CRYPTOGRAPHIE ET LUTTE CONTRE LE TERRORISME : ÉVITER LES FAUSSES SOLUTIONS SÉCURITAIRES

par

Franck LEPRÉVOST

Professeur de mathématiques à l'Université Grenoble I
Chercheur à l'Institut Fourier

Selon des articles parus dans la presse, et pour lesquels nous ne disposons pour l'instant d'aucune confirmation officielle, il semblerait que l'organisation terroriste responsable des attentats du 11 septembre 2001 pourrait avoir utilisé la stéganographie pour communiquer de manière confidentielle. Cette méthode, qui consiste à cacher des données (du texte, des sons, des photos, etc) dans d'autres données (de nouveau du texte, ou des photos, ou des sons, ou des vidéos, etc) se distingue fortement des technologies de cryptage. En effet, s'il est aisé de voir sur le format des données transférées de manière cryptée qu'elles sont effectivement cryptées, il en va tout autrement lorsque l'on a sous les yeux, par exemple, une photo : rien ne permet a priori de savoir, juste au vu du format, qu'une photo recèle une information cachée. L'utilisation de cette technologie a en très grande partie des finalités économiques, en particulier pour la gestion des droits d'auteurs ou l'authentification des échanges électroniques. Ceci dit, les évènements tragiques ont poussé certains parlementaires américains à promouvoir un contrôle accru sur le transfert d'information, en particulier en souhaitant introduire des « trap-doors » (un point d'entrée dissimulé permettant l'écoute et le déchiffrement par les services de sécurité) dans les logiciels de cryptage, voire que soit également contrôlée l'utilisation des moyens de stéganographie.

Nous comprenons parfaitement que de telles réactions se fassent jour dans l'urgence, mais il nous semble que profiter de l'horreur des attentats de New York et de Washington pour renforcer exagérément le contrôle de l'usage des technologies de sécurité serait une réponse inadaptée et dont les effets pervers pourraient être dangereux pour les libertés individuelles et pour l'économie européenne.

Certes, il peut paraître choquant que certaines techniques numériques de stéganographie puissent déjouer les contrôles qui existent encore aujourd'hui sur l'exportation (depuis les États-Unis et les autres membres du « Wassenaar Agreement ») ou sur la vente et l'utilisation (comme en France) des moyens de chiffrement. Dans notre rapport au Parlement européen de 1999 (1), nous avions déjà signalé que ces techniques non contrôlées à l'exportation seraient pourtant utilisables pour contourner les restrictions juridiques actuelles. A titre d'exemple, l'on peut cacher 3 pages de texte dans 30 secondes de vidéo, et ce de manière quasi-indétectable, comme l'ont notamment montré certains travaux (2) que nous avions mené en collaboration avec des collègues de l'EPFL. Faut-il pour autant en conclure qu'il est urgent de renforcer les contrôles sur la circulation des technologies de sécurité et de mettre sous surveillance les moyens de stéganographie et de watermarking ? Nous ne le pensons pas. Comme nous le disions dans ce même rapport de 1999, il est évident qu'une organisation mafieuse ou terroriste n'utilisera pas des moyens légalement autorisés dont elle sait qu'ils comporteraient souvent une « trap-door ». Lorsque l'on constate le luxe de précautions qui a été pris apparemment pour la préparation des attentats du 11 septembre, on peut être sûr que ce genre de groupe préférera — surtout s'il est bien doté financièrement — payer quelques ingénieurs (au besoin en les envoyant étudier par exemple dans une université européenne) pour développer un cryptosystème à usage interne et qui utilisera des clefs de longueur arbitraire.

Une mesure de renforcement des prohibitions et des contrôles sur ces technologies numériques n'aurait donc aucun effet réel sur l'état

(1) Franck Leprévost, *Encryption and cryptosystems in electronic surveillance : a survey of the technology assessment issues*, Rapport pour le service d'études du Parlement Européen, STOA, PE 168.184/Vol 3/5/EN, novembre 1999.

(2) Touradj Ebrahini, Raphael Erard, Martin Kutter, Franck Leprévost, Diego Santa Cruz, *How to bypass the Wassenaar Arrangement : A new application for watermarking*, 8th ACM International Multimedia Conference on Multimedia and Security, November 2000, Los Angeles, California, USA.

de la menace terroriste. En revanche, elle ralentirait encore plus la propension (pourtant déjà faible) des entreprises et des utilisateurs des réseaux à se protéger contre le piratage informatique et les différentes formes de criminalité informatique (détournements de données, contrefaçons, ...). Plus précisément encore, une telle politique porterait un coup fatal au développement de l'usage de ces technologies de sécurité (et particulièrement du watermarking et de la signature électronique) pour protéger les droits d'auteur sur l'Internet, comme cela vient pourtant d'être reconnu et encouragé officiellement par la récente directive du 22 mai 2001 sur le droit d'auteur dans la société de l'information (3). Enfin, le gouvernement fédéral américain — qui cherche depuis longtemps à surveiller l'Internet et ses technologies — pourrait profiter de la légitime indignation mondiale actuelle pour tenter de renforcer officiellement sa mainmise sur le cyberespace.

Si l'on en juge par les amendements à la loi sur la sécurité quotidienne qui viennent d'être votés par le Parlement, il semble que les autorités françaises veuillent raison garder dans ce domaine et se contentent de renforcer les pouvoirs de la justice pour obtenir — en cas d'enquête criminelle — la « mise au clair » des données chiffrées (y compris en réquisitionnant les moyens secrets de la défense nationale ou en contraignant un éventuel prestataire de services à livrer une clé de chiffrement). Et il ne semble pas qu'à l'heure actuelle, il soit question de renforcer les contrôles préventifs sur l'usage ou la circulation des technologies, ni de renoncer à l'allégement des contrôles actuels lors de l'adoption (sans doute en 2002) de la future loi sur la société de l'information.

Espérons qu'il en ira de même au niveau européen. Chacun doit être bien conscient du risque qu'il y aurait à vouloir, de manière démagogique ou irréaliste, bâtir une « muraille de Chine » autour de technologies numériques déjà disponibles dans le monde entier et qui sont appelées à jouer un rôle majeur dans la mise en place des infrastructures de sécurité pour notre société de l'information (notamment à l'encontre des agissements bien réels de la criminalité organisée). Au moment où les applications pratiques de la signature électronique (entrée pourtant en vigueur par la loi du 13 mars 2000) et des systèmes de paiement en ligne et de protection numérique des droits d'auteur tardent à apparaître, il faut absolument éviter de sacrifier la vraie sécurité quotidienne de l'information à une pseudo-protection de la société contre des menaces terroristes exceptionnelles et, par nature, changeantes et imprévisibles.

Les effets pervers que nous identifions dans la mise en œuvre de mesures de contrôle trop stricts et trop indiscriminés pourraient, en effet, être importants : dissuader ceux qui n'ont rien à se reprocher d'utiliser des moyens de sécurité fiables ou les mettre en situation d'être espionnés en permanence et de voir leur vie privée ou leurs intérêts économiques légitimes compromis, sans que les criminels ou les terroristes ne soient dérangés de manière efficace dans leurs activités. De plus, il nous semble qu'il y aurait là une grande tentation de détournement des informations, notamment pour certaines officines gouvernementales anglo-saxonnes. Même s'il n'est pas établi que le système « Echelon » mis en œuvre par les pays de l'alliance UKUSA constitue aujourd'hui ce véritable « Big Brother » mondial que certains redoutent, il ne faudrait pas que l'objectif — légitime — de la lutte internationale contre le terrorisme donne finalement aux États-Unis un moyen supplémentaire pour déployer enfin officiellement et à grande échelle un véritable système de traçabilité et d'interception électronique mondial. La protection de l'économie européenne est sans doute également en cause dans ce débat.

F. L.

---

(3) Sur les questions soulevées par la prise en compte des technologies de sécurité dans le contexte de la directive sur le droit d'auteur, cf. Franck Leprévost & Bertrand Warusfel, *Technologies de sécurité pour les médias digitaux*, Rapport pour le service d'études du Parlement Européen, STOA, PE 296.705/ Fin. St., mai 2001.