués dans le monde sont sérieusement contrôlés par les services secrets qui ont des gens à eux dans la place, jusqu'au directeur général ou au fondateur de la société, on ne peut s'empêcher de penser que s'il existe effectivement un sport qui consiste à parader sur les réseaux, il y a aussi, derrière, des gens qui manipulent, soit par intérêt économique, soit parce que nous sommes dans un monde de compétition.

P. de Brem :

En ce qui concerne les *spams*, je vous présente certains que j'ai reçus aujourd'hui : pour un site de rencontres, un site de Viagra®, un patch pour perdre du poids, pour faire un voyage, et enfin un *spam* que je n'avais encore jamais reçu, sur le principe suivant : «Je vous vends une méthode pour vendre et acheter aux enchères bien mieux que les autres sur eBay, le site de vente aux enchères, et vous allez pouvoir me payer avec le système PayPal.» Est-ce ce qu'on appelle du *phishing* ? Qu'est-ce que le *phishing* ?

P. Lointier :

En tant que citoyens, nous sommes confrontés à trois problèmes :

- Le *spam*, où vous recevez des choses que vous ne désirez pas.
- Le *phishing*, élément marquant de la fin 2003 ; *phishing* est un néologisme, de *fish*, pêcher, en anglais, excepté le fait que dans ce cas-là, on pêche des mots de passe et des informations confidentielles. Cela repose toujours sur des démarches d'ingénierie sociale comme dans l'exemple du téléphone précédemment. Pour citer un exemple arrivé à la fin de l'automne, vous allez recevoir un e-mail vous disant : «Bonjour, je suis la Bank of England, nous avons amélioré notre système de sécurité, veuillez cliquer sur tel lien pour en bénéficier.», ou bien : «Nous avons besoin de telle information, veuillez nous la transmettre.» La personne est en confiance soit parce que l'e-mail a l'en-tête «Bank of England» soit parce qu'elle a cliqué sur un lien qui a l'apparence du lien de la banque. En fait c'est un contre-site ou faux site sur lequel on va lui demander de taper des informations qui seront ensuite exploitées. Ces informations ne sont pas simplement le numéro de votre carte bancaire et sa date d'expiration, mais peuvent être également votre date de naissance, les noms de vos père et mère, informations utilisées par différents organismes pour vous authentifier lorsque vous faites un achat par téléphone ou par Internet. Ces sites de *phishing* vont également vous demander les trois chiffres qui sont derrière votre carte confidentielle et qui permettent soi-disant de lutter contre la fraude sur Internet puisque normalement ce numéro n'apparaît pas ; or là, c'est vous-même qui allez le donner. Donc le *phishing* repose sur la crédulité, l'insouciance ou la méconnaissance des gens.
- La troisième menace pour les citoyens est complètement externe et encore moins contrôlable car, si l'on dispose de logiciels filtrants contre les *spams*, et s'il suffit, pour se prémunir du *phishing*, d'être vigilant

lorsqu'on reçoit un message inhabituel de sa banque ou d'un organisme classique, là, ce sont les données financières ou les données privées qui sont stockées sur des sites pour lesquels vous n'avez aucune garantie de sécurité. On en revient au problème de la loi de 1978 où peut-être, en France, on pourrait sévir contre un Web français qui aurait été négligent en termes de sécurité. Mais maintenant on fait des achats partout sur l'Internet et vous ne savez pas où sont stockées vos données financières et privées. Imaginez qu'une personne usurpe votre identité sur l'Internet. Si l'on pirate votre carte bancaire ou si l'on utilise votre numéro de téléphone pour faire du harcèlement, vous changez de carte ou de numéro de téléphone et c'est terminé. En revanche, si vos données privées sont récupérées par du *phishing* ou sur des sites légaux mais qui ont été mal protégés et piratés, c'est toute votre vie, votre «légende» qui peut être contrefaite et utilisée par des personnes malveillantes. Je n'ai pas connaissance de telles affaires mais c'est une vraie menace, car aujourd'hui, nous sommes dans un Web mondialisé et vos informations de citoyens vont être sur des sites pour lesquels, malheureusement, nous n'aurons pas forcément une bonne visibilité du niveau de protection et de sécurité des informations financières et privées qui y sont stockées.

C. Pallez :

Je voudrais faire la remarque préalable que tout le débat que nous avons amorcé tourne autour de l'idée que les menaces à la vie privée viennent de délinquants ou d'actes de piratage, de malveillance. Or, je vais vous citer un exemple sans malveillance, celui des Etats-Unis qui ont exigé des compagnies aériennes qu'elles leur transmettent les données personnelles de leurs passagers sur les vols Paris-New York ou Paris-Los Angeles, notamment les numéros de cartes bancaires ou de téléphone, soit peut-être des centaines de milliers de numéros de cartes bancaires ou de numéros de téléphones privés qui ont été fournis aux autorités américaines.

On n'est plus ici dans le domaine du piratage, mais bien dans une forme de légalité - contestée par les pays européens -, dans laquelle des masses de données personnelles sont transférées. Attention donc, ne regardons pas le problème de l'atteinte à la vie privée uniquement sous l'angle du piratage informatique, qui est certes très important, mais il existe des phénomènes beaucoup plus concrets qui sont tout aussi massifs.

P. de Brem :

Vous me citiez l'exemple de la SNCF.

C. Pallez :

Oui, je peux prendre un exemple encore plus trivial : je suis toujours frappé, chaque fois que je fais une réservation de billet SNCF, de constater que si je veux avoir simplement la réservation, sans même effectuer de paiement par carte bancaire, je dois cliquer sur la case : «Vous adhérez aux conditions générales» ; en adhérant à ces conditions générales, qu'évidemment je ne vais pas lire, j'accepte sans le savoir de recevoir ensuite régulièrement des messages, que j'appellerais presque du *spam*, qui m'incitent à acheter des voyages à prix réduits pour des destinations exotiques, tout cela dans le cadre de la SNCF.

Donc il existe beaucoup de phénomènes très concrets, touchant à notre vie quotidienne, qui ne sont pas uniquement des questions de piratage, et dans lesquels la vie privée est en jeu.

Question :

Je suis particulièrement satisfait des deux dernières interventions parce que j'avais l'impression, depuis le début du débat, qu'on s'éloignait de la vie privée, notamment quand vous parliez des services secrets, de l'espionnage industriel, qui sont un autre débat.

Ma première question concerne les cartes bancaires, qui fonctionnent toujours avec un code de quatre caractères, ce qui est notoirement insuffisant pour avoir une protection ; il est facile de mettre en œuvre des moulinettes pour trouver le code secret en question. Pourquoi ne sommes-nous pas passés à des codes plus sophistiqués ? J'ajoute que les codes des cartes bancaires sont numériques et même pas alphanumériques. Je note que, lorsqu'on travaille avec un simple minitel, si l'on veut correspondre avec sa banque, on a un identifiant d'une dizaine de caractères, qui peuvent être ou non alphanumériques, et un code d'accès à six caractères, qui peuvent être aussi alphanumériques, ce qui est quand même un peu plus sérieux que les quatre chiffres de la carte bancaire.

Ma seconde question concerne l'Internet. Quand je reçois des courriers publicitaires, il est indiqué très souvent en bas des correspondances que je peux m'adresser à la CNIL pour me faire retirer de ces listes de publipostage. Cela ne me coûte qu'un timbre et je n'ai pas besoin de pare-feu sur mon PC ! Quand cela m'arrive sur mon PC avec les *spams*, à qui dois-je m'adresser pour me protéger, dans ma vie privée, de toutes ces désagréments, qui ne sont pas de mon fait mais qui sont dus au média de transmission qu'est l'Internet ?

J. Stern :

Je vais un peu prendre la défense de la carte bancaire. Le code à quatre chiffres que nous connaissons tous est l'identification du porteur à la carte. On peut juger que c'est insuffisant, j'y reviendrai après, mais une fois que cette identification du porteur à la carte est faite, c'est la carte qui travaille et, à l'intérieur de sa puce, elle a un certain nombre d'outils cryptographiques qui font qu'il n'est pas simple de la contrefaire. Il y a donc deux étapes : le code secret pour prouver que c'est le légitime propriétaire de la carte qui est présent et non quelqu'un d'autre, et ensuite, la carte elle-même, qui met en œuvre les mécanismes cryptographiques présents à l'intérieur de sa puce.

On peut juger que les quatre chiffres sont insuffisants et qu'on aurait pu demander au porteur de taper six chiffres. Par exemple, dans le cas de vol de la carte, cela rendrait le code confidentiel plus difficile à deviner. Le danger est que l'utilisateur tombe alors dans ce qu'il ne faut surtout pas faire, à savoir copier son code sous forme d'un numéro de téléphone par exemple, car les voleurs savent très bien où chercher les codes de cartes de crédit dans un carnet d'adresses. Donc si l'on n'a pas mis six chiffres, c'était sans doute parce qu'on pensait que les gens pouvaient sans problème mémoriser quatre chiffres, mais plus difficilement six. Dans certains pays, il n'existe même pas de code confidentiel, en Angleterre notamment.

Pour vous rassurer, les quatre chiffres ne sont pas la seule protection de la carte de crédit.

En cas de vol, la seule protection restante est le blocage de la carte après trois essais de code confidentiel. Est-ce suffisant ou non au regard du risque que vous courez contractuellement ? Je n'en sais rien. Je peux juste dire qu'il existe une autre cryptographie dans les cartes que celle des quatre chiffres.

P. Lointier :

Trois techniques existent pour récupérer le code, qu'il soit à trois, quatre ou six chiffres.

La première : lorsque c'est un portefeuille ou un sac à main qui est volé, il y a de fortes chances qu'on trouve quelque part le code, qui aura été vaguement maquillé comme un numéro de téléphone ou une addition quelconque. Les professionnels ont le nez pour cela.

La seconde méthode a été utilisée notamment dans le sud de la France : vous venez de voler une carte à une personne dont vous avez les coordonnées téléphoniques puisque vous détenez l'ensemble de ses papiers. Vous lui téléphonez : «Bonjour, je suis M. Untel de la brigade de l'Office central de lutte contre la criminalité. On vient de retrouver votre carte bancaire, mais j'ai besoin de votre code confidentiel pour pouvoir porter plainte auprès du GIE des cartes bancaires.» Ou bien les délinquants appelaient d'une cabine téléphonique, avec un bruit sonore de guichet bancaire, et demandaient à la personne pour une raison x ou y de rappeler un numéro qui était celui de la cabine publique. La personne était donc en confiance puisqu'elle rappelait un numéro où il y avait un bruit d'activité bancaire ; sous l'effet du stress d'avoir perdu sa carte et de l'avoir retrouvée une heure après, elle donnait le code.

La troisième méthode, qui sévit beaucoup en ce moment à Paris, est le *skimming* : une goulotte lectrice de bande magnétique est collée sur la fente du distributeur dans laquelle vous insérez la carte ; une microcaméra placée au-dessus du distributeur va vous voir composer le code confidentiel. Dans ce type de réseaux, ce dispositif est placé quelques heures sur un distributeur, les informations sont transmises par GSM immédiatement à un collaborateur un peu plus loin, et les données partent immédiatement sur les pays de l'Est où il y a contrefaçon et exploitation de la carte.

P. de Brem :

Contrefaçon, c'est-à-dire qu'une fausse carte est créée en en connaissant tous les détails.

P. Lointier :

Et en plus on a le code qui permet de faire un retrait. Donc la longueur du code n'a rien à voir.

P. de Brem :

A qui devons-nous nous plaindre en cas de *spams* ? A vous, M. Pallez ?

C. Pallez :

Dans le cas d'un courrier papier non sollicité, on se plaint d'abord à la personne qui l'a envoyé, en lui demandant de ne plus en envoyer, et si elle continue, on se plaint à la CNIL.

A priori, pour le *spam*, la démarche est la même : on s'adresse à l'expéditeur du *spam*, et ensuite à la CNIL. Il est évident que les expéditeurs de *spams* sont souvent absolument injoignables ou ne répondent pas ; c'est la caractéristique de cette profession. Dans ce cas, on peut se plaindre à la CNIL, qui a d'ailleurs monté des dossiers et fait des dénonciations au Parquet pour cinq sociétés. Pour le moment, cela n'a pas donné des résultats extraordinaires, néanmoins une société passe en jugement en juin 2004 devant le Tribunal correctionnel de Paris.

Question :

Bonsoir. Je suis étudiante en droit et mon mémoire porte exactement sur votre sujet, dans le droit américain et dans le droit européen. J'ai une question technique, une question juridique et une question générale.

Question technique : comment se passe techniquement la cybersurveillance ? Comment un Etat peut-il collecter des informations sur un utilisateur d'Internet ? Comment peut-on collecter les informations par les *cookies* ?

Question juridique : j'ai le sentiment que, dans ce débat, on a mis dans le même groupe les grandes sociétés et les simples utilisateurs d'Internet. M. Pallez, pourriez-vous nous parler de la *self-regulation* qui se fait aux Etats-Unis ? Pourquoi cela dérange-t-il la société qu'un Etat régule l'Internet ?

Question générale : quels sont les risques d'invasion de la vie privée dans les *data flows* ou *data transfers*, par exemple entre pays ou banques qui s'envoient des données ?

P. Lointier :

Je ne fais pas partie des organes étatiques qui surveillent les citoyens.

P. de Brem :

La question est technique : comment surveille t-on ?

P. Lointier :

Tout ce que contient une puce ou un système de traitement, tout ce qui communique ou qui passe par la magné-

tosphère peut être capté. On peut localiser les personnes. Certains Etats dépensent beaucoup d'argent pour récupérer ces données ; d'autres Etats, un peu moins riches, le font de façon artisanale, mais tous les Etats le font.

Je prendrai pour exemple la façon dont, au milieu des années quatre-vingt-dix, l'Allemagne a réussi à localiser le reste de la bande à Baader en regardant la consommation d'électricité des appartements loués. Ces gens avaient besoin de planques, en changeaient souvent et donc louaient à l'avance des appartements. En regardant la consommation d'électricité des appartements loués, on pouvait observer des pics de consommation et des périodes sans consommation. On corrélait ensuite ces informations avec d'autres fichiers, pour savoir si l'on avait affaire à des voyageurs de commerce, des capitaines au long cours, des pilotes de ligne, etc. ; quand ce n'était pas le cas, les personnes étaient à priori suspectes et l'on envoyait des enquêteurs sur place. Le croisement des fichiers était assez efficace puisque, sur plusieurs grandes villes, ils étaient parvenus à 300 suspects possibles, ce qui, pour un organisme d'Etat, est facile à vérifier. Ils ont finalement obtenu les résultats qu'ils recherchaient.

P. de Brem :

Ce qui est étonnant, c'est le traitement de la donnée, et que quelque chose d'aussi simple et banal que la consommation d'électricité puisse mettre la police sur la piste d'un terroriste.

P. Lointier :

Regardez comment les assassins du préfet Erignac ont été localisés : avec un téléphone portable.

C. Pallez :

Avant de répondre à la seconde question, je vais me permettre d'ajouter quelque chose à la réponse à la première question.

En ce qui concerne la cybersurveillance massive des citoyens, je vais vous donner un exemple français que nous allons vivre : légalement, l'ensemble des données de connexions téléphoniques Internet des personnes résidant en France seront conservées pendant un an par les opérateurs de téléphonie à des fins d'exploitation par les autorités judiciaires notamment, et la police de façon plus générale. Voilà un exemple massif de cybersurveillance des citoyens. On peut en penser ce qu'on veut, mais c'est la loi qui l'a décidé.

P. de Brem :

De quelles données s'agit-il ?

C. Pallez :

L'heure à laquelle vous avez appelé ou l'heure à laquelle vous vous êtes connecté à tel site Internet, sur quel appareil, c'est-à-dire tout ce qui concerne la communication téléphonique, mais pas son contenu. Ce sont tous les éléments qui permettent d'identifier la communication téléphonique (téléphone et Internet).

P. Lointier :

Il faut tempérer car ce n'est pas l'Etat qui se charge de stocker ces données, mais les opérateurs, qui ne donnent ces données à la police que sur requête d'autorités judiciaires. C'est donc encadré par une procédure judiciaire.

C. Pallez :

Bien sûr ! Mais c'est une procédure judiciaire extrêmement banale, au même titre que les écoutes téléphoniques qui sont faites par dizaines de milliers par an. C'est le moyen d'enquête le plus banal de la justice et cela fait partie de la cybersurveillance. Bien évidemment, nous ne sommes pas des délinquants donc nous ne nous sentons pas concernés, mais l'on peut tout de même se poser des questions.

J'en viens maintenant à la seconde question sur la *self-regulation* par opposition à une loi.

P. de Brem :

La *self-regulation* est l'autorégulation. En quoi consiste- t-elle ?

C. Pallez :

C'est une approche plutôt anglo-saxonne, qui consiste à dire qu'en l'absence de loi imposant des principes, chacun décide d'adhérer à des codes de conduite, des chartes, et les met en avant sur son site, ce que font beaucoup d'entreprises américaines. Cette approche, qui n'est pas l'approche française, est intéressante même si elle a ses limites. Elle correspond à un certain état du droit, une certaine culture juridique. L'engagement que prend une personne privée est très fort, et de ce fait, la violation de cet engagement peut être sanctionnée de manière très forte par le juge.

En ce qui concerne les transferts de données, c'est un vaste sujet sur lequel une autorité nationale comme la nôtre a le moins de prise. D'après l'expérience pratique de la CNIL dans ce domaine, les données qui sont le plus transférées actuellement sont celles concernant les salariés, parce que les entreprises sont multinationales et que l'on gère le personnel au niveau central, aux Etats-Unis ou ailleurs. Certaines entreprises, sur lesquelles on peut avoir un certain contrôle, se conduisent correctement, alors que d'autres le font sans qu'on s'en aperçoive et sans que cela se fasse dans le respect de règles garantissant un droit de regard pour les personnes dont on transfère les données. C'est un sujet tellement complexe et vaste que j'hésite à l'aborder plus que je ne viens de le faire.

P. de Brem :

Donc les fournisseurs d'accès sont tenus maintenant de garder pendant un an des données importantes. Les sites Internet sur lesquels vous vous rendez gardent égale-

ment beaucoup de choses en mémoire. On vous en donne une démonstration sur le site de la CNIL : quand vous vous connectez à ce site, on vous indique que le site connaît l'adresse IP de votre machine, c'est-à-dire le chiffre qui vous identifie. Il sait quel ordinateur, quel système d'exploitation et quel navigateur vous utilisez. Il sait quel a été votre parcours sur le site et comment vous en êtes arrivé à ces différentes pages. De seconde en seconde, on sait où vous vous êtes rendu. On peut même vous dire : «Bonjour, c'est la troisième fois que vous consultez cette rubrique ; la dernière fois, c'était le 15 janvier 2004.» Les ordinateurs ont de la mémoire !

Question :

En vous écoutant, on est convaincu qu'il n'existe aucune protection de la vie privée. Je m'adresse en particulier au représentant de la CNIL : en ce qui concerne les sites de dépôt de curriculum vitae par exemple, qui intéressent les employés jusqu'aux cadres supérieurs, certaines sociétés sont américaines ou anglo-américaines ou avec des capitaux américains ; il en est de même pour des logiciels d'échange d'e-mails. Personnellement, je suis très pessimiste sur le respect de la vie privée.

Ma deuxième remarque concerne ces *spams* en provenance de particuliers africains proposant des pourcentages sur des sommes détournées par d'anciens gouvernants. Quelles sont les possibilités de la CNIL pour mettre fin à ce genre de *spams* ?

C. Pallez :

La CNIL n'est pas la commission de la vie privée mais la commission de la protection des données.

La vie privée est aussi une question d'auto-protection c'est-à-dire ce que l'on consent à exposer. En mettant votre CV sur un site, vous acceptez que ce CV soit transféré à certaines branches de la même organisation. Si vous avez le sentiment qu'il y a eu, à partir de là, un comportement anormal, cela devrait donner lieu à une plainte et l'on pourra peut-être faire quelque chose. Je reconnais que la réponse est légère par rapport à l'importance des problèmes que vous citez.

En ce qui concerne le fils de Mobutu et autres dictateurs africains, cela ne relève pas de la compétence de la CNIL. Ces messages sont une escroquerie manifeste et relèvent des tribunaux, qui d'ailleurs ne sont guère en mesure d'agir.

P. de Brem :

Néanmoins, il y a une espèce de mondialisation de la délinquance et du crime avec l'Internet, et l'on imagine assez facilement que certains pays puissent avoir du mal à faire respecter certaines règles dans d'autres pays. M. Longeon, vous parliez de paradis de données, comme il y a des paradis fiscaux, où nos données peuvent être conservées, sans CNIL pour protéger nos droits.

C. Pallez :

Effectivement, certaines zones sont assez correctement protégées comme la zone européenne et quelques autres pays. Aux Etats-Unis, de larges possibilités d'actions existent, et les associations sont vigilantes et actives. Enfin, il y a beaucoup de pays d'Asie où la notion de protection des données n'est même pas une notion qui puisse être comprise, par un Chinois par exemple.

Question :

Je voudrais savoir si ce qui m'arrive de temps en temps arrive aussi à d'autres personnes. Une fois tous les quinze jours, lorsque je me connecte à Club Internet, la page Microsoft s'affiche. Ma réaction est immédiatement de «scroller» pour passer sur une autre adresse. D'autres personnes rencontrent-elles ce type de désagrément ? Ma réaction est-elle suffisante pour me préserver ?

P. de Brem :

Quelle est votre crainte ?

L'intervenante :

Qu'on vienne faire un tour chez moi et qu'on regarde tout ce que j'ai fait, à qui j'ai écrit pendant les quinze derniers jours... C'est extrêmement désagréable. Je suis chez Club Internet et pas chez Microsoft.

P. de Brem :

Les craintes de madame sont-elles fondées ?

P. Lointier :

Il s'agit de Windows Update, qui est un système de mise à jour automatique mis en place par Microsoft. C'est vous qui avez accepté - vous avez dû configurer votre ordinateur. Vous pouvez toujours refuser, mais si vous ne mettez pas à jour votre version de Windows®, ce ne sera plus Microsoft qui viendra chez vous, mais le reste du monde !

P. de Brem :

Il faut rassurer madame : lorsque la page de Microsoft s'affiche, cela ne signifie pas que Microsoft regarde.

P. Lointier :

Si, malheureusement, c'est ce qui se passe. Windows Update commence par faire un balayage de votre machine pour voir quel système vous avez, si vous avez bien installé les derniers *patchs* de sécurité, et s'il vous en manque un, il vous le propose. Il charge ce qu'il a envie de charger dans votre machine.

P. de Brem :

Le fait de «scroller» tout de suite est-il suffisant ?

P. Lointier :

Vous pouvez aller plus vite que les électrons, mais c'est rare ! Le mieux est de désactiver Windows Update,

si, entre deux risques, vous préférez le pire, celui de ne pas mettre à jour votre système. Vous pouvez aussi faire fonctionner Windows Update sur demande plutôt que cela se fasse tout seul.

P. de Brem :

Windows Update est un système qui met à jour votre système d'exploitation, et vous avez intérêt à faire ces mises à jour qui réparent des failles découvertes dans le système et vous protègent ainsi de possibles attaques.

P. Lointier :

En bonne logique, à moins que vous ne soyez un concurrent sérieux de Microsoft, il n'y a aucune raison que Microsoft aille collecter vos courriers personnels.

Question :

Je voudrais savoir si les logiciels libres protègent mieux la vie privée que les logiciels Microsoft ?

P. de Brem :

Il faut rappeler au préalable ce qu'est le logiciel libre.

P. Lointier :

Il existe surtout des «logiciels propriétaires», qui sont notamment ceux de Microsoft ou des grandes industries de la fabrication de programmes. Il y a quelques années est apparue une nouvelle mouvance dans la programmation qui consistait, pour des groupes d'informaticiens, à créer des codes source de programme et surtout à les laisser accessibles via l'Internet. Ce phénomène est historiquement apparu lorsque Microsoft a quitté Windows 98®, qui devenait instable, c'est à dire qui «plantait», pour aller vers Windows 2000® ou Windows NT®.

En fait, la grande force du logiciel libre est d'être un système stable, mais il faut bien voir que ces logiciels libres sont des systèmes d'exploitation de type Unix (qu'on appelle Linux), qui sont des usines à gaz ; si vous n'êtes pas du domaine, vous ne saurez pas les paramétrer. C'est très sécurisé pour des gens qui savent les paramétrer, mais si vous achetez un Linux dans sa boîte ou si vous le téléchargez, vous aurez un niveau de sécurité qu'il faudra ensuite renforcer. La force du libre est sa stabilité.

Deux phénomènes ont été intéressants en 2003.

D'une part une conférence de pirates, au cours de laquelle un étudiant a expliqué l'exercice de style qu'il a fait : en 48 h, il a trouvé des failles de sécurité gravissimes sur un des noyaux de ces logiciels libres, le noyau étant le cœur du système d'exploitation. Cela démontre qu'un système libre n'est pas plus sécurisé, qu'il a des failles de sécurité. L'avantage du système libre, c'est que la communauté de ses programmeurs réagit extrêmement vite. L'étudiant a prévenu le groupe qui programmait, qui a «patché» et corrigé immédiatement... jusqu'à la prochaine faille.

D'autre part, en octobre dernier, quelqu'un a introduit un cheval de Troyes dans le noyau d'un de ces logiciels libres - un cheval de Troyes est un programme permettant de prendre le contrôle d'une machine à l'insu de son utilisateur. Il y a donc eu compromission du noyau mis en ligne sur un serveur pour que tout le monde puisse le télécharger. Le logiciel libre n'est pas une panacée en soi car il y a des gens qui veulent aujourd'hui compromettre ces systèmes. Mais, par exemple, cette attaque contre le serveur de distribution du noyau n'a duré que quelques heures parce qu'ils ont été extrêmement réactifs.

Cela signifie que, par rapport au logiciel libre, on trouve deux populations : d'une part, les personnes qui sont du domaine ou un peu «branchées» sur ce domaine, et qui vont suivre les avis de sécurité, recevoir les listes de diffusion des groupes de programmeurs, et qui, de ce fait, auront une bonne sécurité ; d'autre part, l'internaute lambda, qui va acheter un Linux, un Redat, un Debian, un Free Bsd ou autre, qu'il ne va pas savoir sécuriser, c'est-à-dire configurer, qui va rester avec la même version pendant un an, et donc son système ne sera pas plus sécurisé que s'il avait Windows®.

Les systèmes libres, c'est bien quand on est du métier, mais pour la grande majorité des gens, ils resteront toujours exposés à des volontés de compromission de ces noyaux, qui sont de plus en plus répandues.

Question :

Ma question s'adresse à M. Lointier. Je rebondis sur ce que vous venez de dire. Pour les sociétés comme pour les privés, l'achat d'un pare-feu américain me semble illusoire puisque les services de renseignements peuvent récupérer toutes les données via les sociétés américaines. Doit-on utiliser un pare-feu français... qui lui-même sera piraté par les services de renseignements français !

P. de Brem :

Un pare-feu est un système qui protège contre certaines intrusions.

P. Lointier :

Votre question appelle une réponse vaste. Je reviendrai sur les propos de monsieur par rapport à Echelon, système d'obédience américaine. Personnellement, je ne me soucie pas d'Echelon, qui est un réseau de surveillance satellitaire et également par câble sous-marin.

Dans le cycle du renseignement, vous avez plusieurs étapes : d'abord une étape d'interception, ensuite une étape de traitement de l'information, de collation, de remise en perspective, et enfin une étape de diffusion à la personne qui en a besoin. Il est donc fort probable que les informations vous concernant ne les intéressent pas ou ne feront jamais l'objet d'un traitement.

La seconde remarque concernant Echelon est que l'interception est une chose, mais qu'après, il faut diffuser au bon moment et à la bonne personne. Les événements de 2001 ont bien montré que le renseignement électronique n'a pas suffi, alors que les informations existaient et ne demandaient qu'à être gérées correctement.

Je ne me soucie pas d'Echelon mais de *toutes* les interceptions. La France, et tous les pays industrialisés, ont des réseaux d'interception. Le problème n'est pas de se dire qu'Echelon existe, mais que, lorsque vous êtes chercheur ou VIP d'une entreprise dans une activité sensible, il faut partir du postulat que vous êtes interceptable, et donc aller vers des moyens de chiffrement qui vont vous protéger ou améliorer votre protection.

Donc au lieu de parler systématiquement d'Echelon, je préférerais qu'on fasse la promotion de blocs cryptographiques sur des téléphones GSM pour que les gens qui sont à l'étranger aient des téléphones sécurisés. La sécurité n'est pas une ligne Maginot, mais une défense en profondeur. Vous pouvez très bien avoir un pare-feu d'une marque et un système de détection d'une autre marque, qui sera peut-être américain, mais pas forcément de la même obédience, ou vous pouvez avoir des produits français. Il faut arrêter de dire : «C'est américain, donc c'est dangereux.» ! Si des sociétés américaines veulent faire du renseignement, elles le feront à travers des Français et des firmes françaises.

Question :

Une question pour M. Pallez. Je suis l'auteur du livre *Halte au spam*. J'ai une question au sujet de la loi informatique et libertés de 1978, qui est vraiment un grand texte - la France a été un précurseur dans ce domaine. J'ai eu l'occasion d'interviewer des victimes de *spams*, et aussi des *spamers*, surtout des M. Jourdain du *spam* qui me disent qu'ils ne savaient pas qu'il existait une loi.

Cela m'inquiète d'autant plus lorsque je suis le projet de loi actuel, passé il y a quelques jours en seconde lecture à l'Assemblée et qui passera prochainement au Sénat. Cette loi, personne ne la comprend ou ne veut la comprendre - on voit aujourd'hui des prestataires techniques monter en épingle certaines décisions. Comment peut-on espérer qu'une loi soit appliquée et protège le citoyen si personne ne la comprend ? Le texte tel qu'il est présenté, notamment sur le site de la CNIL, qui fait d'ailleurs beaucoup d'efforts d'explications, n'est pas très compréhensible. A moins d'être juriste, on ne comprend pas bien quels sont nos droits. Avec le nouveau texte pour la confiance dans l'économie numérique, plusieurs chapitres, dont l'article 14, vont traiter de la publicité électronique - et non pas du *spam*, car ce n'est pas une loi anti-*spam*. Mon inquiétude est que personne ne fasse les efforts d'explications. Seuls les juristes, les professionnels, un petit cercle d'initiés vont comprendre.

P. de Brem :

Expliquez-nous cette loi, et n'est-elle pas trop compliquée ?

C. Pallez :

Il n'est effectivement pas évident de comprendre que la loi de 1978 s'applique aux *spams*, parce qu'il faut des raisonnements complexes pour se dire que s'il y a *spam* c'est qu'il y a eu collecte d'adresses électroniques sur les espaces publics d'Internet ou ailleurs.

La loi pour la confiance dans l'économie numérique et son article 14, auxquels vous faites allusion, rend, d'une certaine façon, les choses beaucoup plus simples puisque la prospection par envoi de courriers électroniques non sollicités est interdite ; une exigence de consentement des personnes pour recevoir de tels courriers est nécessaire.

Les choses sont plus simples mais il faudra néanmoins les expliquer, et c'est le travail de la CNIL - nous le faisons plus ou moins bien, avec les moyens dont nous disposons, et ce n'est pas forcément parfait. Je dois dire aussi que le Gouvernement commence à prendre les choses très au sérieux puisque demain a lieu la première réunion du groupe mis en place par les services du Premier Ministre contre le *spam*, qui va se mettre au travail et faire, je pense, un peu avancer les choses dans la société française. Ce phénomène est donc pris au sérieux, et effectivement, il y a beaucoup de pédagogie à faire. Néanmoins, les limites sont que les *spamers* sont probablement ailleurs qu'en France, ce qui explique qu'on ait des difficultés à les contrer.

P. de Brem :

Il faut rappeler qu'en Europe, un e-mail sur deux est un *spam* et qu'aux Etats-Unis, ce sont trois e-mails sur quatre.

C. Pallez :

Je voudrais juste ajouter un point concernant cette démarche gouvernementale : un site officiel français sur le *spam* vient d'être ouvert, pour informer les gens et avoir une remontée d'information.

Question :

J'aimerais revenir sur la protection des données personnelles au travers des anti-virus. Quand j'achète un anti-virus, et que je l'installe, on me propose ensuite régulièrement des mises à jour. Qu'en est-il de ces mises à jour ? Que se passe-t-il réellement ? J'imagine que lorsqu'on visualise le contenu de mon disque pour voir si tout se passe bien, on peut avoir d'autres objectifs en tête, à moins que ce ne soit ma paranoïa qui parle !

P. Lointier :

A mon avis, oui ! Il s'agit d'une mise à jour des signatures de virus. Une base de signatures, ce sont des caractères informatiques hexadécimaux permettant d'identifier le virus lorsqu'il risque d'arriver sur votre machine. Donc pour faire une mise à jour d'un anti-virus qui le nécessite - car il existe d'autres modes de lutte contre les virus -, il faut effectivement enrichir la base de signatures pour détecter les nouveaux virus. Soit cette mise à jour se fait automatiquement si vous avez sélectionné l'option automatique, soit vous allez récupérer vous-même la dernière base sur le site du fournisseur du produit, et dans ce cas vous voyez bien qu'il n'y a pas aspiration de votre site.

Je pense que c'est de la paranoïa que de s'imaginer que l'éditeur va complètement balayer votre disque - pour y voir quoi et en faire quoi ? -, et que, de manière automatique et systématique, on va aspirer tous les disques durs à chaque mise à jour d'un anti-virus ou d'un logiciel Windows®. Il existe d'autres menaces beaucoup plus fortes à travers le *phishing*, avec des gens qui vont vous cibler.

Question :

J'imagine que le simple citoyen que je suis parmi les six milliards de la planète n'intéresse pas trop ces grandes entreprises, mais ne peut-on pas récupérer des informations statistiques concernant les populations ?

P. Lointier

Je crois qu'un des dangers important est là. Aujourd'hui, l'informatique représente une révolution par la capacité de traitement : on peut analyser plusieurs centaines de milliers de pages Web à l'heure. Le danger est que ces données soient récupérées pour en tirer des informations, et à partir de là, une connaissance en vue d'un objectif. On peut imaginer par exemple que des entreprises ayant besoin de faire des études de marché, collectent des données ciblées en fonction d'un certain nombre de critères et en tirent des informations. Ce n'est pas directement une atteinte à la vie privée des gens, néanmoins on essaye de tout connaître sur vous pour pouvoir mieux vous vendre des produits, c'est-à-dire vous manipuler.

P. de Brem :

Nous avons ici l'un des grands spécialistes français, sinon mondiaux, de la cryptographie, Jacques Stern, qui n'a pas beaucoup parlé, et M. Klapisch a une question à lui poser.

R. Klapisch :

Nous avons parlé des cartes à puces ; lorsque je veux acheter un livre chez Amazon, on me demande de donner mon numéro de carte de crédit et l'on me dit que le site est sécurisé. Comment se passe cette sécurisation et est-elle, à votre avis, fiable ? Peut-on donner son numéro de carte de crédit et que risque-t-on ?

P. de Brem :

Achetez-vous sur Amazon, M. Stern ?

J. Stern :

Je suis un peu comme Pascal Lointier c'est-à-dire que je n'ai pas très peur d'Echelon, et je n'ai plus peur non plus de transmettre un numéro de carte de crédit sur l'Internet si j'achète sur un grand site sécurisé par le protocole cryptographique qu'on appelle SSL, qui est une méthode assez simple, sans doute pas fiable à 100 %, mais suffisamment pour éliminer nombre d'attaquants, dont le but serait juste d'observer l'information qui transite entre vous-même et le site sur lequel vous achetez.

Quand vous utilisez votre navigateur et que SSL est actif, vous avez un petit cadenas qui se ferme. Bien sûr M. Lointier va m'expliquer que ce n'est pas parce que l'image du cadenas se ferme que le cadenas se ferme vraiment, mais cela ne m'inquiète pas trop.

Ce qui m'inquiète beaucoup plus, et cela a été mentionné à plusieurs reprises, c'est de savoir comment sera conservé mon numéro de carte de crédit une fois envoyé, par exemple pour l'achat de billets pour une exposition - je préfère deux minutes sur le Net que deux heures de queue dans le froid ! Quand je constate que, la fois suivante, je peux de nouveau payer sans redonner mon numéro de carte de crédit, cela m'ennuie plus car cela veut dire qu'il a été archivé, et je ne sais pas comment la base de données qui détient mon numéro de carte de crédit est protégée sur le site.

Je fais assez confiance aux grands noms en me disant qu'Amazon, par exemple, doit avoir vraisemblablement - du moins je l'espère mais je n'en suis pas certain -, un champ chiffré au moins pour le numéro de carte de crédit, c'est-à-dire qu'au lieu de coder directement le numéro en clair, celui-ci va être transformé, avant son stockage, en un numéro incompréhensible par lecture directe. Donc le vrai problème n'est pas le lien. Je crois qu'aujourd'hui, on peut faire confiance car après tout il existe d'autres risques bien plus rudimentaires sur les captures de numéro de carte dans beaucoup d'environnements, et ce n'est pas pire sur l'Internet. En revanche, qu'est-il fait de mon numéro de carte une fois celui-ci archivé ?

P. Lointier :

Je voudrais faire deux commentaires.

Mon souci premier est que je ne peux pas avoir confiance sur l'Internet, même sur Amazon, parce que je ne sais pas comment l'information est conservée, mais ce qui me rassure, c'est que, lorsqu'il y a un piratage de carte bancaire sur un site de commerce, ce n'est pas une carte qui est piratée, mais ce sont cinquante ou cent mille cartes. Et je me dis que sur cent mille cartes, la probabilité que ce soit ma carte qui soit utilisée me permet de dormir tranquille. Je vous rappelle qu'en droit bancaire français, comme vous n'avez pas composé votre code confidentiel, vous pouvez répudier tout achat sur l'Internet.

Concernant Amazon, le site n'est pas sécurisé parce qu'à un moment le cadenas ou la clé va se fermer, mais seulement une fois que vous aurez composé votre identifiant et votre mot de passe. Cela signifie que l'identifiant et le mot de passe transitent en clair et qu'après, vous êtes dans une partie sécurisée. Donc le seul risque pourrait être, que sur votre machine, quelque part dans le cheminement, soient interceptées les données de transaction pour ensuite faire ce qu'on appelle dans le domaine un «rejeu», une «mascarade» : on se fait passer pour vous, on a votre mot de passe puisqu'il est passé en clair ; les données financières sont conservées, et il ne reste qu'à faire changer le lieu de livraison.

P. de Brem :
Achetez-vous des livres sur Amazon ?

P. Lointier :
J'y ai été contraint parce que je ne les trouvais pas en France !

R. Klapisch :
Non seulement il y a la carte de crédit, mais des maisons comme Amazon ou la FNAC connaissent vos goûts et vous proposent des produits. Cela ne me dérange pas, mais si quelqu'un voulait connaître tout ce que j'ai acheté, je pense qu'il pourrait le faire.

P. Lointier :
Je fais des courses dans un supermarché et je reçois des coupons de réduction par courrier postal qui correspondent à un profil de consommation que je représente.

Question :
Concernant l'achat par carte bancaire, effectivement j'achète sur Amazon depuis quelques années et je n'ai jamais eu de soucis. On peut donc être relativement rassuré. Le risque statistique est bien moins important par l'Internet que par téléphone, et vous avez la possibilité de répudier l'achat

Informatique et vie privée... Il est clair que la vie privée est surveillée, comme avec le mobile qui permet de géolocaliser et de connaître le nombre d'appels. Vous utilisez votre carte bancaire, on sait donc où vous êtes, le montant de votre retrait, et si vous avez dépassé votre plafond. Vous prenez votre voiture et l'on sait que vous êtes passé à tel péage, tel jour à telle heure. Vous marchez dans la rue, vous êtes filmé.

En revanche, sur l'aspect données informatiques, je pense que c'est le comportement individuel qui va faire la différence. Une fois qu'on a installé les outils de base dont on a déjà parlé (anti-virus, pare-feu, cryptologie, etc.), le risque se situe sur le comportement. On aurait pu citer ce soir des exemples de bonnes pratiques.

Concernant le *spaming*, un conseil pratique est d'avoir plusieurs adresses électroniques : une très privée ; une professionnelle ; et une réservée aux sites qui réclament votre adresse électronique et qui va être inévitablement utilisée pour du *spaming*.

On peut utiliser des logiciels qui permettent d'effacer les *cookies* après chaque surf afin de ne pas laisser de données sur son poste.

Existe-t-il d'autres pratiques de même nature à conseiller aux personnes présentes ?

P. Lointier :
Avant de donner des conseils, je note que vous avez déjà un comportement qui n'est pas celui d'un internaute lambda. Le gros problème réside en effet dans le fait qu'il n'y a pas d'éducation, de recommandations basiques pour le citoyen. Quand on connaît le domaine, on peut parvenir à paramétrer pour garder son anonymat.

Question :
Avez-vous des conseils pratiques, simples à mettre en œuvre, pour se protéger ? Comment choisir son mot de passe, par exemple ?

J. Stern :
Quelles sont les attaques contre un mot de passe ? L'attaque la plus standard, hormis le fait de vous «piquer» le mot de passe quand il est transféré, consiste à essayer tous les mots de passe possibles. Si votre mot de passe est dans un dictionnaire français, il ne tiendra pas trois secondes. Un mot de passe doit être un mot relativement long qui n'est pas dans un dictionnaire, qui contient des signes un peu étranges comme des points et des chiffres, bref quelque chose qui va déjouer ce que nous appelons l'attaque par dictionnaire, qui consiste à examiner tous les mots d'un dictionnaire et à faire les essais correspondants dans tel ou tel contexte technologique. Donc un bon mot de passe est un mot de passe un peu bizarre et assez long.

P. de Brem :
On peut ajouter qu'il faut nettoyer plusieurs fois son disque dur avec un logiciel spécialisé pour être absolument certain qu'il n'y reste aucune trace. Quand on met son ordinateur au rebut, qu'on ne le «nettoie» pas des données personnelles qu'il contient, et qu'on le met dans la rue, que devient-il ?

P. Lointier :
Je vois que vous avez été sensibilisé au dernier sujet de notre conférence : en fait, on peut récupérer énormément de choses sur un ordinateur, mais on en revient à un problème de connaissance. Le simple effacement du système d'exploitation que ce soit sur Unix ou sur Windows® n'efface pas la donnée. Il faut des logiciels spécialisés qui vont réécrire par-dessus tous les octets. Vous allez sur n'importe quel site de téléchargement de produits gratuits et vous aurez des produits qui vous proposeront l'effacement. Néanmoins, si au préalable, vous n'avez pas été sensibilisé à la chose, il est certain que vous mettrez votre disque dur au rebut, et des informations resteront éventuellement exploitables.

Toutefois, dans le monde du renseignement, il ne s'agit pas seulement de récupérer l'information ; elle doit être à destination de quelqu'un, à un moment précis. Donc, il faut que quelqu'un soit intéressé à l'exploiter, indépendamment du fait que cette information soit disponible.

P. de Brem :
Nous n'avons pas beaucoup parlé de l'espionnage de vos mails par la société qui vous emploie. Si vous écrivez «personnel» dans l'objet de votre e-mail, la société pour

laquelle vous travaillez n'a pas le droit d'ouvrir votre courrier pour regarder ce qu'il y a dedans. Vous avez le droit d'utiliser l'e-mail de votre société à des fins personnelles.

P. Lointier :

J'irai plus loin : même un e-mail dit «professionnel» est une communication qui a, pour l'instant, un caractère privé. Une discussion est en cours pour remettre cela en cause, mais, actuellement, un directeur informatique ne peut demander à son responsable réseau ou de messagerie d'accéder à la messagerie de quelqu'un sans l'accord préalable de l'intéressé.

C. Pallez :

Je conteste ce que vous venez de dire.

R. Longeon :

J'ai suivi le procès de F.V., et cette notion a été abandonnée en appel.

P. Lointier :

Oui, mais au niveau des textes, c'est l'interception sur les communications.

C. Pallez :

La jurisprudence ne protège que l'intimité de la vie privée et donc les correspondances qui en relèvent. Donc pour être protégée, elle doit être identifiée comme étant à caractère personnel. En revanche, l'employeur a le droit de prendre connaissance des correspondances qui relèvent du professionnel.

P. de Brem :

D'autant que l'employeur est responsable de ce que vous faites sur votre lieu de travail. Il a besoin de vérifier ce que vous faites.

Question :

Faut-il tout crypter ?

P de Brem :

Maintenant que tout est libéralisé, on devrait pouvoir crypter toute sa correspondance, mais on ne le fait pas.

J. Stern :

Effectivement, maintenant que nous avons des outils de chiffrement, il faut chiffrer (crypter, comme vous dites), tout en étant conscient de ce qu'on est en train de faire. Utiliser des logiciels de chiffrement ou des logiciels qui, de façon transparente, opèrent un chiffrement, sans que vous deveniez pour autant spécialiste de cryptologie, c'est bien, mais cela ne vous protégera que dans une certaine mesure. Ce n'est pas parce que le lien de votre navigateur jusqu'à votre banque à domicile est chiffré qu'il n'y aura pas d'intrusion chez vous ou sur le site bancaire. Cependant, la généralisation des moyens de cryptologie permettra de répondre, au moins en partie, à certaines menaces qui pèsent sur nos données.

Question :

Lorsqu'on s'abonne à un magazine, les groupes de presse s'échangent les adresses et les fichiers. Peut-on imaginer que certaines sociétés qui vendent des logiciels d'eCRM *(Customer Relationship Management)* aux sociétés de distribution et vente par correspondance fassent la même chose ? Quel est le risque et quelle est la protection que pourrait proposer la CNIL ou la loi ?

C. Pallez :

L'échange de fichiers est possible à condition que la personne dont on communique l'adresse ait été mise en mesure de s'opposer à cet échange, c'est-à-dire qu'elle ait été informée que le fichier était susceptible d'être vendu, loué ou cédé, et qu'elle ait la possibilité de s'y opposer. C'est un principe général, et le problème de son application peut, bien sûr, se poser.

De manière générale, les croisements de fichiers entre sociétés commerciales donnent lieu à des déclarations à la CNIL. Nous sommes là pour essayer de veiller, précisément, à ce que ces croisements ne soient pas abusifs et respectent le principe d'opposition.

Question :

Une précision quant à ma première question, qui ne portait pas sur l'efficacité d'Echelon, parce qu'on pourrait étendre le débat sur les guerres internes des services secrets américains, mais qui portait sur le problème des Etats qui bafouent les droits fondamentaux de leurs citoyens. Que faisons-nous avec notre jeunesse lorsqu'on essaye d'introduire un minimum d'éthique ?

J. Stern :

Je suis un peu gêné parce que je crois qu'on demande tout et le contraire de tout. Tout à l'heure, on a expliqué que la CNIL peut connaître mon numéro IP, et puis inversement, dans le cas de certaines attaques qu'on appelle les «attaques par déni de service», on a des ordinateurs infectés par intrusion qui envoient des requêtes dans un site, et l'on aimerait bien remonter à la source pour pister le méchant *(IP trace back)*, or on ne sait pas le faire.

Il doit donc y avoir un équilibre entre la protection de la vie privée et l'élimination si possible, ou du moins la mise en cause par voie juridique, de ceux qui ne respectent pas cette vie privée.

Des services de renseignements existent, mais quand ils font leur travail, on leur dit qu'ils sont méchants, et quand ils échouent, on leur dit qu'ils sont nuls ! Il faut admettre l'existence des services de renseignements et je ne suis pas certain que ces services s'attaquent spécifiquement à la vie privée des gens.

En revanche, le croisement de fichiers commerciaux, le fait que si l'on systématise des méthodes de type «passeport Microsoft», la collecte d'une série d'informations

que je n'ai pas envie qu'on réunisse sur moi, tout cela me semble une préoccupation plus importante.

J'ai donc envie de dire à vos étudiants qu'il est tout à fait regrettable qu'il y ait des interceptions et des écoutes ; que néanmoins, le problème de la vie privée n'est pas tellement là, mais dans des données beaucoup plus banales que celles que les services de renseignements sont en train de récupérer, par le moyen de croisements de fichiers commerciaux. Et dans ce cas, on peut vraiment se protéger, du moins en grande partie, par un certain nombre de méthodes, de sécurités et de mécanismes bien mis en place, avec en plus, la généralisation de la cryptologie.

P. de Brem :

Je suis allé sur un site Internet de *hackers*, que j'ai trouvé extrêmement facilement, où l'on vous propose des systèmes comme par exemple le *Computer Keystroke Grabber*, système permettant de récupérer à l'écran tout ce qui a été tapé sur le clavier. Vous l'installez sur votre ordinateur et quand vos enfants, ou n'importe qui, utilisent votre ordinateur, vous savez tout ce qu'ils ont tapé, leur mot de passe... Vous pouvez bien sûr installer ce système chez un concurrent.

J'ai trouvé un autre système qui est un modificateur de notes scolaires *(School grades changer)*, qui vous permet d'aller sur le site Internet de votre université et de modifier les notes scolaires qui sont stockées sur l'ordinateur.

Avec *Big Money Test Devices*, vous pouvez changer l'identité de votre carte bleue et transformer le crédit. Si vous êtes interdit bancaire parce que vous avez trop dépensé, vous pouvez modifier cela.

J'ai également trouvé un effaceur de dettes instantané ; et un système qui permet de relire et d'écrire sur les cartes à bande magnétique...

P. Lointier :

Plus exactement de lire la partie publique d'une carte bancaire. Vous n'accéderez pas à la clé privée qui se trouve à l'intérieur, mais en revanche, vous pouvez encoder et programmer une carte à puce.

Il faut faire très attention lorsque vous allez sur ce type de site, car vous avez vite fait de croire que tout peut être fait, ce qui est absolument faux. Même avec un lecteur de carte à puce, vous ne verrez pas le contenu d'une SIM parce qu'il faut un mot de passe administrateur pour accéder à certains sous-registres de la SIM. Donc ne nous emballons pas sur ce qu'on peut lire parfois sur le Web.

P. de Brem :

Je vous remercie beaucoup d'avoir été aussi nombreux et de toutes vos questions, et je voudrais en votre nom remercier nos intervenants pour ce très intéressant Café.