SÉCURITÉ INFORMATIQUE
numéro 32 décembre 2000
SÉCURITÉ DES SYSTÈMES D'INFORMATION

Correspondance privée et société de l'information

éditorial

Le tribunal correctionnel de Paris a rendu le 2 novembre dernier un jugement qui condamne trois de nos collègues pour « délit de violation de correspondances effectuées par voie de télécommunication, par personne chargée d'une mission de service public », en vertu de l'article 432-9, alinéa 2 du code pénal.

À l'analyse du jugement, on constatera que les actes ayant fait l'objet de la condamnation étaient motivés par le seul souci de conserver la disponibilité du système d'information de leur laboratoire, donc par le seul souci du service, sans intention de nuire. Le jugement a donc suscité, chez ceux et celles qui ont la responsabilité d'assurer le bon fonctionnement des systèmes informatiques de nos laboratoires, une amertume bien compréhensible, mais aussi, et surtout, de nombreuses interrogations dont notre revue a choisi de se faire l'écho.

Le verdict est fondé essentiellement sur le caractère strictement privé attribué à la correspondance électronique qui « tombe » dans la boîte aux lettres d'un individu, que celle-ci soit localisée à son domicile (par exemple) ou hébergée quelque part dans l'outil informatique mis à disposition par l'employeur sur les lieux de travail.

Le caractère inviolable de la correspondance privée procède de la protection des libertés individuelles et, à ce titre, il ne peut qu'être confirmé. Mais ne dit-on pas que la liberté finit là où commence celle d'autrui ? Le droit de voir respecter la confidentialité d'une correspondance « privée », dès lors que celle-ci est reçue, stockée, ou transmise par l'outil de travail, doit-il nécessairement empiéter sur celui de l'employeur, qui consiste à pouvoir disposer pleinement de l'outil qu'il a mis en place ou encore à pouvoir s'assurer que ledit outil n'est pas détourné de sa finalité pour des usages que la loi réprouve ?

L'analyse faite par nos collègues dans ces colonnes suggère à l'évidence que la réponse n'est pas fatalement « oui ». En effet, pour ne retenir qu'un aspect facilement appréhendable par des non-spécialistes, la mention de l'organisme employeur dans l'adresse électronique ne supprime-t-elle pas, de fait, le caractère strictement privé de la correspondance qui y aboutit ? La situation de l'administrateur qui prend connaissance du contenu d'un courrier électronique par nécessité de service est-elle fondamentalement différente de celle des secrétaires dans les bureaux de nos administrations qui, en l'absence de mention de confidentialité particulière, ouvrent, pour les mêmes raisons, sans encourir les foudres de la justice, des enveloppes qui sont adressées nominativement à d'autres ?

Par ailleurs, les considérations techniques développées au fil des articles sont très vraisemblablement présentes quelque part dans l'« exposé des

..... suite page 6 ...►

Le point juridique

La presse, à juste titre, s'est largement fait l'écho du jugement rendu par le tribunal correctionnel de Paris le 2 novembre dernier. En effet, si des décisions sont déjà intervenues dans des litiges ayant trait à l'usage du courrier électronique, elles ont été tranchées par des juridictions prud'homales et non par des tribunaux correctionnels. C'est donc, à notre connaissance, la première décision rendue en matière pénale. À ce titre, elle doit être analysée avec la prudence qui s'impose, car rien ne permet d'affirmer que l'analyse faite par les magistrats sera reprise dans d'autres affaires similaires à venir.

1 – L'application de l'article 432-9 alinéa 2 du code pénal

C'est sur cet article que le tribunal s'appuie pour retenir l'infraction, en estimant que *« le réseau mondial du Net »* et l'intégralité des services qu'il offre, *« dont la messagerie électronique »*, sont couverts par la législation sur les télécommunications.

S'interrogeant sur la notion de correspondance, il la définit comme *« toute relation par écrit entre deux personnes identifiables, qu'il s'agisse de lettres, de messages ou de plis ouverts ou fermés »*. Relation protégée, nous dit-il, *« par l'article 1 de la loi du 10 juillet 1991 sur les télécommunications »* et par l'article 432-9 alinéa 2 du code pénal, qui vise *« le fait* [...] *d'ordonner, de commettre ou de faciliter, hors les cas prévus par la loi, l'interception* [...] *des correspondances émises* [...] *par la voie des télécommunications »*.

Le cadre juridique une fois posé, le tribunal se demande si la messagerie électronique est bien protégée par le secret de la correspondance, pour conclure par l'affirmative. Il rappelle que cet outil permet à deux personnes identifiées de se transmettre un message écrit personnalisé par le biais d'une adresse électronique unique composée du *« nom »* et de *« l'entité de rattachement »*, avec, le cas échéant, un accès par mot de passe. Pour les magistrats, il devient clair au fil de ces indices que *« l'envoi de message électronique de personne à personne constitue de la correspondance privée »*. Autrement dit, nous sommes bien sur le terrain de la correspondance protégée par le secret.

2 – L'absence de faits justificatifs

Le tribunal écarte ensuite l'argument tiré de la violation de la charte Renater, en relevant tout à la fois que, si ce texte impose un usage strictement professionnel du réseau, il aménage aussi la confidentialité des fichiers qui s'y trouvent (documents qui, par nature, ne sont pas de la correspondance privée). Sur le fait de savoir si, oui ou non, la partie civile avait eu connaissance des règles d'utilisation du réseau, il indique qu'en tout état de cause cela ne pouvait justifier l'ouverture de la correspondance privée. Enfin, il estime qu'à l'époque des faits la sécurité du réseau n'était pas menacée et ne pouvait en conséquence légitimer l'interception des messages.

Encore une fois, même si ce premier jugement n'a pas l'autorité d'une jurisprudence ancienne, assise sur un flot de décisions convergentes, confortées par la Cour de cassation, on ne peut ignorer son existence et ne pas prendre les précautions qu'impose sa lecture. Sachez par ailleurs que les intéressés, en pleine concertation avec la direction juridique, ont fait appel de cette décision.

Dominique Dalmas
Directeur à la Direction des Contrats et des Affaires Juridiques

CNRS CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

Les risques du métier

Ingénieur système et réseaux dans un laboratoire CNRS, je viens de vivre une mésaventure qui pourrait arriver à chacun d'entre nous. Je viens d'être condamnée par le tribunal correctionnel de Paris pour « violation du secret des correspondances ». Si je tiens à m'exprimer ici sur ce sujet, c'est pour que mon expérience profite à d'autres et pour démarrer une réflexion commune sur les risques de notre métier et les moyens que nous devons trouver pour réduire ces risques tout en continuant à assurer notre mission : préserver la sécurité des réseaux de l'enseignement et de la recherche.

Les faits

Je ne vais rappeler qu'à grands traits notre histoire : un étudiant en thèse au laboratoire a commis plusieurs actes de malveillance : harcèlement d'une autre étudiante, destruction de ses fichiers, etc. Inquiétés tout d'abord par ces actes, puis par un volume anormalement élevé de courriers électroniques de cet étudiant, et craignant un autre acte de malveillance de sa part, nous avons regardé dans sa messagerie électronique. Il l'a appris et a porté plainte. Le tribunal nous a condamnés, le directeur de mon laboratoire, un enseignant-chercheur, et moi-même. Les médias se sont largement fait l'écho de ce jugement, car c'est la première fois que la justice française a à se prononcer sur le statut juridique du courrier électronique. Nous avons été condamnés à 10 000 F d'amende chacun et à verser au plaignant 5 000 F chacun pour ses frais de justice, plus, solidairement, la somme de 10 000 F au titre des dommages et intérêts.

Pour commencer, deux conseils

J'aimerais commencer par donner deux conseils aux ingénieurs réseaux et directeurs de laboratoire lecteurs de cette revue. Attention, je n'exprime ici que mon opinion personnelle, je ne suis pas juriste, et même si j'ai beaucoup appris récemment en matière juridique, **je ne peux pas vous assurer que vous serez à l'abri de la justice dès lors que vous suivrez mes conseils !** Cependant, je pense que si nous avions respecté les consignes suivantes, notre position aurait été plus forte vis-à-vis du tribunal.

1. Faites signer une charte d'utilisation du système à tous vos utilisateurs, celle du CNRS, celle de Renater, celle de l'université, peu importe ; ce qui est important, c'est qu'il y soit écrit clairement :

« L'usage des ressources informatiques est réservé exclusivement à l'usage professionnel [...]. La confidentialité des messages non chiffrés ne peut pas être garantie. »

Vous pouvez prendre connaissance de la charte CNRS à l'adresse suivante : http://www.dsi.cnrs.fr/BO/1999/03-99/415-bo0399-dec998407dcaj.htm

En effet, ce que la justice nous a reproché n'est pas tant d'avoir lu le courrier électronique de notre étudiant que de ne l'avoir pas averti que nous allions le faire :
– d'une part, il n'avait pas signé de charte, notre procédure de systématique de signature de charte étant en cours, mais non encore terminée,
– d'autre part, nous ne l'avons pas averti juste avant de lire son courrier.

Avoir affiché la charte Renater au laboratoire n'a pas été retenu en notre faveur puisque le plaignant a déclaré n'avoir pas vu ces affichages. Avoir rappelé par mail l'usage professionnel du réseau n'a pas été davantage retenu, puisqu'il a déclaré n'avoir pas reçu ce message.

Si tous vos utilisateurs ont signé cette charte, il y a moins de risque de tomber sur un mauvais joueur qui vous dise : « Je ne savais pas. » Le simple fait d'avoir signé ce papier affaiblira considérablement sa position en cas de conflit. Attention, cela ne nous autorise pas pour autant à lire les messages de nos utilisateurs.

Faire signer cette charte n'est pas incompatible avec le respect de notre déontologie : ce n'est pas parce que nos utilisateurs signent cette charte que nous devons lire leur courrier, bien sûr. Cela n'empêche pas non plus les utilisateurs d'utiliser la messagerie pour des raisons privées, mais alors ils le font en toute connaissance de cause, ils prennent leurs responsabilités.

2. L'autre leçon que je tire de notre mésaventure, c'est qu'il faut se garder d'une attitude trop permissive : il faut sanctionner tout de suite les comportements malveillants. L'étudiant qui a porté plainte contre nous avait modifié les fichiers d'une autre étudiante. Qu'un utilisateur modifie les fichiers d'une autre personne, c'est grave, et c'est une raison suffisante pour fermer son compte immédiatement et déposer une plainte. Quitte à la retirer plus tard si la situation s'arrange. La contrepartie bien sûr est le risque d'engorgement des tribunaux si arrivent devant la justice tous nos petits démêlés avec les étudiants ou les grincheux ; mais devant un tribunal, mieux vaut être partie civile que prévenu. Mieux eût valu que ce fût à notre étudiant d'expliquer ses actes, plutôt qu'à nous d'expliquer les nôtres. En ne portant pas plainte, de victimes nous sommes devenus coupables aux yeux de la société.

... et quelques questions

Forts de ces deux conseils, nous aurions probablement bénéficié de plus d'indulgence de la part des juges. Pour autant, restent encore des questions en suspens. Faire signer une charte à nos utilisateurs est recommandé, mais cela est loin de régler tous les problèmes. Par ailleurs, la gestion de cette charte pose quelques questions d'organisation pratique, que je ne détaillerai pas :
– Trouver un endroit sûr, fermé à clef, pour ranger ces chartes signées.
– Combien de temps doit-on les garder ?
– Que faire si quelqu'un refuse de la signer ?

Et puis :
– Quelle valeur a une charte rédigée en français et signée par un non-francophone ?
– Cette charte est-elle légale ?

Bref. Le tribunal nous a reproché de ne pas avoir averti notre étudiant que nous allions lire ses messages. Mais celui-ci nous avait dit – et il l'a déclaré de nouveau au tribunal – qu'un pirate avait usurpé son identité. Il nous avait donc semblé absurde de lui envoyer un message pouvant être lu par « le pirate ». Or lui-même ne venait plus que la nuit ou le soir très tard au laboratoire. Sans doute aurions-nous dû lui envoyer un courrier recommandé avec accusé de réception. Ces précautions étant prises, aurions-nous eu le droit de lire ses messages ? Je ne sais pas.

J'aimerais attirer votre attention sur les textes qui ont conduit à notre condamnation :
Le secret des correspondances est protégé par deux articles du code pénal :
– 432-9 pour des personnes investies d'une mission de service public,
– 226-15 pour les autres.
(http://www.canevet.com/legis/textes/secret-corr.htm *ou* http://www.legifrance.gouv.fr/)

Je vous engage vivement à lire ces deux articles du code pénal, en particulier le 432-9 si vous êtes fonctionnaire. (Vous remarquerez au passage

que notre qualité de fonctionnaire a aggravé notre cas. En effet, pour les fonctionnaires, la mauvaise foi n'est pas nécessaire pour que le délit soit constitué. Peu importe que nous soyons de bonne ou de mauvaise foi, peu importe que nous ayons agi pour défendre la sécurité du laboratoire et non pour des motifs personnels.) Pesez chaque mot et interrogez-vous sur votre pratique quotidienne au regard de chacun de ces mots.

En particulier, avons-nous le droit de mettre en place des filtres anti-spam à l'entrée de nos sites ? N'est-ce pas du détournement de correspondances ? Avons-nous le droit de détecter et de détruire les messages porteurs de virus ? N'est-ce pas de la destruction de correspondances ? De même ,avons-nous le droit de détruire les courriers électroniques laissés sur nos disques durs par des utilisateurs partis du laboratoire ou de notre université ? Avons-nous le droit de fermer un compte et ainsi d'empêcher une personne d'accéder à sa correspondance privée ?

Est-il nécessaire de décrire tous ces cas de figure pour en avertir nos utilisateurs dans la charte que nous leur faisons signer ? Au risque de devoir modifier la charte dès qu'un nouveau cas se présente ?

L'article 432-9 du code pénal a été vraisemblablement écrit en pensant aux facteurs qui lisent le courrier des gens, puis il a été étendu aux télécommunications.

Mais le courrier électronique est-il vraiment une télécommunication ? Ou plutôt, n'est-il pas plus qu'une télécommunication ? Télécommunication quand le courrier circule sur le réseau, ne devient-il pas à l'évidence fichier dès lors qu'il arrive sur un ordinateur ? Et dès lors, quel statut a-t-il ? Quel statut ont les pièces attachées au message, images, son ou vidéo ?

Dans son jugement, le tribunal démontre le caractère privé de la messagerie électronique : *« Il convient donc de considérer que la messagerie électronique de la partie civile, à laquelle il n'était possible d'accéder qu'en utilisant son mot de passe, était protégée par le secret de la correspondance émise par voie de télécommunications, dont la violation tombe sous le coup de la loi pénale. »*

Inviolabilité pour la sécurité informatique et sanctuarisation pour les pirates

Si nous admettons le caractère privé et inviolable du courrier électronique sur le lieu de travail, alors ce caractère d'inviolabilité s'applique si le courrier est dans la boîte aux lettres d'arrivée (/var/mail) ; il s'applique aussi aux messages que l'utilisateur a lu et rangé dans son répertoire personnel sur le disque partagé (/home). Je restreins mon raisonnement à un environnement Unix, puisque c'est précisément notre cas et celui de beaucoup d'autres laboratoires.

Comme nous ne pouvons pas distinguer *a priori*, sans en regarder le contenu, un fichier de message d'un fichier de données, d'un programme, d'un texte quelconque, c'est tout le répertoire des utilisateurs qui devient un sanctuaire inviolable. Il faut donc s'interdire de regarder dans les répertoires personnels des utilisateurs et d'ouvrir des fichiers sans leur accord.

Très bien, c'est effectivement ce que nous faisons dans le fonctionnement normal de notre activité : nous n'avons besoin ni de lire les courriers de nos utilisateurs, ni d'ouvrir leurs fichiers, sauf à leur demande pour régler des problèmes ponctuels.

Mais il arrive parfois que surgissent des difficultés imprévues. Je me souviens avoir eu un piratage il y a quelques années : le pirate avait usurpé le mot de passe d'un utilisateur et s'était connecté en son nom. Je m'en étais aperçue tout de suite car j'avais été alertée par la bizarrerie de cette connexion. Par chance, mon utilisateur était au laboratoire, j'avais pu aller le voir tout de suite et nous avions fait ensemble des recherches dans son répertoire. Nous y avions trouvé un « root kit », c'est-à-dire l'attirail de logiciels qui permettait de devenir « root » en exploitant une faille du système. Mais si mon utilisateur avait été absent ce jour-là ? Que devais-je faire ? Fermer le compte tout de suite et attendre qu'il revienne pour regarder dans son répertoire ? Mais, pendant ce temps, les logiciels qu'a installés le pirate continuent de tourner et risquent d'aggraver le piratage. Ré-installer tout de suite le système sans attendre de savoir de quelle façon notre machine a été piratée et ce qu'a fait le pirate ? Regarder sans son accord, mais alors je risque d'ouvrir un fichier qui contient un message, et je tombe sous l'article 432-9 ? Car le délit est constitué dès lors que l'on a pris connaissance d'une correspondance qui ne nous est pas destinée, même si nous n'en divulguons pas le contenu.

Je prends un autre exemple qui nous est arrivé à tous un jour ou l'autre : imaginons la boîte aux lettres d'un utilisateur, qui ne cesse de grossir de jour en jour en son absence et qui menace de saturer notre espace disque au point que la messagerie de tout le laboratoire ne pourrait plus fonctionner. Que faire ? Chacun a sa solution et bricole dans son coin en essayant de sauvegarder l'intérêt général sans nuire à l'utilisateur, mais parfois au mépris de l'article 432-9.

Déplacer tout son courrier sur un autre disque ? N'est-ce pas du détournement et, pire, de l'archivage ? Détruire les courriers les plus vieux ? N'est-ce pas de la destruction de correspondance ? Et pour sélectionner les plus vieux, il faut bien les lire, même si cela peut être fait automatiquement. En avons-nous le droit ? La seule solution légale est-elle de courir acheter un autre disque ?

Nous savons bien que, dans la majorité des cas, les pirates utilisent le compte d'un utilisateur pour se connecter sur nos machines, puis usurpent les droits de « root » pour installer des outils qui leur permettront de commettre d'autres piratages ici ou ailleurs dans le monde depuis nos machines. Si nous ne pouvons plus ouvrir les fichiers de nos utilisateurs, les pirates seront ravis !

Je crains qu'en poussant jusqu'au bout la logique de l'inviolabilité absolue de la messagerie dans nos laboratoires, nous perdions tout contrôle sur une partie de notre espace disque. Cela a un coût et comporte un risque sur la sécurité de nos systèmes. Cela peut conduire à se poser alors la question de l'opportunité de créer des adresses électroniques à toutes les personnes qui viennent travailler chez nous. Mais ce serait quand même dommage qu'Internet, qui est à son origine un outil scientifique développé dans les universités, nous soit en partie retiré par une réglementation inadaptée.

Conclusion

Pour conclure, admettons le principe que la correspondance par e-mail est une correspondance privée, cela semble logique et indiscutable pour les particuliers. Dans un cadre professionnel, cela peut être discutable ; mais, si nous admettons ce principe, nous ne pouvons plus alors faire correctement notre travail sans enfreindre ce fameux article 432-9.

Cependant, les facteurs, pour lesquels cet article a été écrit, disposent d'une réglementation pour leur permettre de faire leur travail sans enfreindre la loi : si un paquet fait « tic-tac », ils ont le droit de l'ouvrir ou de le détruire. Pourquoi n'aurions-nous pas nous aussi un ensemble de règles écrites spécifiques à notre profession, qui nous permettraient d'entrer dans « les cas prévus par la loi » du fameux 432-9 ? Si nous voulons continuer à assurer correctement notre mission sans courir le risque de commettre un délit, nous devrons absolument nous atteler à cette tâche. Les juristes devront nous y aider, car on ne peut pas continuer à exiger de nous des compétences techniques rares sur le marché du travail et des compétences juridiques en plus. Nous ne sommes pas des surhommes !

Françoise Virieux
Ingénieur systèmes et réseaux LPMMH, CNRS-ESPCI
virieux@pmmh.espci.fr

Que faire ?

La sécurité informatique est, bien sûr, la protection contre toutes les formes d'intrusion. Un site bien connecté à Renater, visible, voit passer un scan réseau par jour, aux origines les plus diverses. Les parades sont connues: des réseaux fermés, des gardes-barrières, des machines bien entretenues et à jour de tous les correctifs de sécurité. Mais il y a deux autres vecteurs d'insécurité, deux vecteurs d'information vraiment très utilisés: les pages Web et le courrier électronique ! En 1990, on voyait passer : « N'ouvrez pas le courrier X, il va détruire votre disque dur. » À l'époque, c'était un pur mensonge. La réalité en 2000 est tout autre ! Quels sont donc les risques associés aux courriers électroniques, et quelles sont les particularités de notre milieu de la recherche par rapport aux fournisseurs d'accès Internet (FAI) ?

Les virus

Un courrier électronique est découpé en attachements, pouvant contenir aussi bien un document (Word ©), une image, un exécutable (Navidad.exe), un script (Visual Basic ©). Le monde PC/Windows/Word/Outlook est ainsi un remarquable vecteur d'insécurité. Par sa quasi-monoculture, il est la cible de choix ; et le nombre de virus existants le prouve : 54 000 virus connus, cela fait une dizaine de nouveaux virus par jour. ILoveYou (mai 2000), Navidad (nov. 2000) qui s'est propagé parmi les correspondants Xlab, sont deux exemples. Certains virus sont assez innocents, d'autres installent des chevaux de Troie, d'autres espionnent et divulguent des informations (style mots de passe), d'autres détruisent des fichiers, etc. Cas d'école : un virus se propage très vite, moi administrateur système, j'en entends parler (alerte CERT/Renater, media grand public), je l'ai déjà reçu – donc ce n'est pas une rumeur –, les anti-virus ne sont pas encore à jour. Que faire ? Le chercher et l'éradiquer viole le caractère privé des courriels ; supprimer les boîtes aux lettres électroniques est de *« la destruction de données par personne chargée de mission de service public »*. Laisser faire peut être considéré comme une faute professionnelle : « Je connais un danger, mais ne fais rien contre. » Arrêter le service de courrier pour ne pas empirer la situation est-il raisonnable, en 2000 ?

Le volume

Nos courriers contiennent beaucoup de documents, par exemple des articles. Il est donc peu concevable de limiter les tailles des courriers, et la taille de la boîte-aux- lettres, à des valeurs basses. Une politique – la mienne en tout cas – est : « Mettons une zone de spool, et advienne que pourra. » En outre, nous permettons des facilités, comme « .forward », ou « procmail ». Une faute, et c'est la boucle qui dégénère. Avoir un compte utilisateur dans un laboratoire est-il équivalent à prendre un abonnement à AOL, Wanadoo ou autres ? Dans ce cas, doit-on prévenir ce type d'incident comme le font les « FAI », en limitant les tailles des courriels ? En cas de belle avalanche – cela m'est arrivé la semaine dernière, à raison de 2 Mo de courriels par minute –, déplacer la « mailbox » ne suffit pas, il faut arrêter l'avalanche, donc chercher la cause.

Les informations

Enfin, nos machines de recherche contiennent et accèdent à des informations confidentielles : mots de passe, sujets d'examen, résultats de concours, recherche en cours, etc. Le piratage d'octobre 2000 chez Microsoft comprenait, outre un virus, un outil d'espionnage des mots de passe qui envoyait les informations récoltées par courrier électronique. Question : peut-on filtrer/rechercher ce type de courrier automatique ? Peut-on chercher leurs destinataires (en traitant des journaux) ? Une des tendances du dernier salon Interop était aussi l'analyse de contenu, par exemple pour identifier des contenus illégaux (*cf.* l'affaire Yahoo : puis-je/dois-je intercepter des contenus nazis ?), ou des contenus non professionnels (notre charte Renater stipule un usage professionnel : suffit-il de dire ou doit-on faire respecter ?).

Jacques Beigbeder
Service de Prestations Informatiques
École normale supérieure
Jacques.Beigbeder@ens.fr

Suite à ma récente condamnation, je me pose la question de savoir comment assurer dorénavant la sécurité du système informatique dans mon laboratoire. Étant directeur, je suis officiellement, selon les directives du CNRS, le responsable pour la sécurité et le bon usage du système informatique. Comme dans tous les laboratoires, ce n'est pas moi personnellement qui contrôle les ordinateurs, mais je délègue cela à l'ingénieur système, et je dois avoir (et c'est en effet mon cas) confiance en lui, car étant « super-*user* » et étant bien plus compétent que moi, il échappe à mes possibilités directes de surveillance.

Après ce jugement, comment dois-je gérer ma délégation de pouvoir à l'ingénieur système ? Comment l'ingénieur système peut-il dorénavant remplir ses tâches sans peur, sachant que notre condamnation s'étend aussi au cas d'ouverture non intentionnelle des fichiers contenant de l'information dite « privée » ? Comment l'ingénieur système peut-il se défendre contre les ruses de plus en plus sophistiquées des « pirates », si ses supérieurs ou les juristes ne comprennent pas les contraintes et les pannes dans un système Unix ?

Notre condamnation ouvre un débat juridique, et à mon avis il faut éviter qu'une jurisprudence se mette en place qui accroîtrait trop les difficultés du métier de l'ingénieur système et mettrait en contradiction la direction d'un laboratoire dans sa fonction d'assurer le bon fonctionnement du système informatique. Il est clair que l'intimité de la correspondance est un principe qui ne doit pas être contesté. En même temps, il faut éviter que les moyens informatiques communs soient victimes des abus et des actions malveillantes. Comment peut-on assurer qu'il n'y a pas des conflits entre ces deux propos ? Si le courrier « privé » nuit ou met en péril la communauté, comment le neutraliser ? Le débat juridique ne peut pas se restreindre aux questions d'éthique, mais doit prendre en compte aussi l'aspect technique des réseaux informatiques et la réalité au jour le jour dans un laboratoire de recherche.

Hans J. Herrmann,
Directeur du LPMMH, hans@ica1.uni-stuttgart.de

Définition du courrier professionnel

Jusqu'à ces derniers jours, je pensais (j'avais écouté des juristes passionnés et compétents) que la situation juridique de l'Internet (au moins l'Internet français) était claire : il n'y avait pas « vide juridique », il y avait des textes à appliquer, un point c'est tout. Cette thèse ne fait pas l'unanimité, mais elle est défendue par de nombreux juristes. Depuis la condamnation de nos collègues, j'ai changé d'avis : il n'y a pas à proprement parler « vide juridique », mais il y a « inadéquation » ; on ne peut se contenter d'appliquer les textes existants sans se poser la question de savoir si leur extrapolation à la réalité quotidienne actuelle ne serait pas source de confusions, voire d'injustices (au moins pour certains aspects particuliers, en l'occurrence le courrier électronique, pour le débat qui alimente ce numéro).

La définition qui a été donnée du courrier électronique au cours du jugement de nos collègues me semble sujette à débat contradictoire. En effet, le jugement condamne les prévenus en application d'un article du code pénal concernant les *« correspondances échangées par voie de télécommunication »* (article 432-9 du code pénal, et loi 33.1 du code des postes et télécommunications). En application de ce qui a été démontré alors, les « correspondances » mises en cause ont été qualifiées de « privées » et n'ont plus été considérées comme du courrier d'entreprise (négation de la prépondérance du caractère exclusivement professionnel de l'usage et du contenu de l'outil de travail). Or les textes définissent l'aspect « télécommunication » par *« toute transmission, émission ou réception* [...] ». Ici, il n'y a pas « interception de transmission », et je pense que le courrier électronique doit être (à défaut de faire l'objet de textes législatifs spécifiques et précis) assimilé à du courrier papier, et non pas à une communication téléphonique.

Le double caractère du courrier électronique

La législation qui a été utilisée pour condamner nos collègues a été créée dans l'esprit de réguler les « écoutes téléphoniques », suite à des affaires célèbres et médiatiques. Une communication téléphonique, pour parvenir à la connaissance d'un tiers, doit être explicitement et techniquement interceptée, et, comme le prévoit la loi, au niveau de sa transmission ou du dispositif d'émission ou de réception. De surcroît, une conversation téléphonique étant par nature volatile, il faut en général, pour matérialiser l'interception, enregistrer la communication sur un dispositif tiers ; pour en connaître le contenu, il faut la « rejouer » ou la transcrire en temps réel. Une telle interception est donc caractérisée par cet élément matériel qu'est le dispositif d'enregistrement ou de transcription. Ce caractère suffit à lui seul à démontrer l'élément intentionnel (et la mauvaise foi) de la prise de connaissance d'une communication téléphonique privée. Et nous sommes d'accord : c'est mal !

Dans le même esprit (celui de la législation invoquée), il faut également relever que le jugement requalifie le délit, pour appliquer le deuxième alinéa de l'article 432-9, c'est-à-dire pour considérer que nos collègues étaient *« chargés de mission de service public »,* facteur aggravant. Le législateur ici n'a pas voulu dire que tout fonctionnaire est investi implicitement de tous les services publics et en est responsable ! En l'occurrence, en ce qui concerne les télécommunications, il est question des agents en charge de la gestion du réseau de télécommunication **public.** Nos collègues n'avaient pas cette mission, et leur appartenance à la fonction publique ne devrait pas requalifier le délit invoqué (cette requalification n'est pas sans conséquence, puisqu'elle entraîne qu'il n'y a plus alors nécessité légale d'être de *« mauvaise foi »* pour qu'il y ait délit). Il n'échappera à personne que les matériels de l'ESPCI et du laboratoire PMMH ne sont pas un « service public », l'école n'est pas un opérateur de service public de télécommunication. La disposition d'une boîte aux lettres électronique au sein de l'école n'est pas un droit citoyen, c'est une éventuelle nécessité pour l'accomplissement d'un travail professionnel donné, et sa création et sa gestion sont un processus qui appartient à la direction de l'établissement qui apprécie cette nécessité pour un usage donné et dans un cadre contractuel, et devient par là et exclusivement un **outil de travail.**

Cela dit, ici, l'objet de la discorde n'est pas la communication proprement dite, mais un «objet» informatique bien plus complexe. Un courrier électronique subit dans sa vie plus ou moins brève un certain nombre de transformations. Sa composante « télécommunication » n'en est qu'un aspect très bref et volatil, et il est vrai que, pendant son transfert, il est imaginable qu'il soit intercepté d'une façon totalement similaire à une communication téléphonique (on pourrait appeler un tel dispositif « Échelon »...). Dans l'affaire présente, il n'y a pas eu (et le jugement ne fait pas de telle mention d'ailleurs) interception d'un signal électrique (ou optique, ...). L'élément matériel qui est en cause est un *fichier.* Techniquement, il est impossible, sans prendre connaissance du contenu d'un fichier, de connaître la nature de celui-ci. En conséquence, un fichier qui contient un courrier électronique est *strictement* identique à tous les autres fichiers présents sur le système informatique. De très nombreuses opérations techniques, routinières ou de traitement d'incidents de fonctionnement, nécessitent la prise de connaissance du contenu de fichiers présents sur le système par les exploitants. Ces exploitants ont des obligations de secret professionnel dans la mesure où une telle situation se présentera fatalement un jour ou l'autre. L'exécution de leur travail *ne permet pas* de supposer que des fichiers présentant un caractère privé échappant au règlement intérieur de l'entreprise sont présents, ou du moins que, s'il venait à y en avoir, la seule découverte de leur présence ou de leur contenu deviendrait un délit pour eux-mêmes !

Pour prendre une autre image, éloignée des définitions juridiques certes, on voit bien qu'une communication téléphonique utilise l'ouïe, et le courrier papier la vue, associée au toucher pour la rédaction (le stylo). Le courrier électronique utilise également la vue et le toucher (le clavier), et cette image confirme sa similitude avec le courrier (d'entreprise) papier. Dans sa phase matérielle, le courrier électronique *n'est pas* une télécommunication, et donc la législation concernant les télécommunications est inadaptée.

Courrier privé et courrier d'entreprise

Le jugement caractérise également le courrier électronique par *« une adresse électronique dont les deux composantes – son nom et celui de l'entité à laquelle elle est rattachée – définissent son identité informatique, qui est unique ».* Cela est parfaitement exact, mais que contient le champ caractérisant l'entité si ce n'est la raison sociale de celle-ci ? Ainsi, un courrier envoyé à <gerard.lambert@cnrs.fr> caractérise sans ambiguïté M. Lambert Gérard, employé au CNRS, et non M. Lambert Gérard, citoyen habitant (par exemple) à Paris. L'unicité de son adresse est une unicité indissociable de l'hébergement de la boîte aux lettres électronique, à savoir son lieu de travail dans l'affaire qui nous intéresse. Cela est strictement similaire à un courrier papier profes-

..... suite page 6 ..... ►

suite de l'éditorial de la page 1

motifs » introduisant la loi dont nos voisins britanniques viennent de se doter et qui autorise les entreprises à exercer une certaine surveillance sur les courriers électroniques de leurs employés. Les promoteurs de l'« Habeas Corpus Act » seraient-ils devenus moins protecteurs des libertés individuelles que nous ne le sommes ?

L'émergence des nouvelles technologies de l'information nous fait entrer dans un nouveau type de société, la société de l'information. Nos responsables gouvernementaux ont entrepris de faire élaborer de nouveaux textes et d'en adapter d'autres afin de créer un contexte juridique prenant en compte les possibilités, contraintes et problématiques nouvelles inhérentes à cette évolution. Un texte réglementant la « tolérance » que constitue l'utilisation des moyens de communication de l'entreprise à des fins personnelles aurait sans doute sa place dans la liste prévue. En tout état de cause, il nous faut continuer à assurer, autant que faire se peut, la sécurité des systèmes d'information de nos laboratoires.

Un groupe de réflexion ayant mission d'édicter des consignes à cet effet est en cours de constitution, mais la compétence technique ne parviendra sans doute pas à pallier l'absence de support à caractère législatif et réglementaire incontesté. En outre, l'émotion, tout comme la colère, est mauvaise conseillère ; il n'y a donc pas lieu de se précipiter.

À très court terme, et faute de mieux, la solution passera par une utilisation optimale de la charte et par un effort de communication des directeurs de laboratoire et des administrateurs pour y faire « adhérer » les utilisateurs, permanents et non permanents, de préférence sous la forme de l'apposition d'une signature.

Lorsqu'une situation « anormale » ne pourra être résorbée par la seule mise en œuvre de l'esprit de la charte, il conviendra d'aviser le service du fonctionnaire de défense. Celui-ci ne dispose certes pas de pouvoirs spéciaux. Il pourra en revanche conseiller un dépôt de plainte. L'effet sur l'ambiance ne sera pas des meilleurs, mais il se résorbera sans doute plus facilement que le sentiment d'impuissance, voire d'injustice, qui est actuellement perceptible chez ceux et celles qui se consacrent avec dévouement et compétence à la sécurité de nos systèmes d'information.

Alfred Schwenck
Fonctionnaire de défense

suite de la page 5

sionnel qui lui serait adressé sur son lieu de travail. Si un utilisateur du réseau désire savoir qui est responsable de l'usage de cette adresse, il consulte une base de type « internic » qui fait la relation entre le domaine (ici cnrs.fr), et l'exploitant enregistré comme étant responsable de l'usage de ce domaine et qui possède cette adresse. Cela démontre bien qu'en utilisant une adresse électronique d'employeur, on engage en premier lieu la responsabilité de celui-ci. Ce fait est d'autant plus grave si le contenu venait à être diffamatoire pour l'employeur !

Le courrier papier d'entreprise, s'il ne comporte pas (sur l'enveloppe, double si possible) de mention explicite telle que « personnel », peut bien entendu être ouvert par l'entreprise dont il est la propriété (il est susceptible de contenir des factures, des contrats, ...), il *appartient* à l'entreprise. Toute personne qui désire faire du courrier électronique à titre privé dispose de l'accès à des prestataires extérieurs qui lui permettront de le faire sans engager le nom (la réputation, la responsabilité) de son entreprise. C'est donc un choix *conscient et délibéré* de faire du courrier (électronique) privé depuis et avec du matériel d'entreprise, et en impliquant la responsabilité de celle-ci à travers l'usage de son nom. Il semble donc naturellement évident que l'usage de la messagerie électronique professionnelle à d'autres fins ne peut se faire qu'aux risques et périls de celui qui en use (abuse), car il devient inimaginable que cela puisse être aux risques et périls de celui (l'institution) au détriment duquel cet abus a lieu. Dans le cas contraire, on comprend très bien qu'en cas de faute professionnelle, il suffirait (exemple fictif) d'en faire état dans un courrier soi-disant privé en prenant soin qu'il puisse indirectement (par exemple, fictif toujours, en se plaignant auprès de l'administrateur système de la violation de sa propre messagerie) arriver à la connaissance de la direction pour tenter d'obtenir un avantage dans une procédure liée à cette faute et « retourner » la situation à son avantage.

En conséquence, et à défaut de mieux, un courrier électronique sur une messagerie d'entreprise qui ne comporte pas (en évidence, dans l'entête par exemple, le *subject*) une mention signifiant le contraire ne peut être considéré que comme non privé. Il est évident qu'il se présentera des situations techniques où la seule présence de cette mention ne suffira pas à garantir la non-divulgation du contenu à un tiers (par accident, à l'occasion d'une opération de maintenance, etc.), et que la **seule** technique qui permette de garantir la confidentialité en toute situation est le chiffrement du contenu : si, par définition, propriété mathématique, un message ne peut être lu que par son destinataire, il est clair qu'on ne pourra ni craindre qu'il perde sa confidentialité, ni se plaindre qu'il l'ait perdue. Dans une telle situation, l'employeur pourra démontrer le caractère contraire au règlement intérieur de l'usage de l'outil professionnel, mais ne se trouvera pas en situation de découvrir le contenu de correspondances privées.

Conclusions

En conclusion technique de ce papier, je tire donc au moins deux leçons de l'affaire dont il est question dans ce numéro : il faut légiférer pour traiter des spécificités concrètes de l'Internet, et ne pas tenter d'appliquer des législations qui n'ont pas intégré la complexité technique de ce réseau. Et il faut encourager le chiffrement des échanges et fournir les outils et techniques aux utilisateurs pour le faire. Cela nécessite sans doute que la législation annoncée par le Premier ministre voici près de deux ans libéralisant totalement le chiffrement en France voit le jour.

En conclusion plus personnelle, je m'interroge sur les causes de société qui ont provoqué cette affaire, et sur ses conséquences. Aujourd'hui, il va devenir difficile de trouver des volontaires pour être maire de commune, pour être directeur d'établissement scolaire, pour être médecin (anesthésiste), etc. Va-t-il devenir difficile de trouver des « volontaires » pour être administrateurs de réseaux informatiques et, encore plus, de la gestion de leur sécurité ? Jusqu'où la copie du modèle juridique américain va-t-elle envahir les esprits, pour toujours trouver dans son voisin ou son collègue un responsable de tout et de n'importe quoi, pour le plus grand profit de cabinets d'avocats « spécialisés » ?

L'obtention d'une thèse va-t-elle devenir en dernier recours dépendante d'une décision de justice et non le résultat d'un travail ?

« Summum jus, summum injuria. »*

Bernard Perrot
Laboratoire de l'accélérateur linéaire, IN2P3, CNRS
bernard.perrot@in2p3.fr

* « Comble de justice, comble d'injustice » (Cicéron).

SÉCURITÉ INFORMATIQUE
numéro 32 décembre 2000
SÉCURITÉ DES SYSTÈMES D'INFORMATION

Sujets traités : tout ce qui concerne la sécurité informatique. Gratuit.
Périodicité : 5 numéros par an.
Lectorat : toutes les formations CNRS.

Responsable de la publication :
ROBERT LONGEON
Centre national de la recherche scientifique
Service du Fonctionnaire de Défense
c/o IDRIS - BP 167. 91403 Orsay Cedex
Tél. 01 69 35 84 87
Courriel : robert.longeon@cnrs-dir.fr
http://www.cnrs.fr/Infosecu

ISSN 1257-8819
Commission paritaire n° 3105 ADEP
La reproduction totale ou partielle des articles est autorisée sous réserve de mention d'origine

Conseil et coordination : CNRS - DIST - Jacqueline Leclère • Conception et réalisation : La Souris 01 45 21 09 61