Le Monde.fr

29/11/2012 14:25

Irène Bouhadana, Yves Charpenel, Christiane Féral-Schuhl, William Gilles, Jean-Christophe Le Toquin,

Comment mieux protéger les citoyens et l'économie contre le cybercrime ?

En 2011, le coût global du cybercrime était estimé à 338 milliards de dollars, dépassant le trafic de drogue. Selon une étude de 2010 citée par l'OTAN et l'agence européenne ENISA, contrôler un réseau de dizaines de milliers d'ordinateurs personnels pour les faire participer à des attaques contre des gouvernements ou pour des activités frauduleuses, rapporte de 10 000 dollars à 10 millions de dollars à leurs instigateurs.

Comme toute forme de délinquance, la cybercriminalité légitime des réponses préventives et répressives. Si la lutte contre la cybercriminalité présente des enjeux d'importance évidente, son cadre juridique et institutionnel reste perfectible.

Irréel. Le cybercrime est en droit une notion quasiment irréelle. Aucun texte ne le définit, et celui-ci se résume à quelques incriminations spécifiques à la cybercriminalité telles que la consultation d'images de mineurs à caractère pornographique par exemple. Au niveau de la justice, seuls sont disponibles les chiffres des condamnations. Comme il n'y a pas de condamnation sans texte, et qu'il n'y a pas de texte, comment s'étonner que des magistrats peinent à cerner la réalité du phénomène ?

Insaisissable. Où le cybercrime est-il commis ? Sur les serveurs ? Peut-être : l'article 113-2 du Code pénal fait appliquer la loi française dès lors que l'un des faits constitutifs de l'infraction a lieu sur le territoire français. La localisation des serveurs d'où sont diffusés les éléments susceptibles de constituer une infraction a donc un impact limité sur la compétence juridictionnelle française. Chez le citoyen qui peut y être exposé ? Peut-être : dans un arrêt du 29 mars 2011, la chambre commerciale de la Cour de cassation a affirmé que le juge français n'est compétent que lorsque le contenu du site concerné est *«orienté vers un public français»*.

Submergeant. Les cybercriminels stockent et échangent des terra-octets de données, qui submergent la capacité opérationnelle de traitement des enquêteurs, alors qu'il n'existe pas de texte de procédure pénale spécifique et clarifié couvrant les aspects de l'enquête en environnement numérique. Il n'existe pas non plus de texte adapté à la perquisition des données stockées «dans le nuage»... un service qui est pourtant aujourd'hui aussi banal qu'un compte email ou un réseau social.

Hors d'atteinte. La mise en place d'une entraide répressive internationale avec des équipes communes d'enquêtes entre Etats désireux de respecter loyalement les principes procéduraux a requis plusieurs dizaines d'années. Combien de temps faudra-t-il attendre des équipes communes de cyber-enquêtes ?

Clos. La justice française ne dispose pas de services dédiés à la lutte contre la cybercriminalité alors

Comment mieux protéger les citoyens et l'économie contre le cybercrime ?

qu'un tel dispositif existe actuellement dans tous les pays européens ou ailleurs comme au Canada par exemple. Faute de direction, les différents acteurs concernés, qu'ils soient experts judiciaires en informatique ou prestataires techniques, demandent à multiplier les échanges avec les magistrats. Les divers services de l'Etat n'ont pas d'interlocuteur dédié au sein du système judiciaire.

Intransmissible. La lutte contre la cybercriminalité ne pourra être efficace que si tous les acteurs concernés sont formés à ces problématiques, ce qui suppose de renforcer la place du droit numérique non seulement à l'université mais aussi au niveau de la formation professionnelle des avocats et des magistrats. Si certaines universités s'approprient le sujet et commencent à dispenser des formations dédiées, la place du droit numérique au sein du monde académique reste encore insuffisante au regard des enjeux.

Alors que les lacunes sont réelles, ces enjeux appellent des réponses à la hauteur de la protection de l'ordre public. Chacun dans son rôle mesure l'étendue du problème.

A côté des magistrats et des policiers, l'avocat est lui-même dans une position complexe. Il a un rôle social, porté pour l'essentiel par son Barreau, qui est de veiller au respect des libertés publiques et du droit de chacun de n'être poursuivi qu'en vertu de textes existants, présents, concrets et non de projets anticipant une évolution incertaine et imprévisible. Aujourd'hui règne l'empirisme. On va chercher du droit là où il existe pour le transposer dans un univers qui lui est complètement étranger. Il est évident que si cela peut pallier au plus pressé il ne s'agit que de pis-aller qui atteignent très vite leurs limites.

COMPLÉMENTARITÉ ENTRE ACTION PUBLIQUE ET PRIVÉE

Face à cette réalité, les praticiens du droit, législateur, magistrats et policiers, avocats et juristes d'entreprises, professeurs apparaissent démunis. Pourtant ils ont la compétence nécessaire et les projets propres à faire face aux défis du cybercrime. Mobilisés, ils peuvent permettre que le droit facilite le partage d'informations sur les atteintes et les infractions, permette la lutte contre les infractions et assure la protection des victimes dans le respect des droits de la défense et la protection des libertés individuelles.

Face à une menace toujours plus complexe techniquement et transversale aux différentes composantes humaines et techniques de notre société, il est temps de coordonner l'action des autorités publiques, des autorités indépendantes, du monde de l'entreprise (télécoms, banques, groupes industriels), du secteur associatif et des universités, et de redonner sa voix au citoyen. La complémentarité est réelle entre action publique et privée contre le cybercrime ; méconnue, elle a fortement besoin d'être relayée et étendue sur le plan gouvernemental et interministériel.

Il n'est plus possible de remettre à plus tard les mesures proportionnées qu'exige la lutte efficace contre le cybercrime, sans manquer à la mission primordiale du gouvernement, qui est d'assurer la protection des citoyens et des entreprises.