



Halte à la liberté

Liberté, j'écrivais ton nom



REPORTER VILLAGEOISE

SERKET

03.01.1967.F
PARIS RP - FRANCE
Responsable de la rubrique Droit.
Retenue en région parisienne par ses obligations professionnelles, elle aspire à une retraite méritée mais encore lointaine sous des cieux plus cléments.

Il en était question depuis plusieurs années, l'épée de Damoclès surplombait la toile inexorablement. Le couperet menaçait de tomber sur le cou des acteurs de l'Internet que sont les fournisseurs d'accès, webmestres et internautes. L'attente si longue va enfin se terminer. Cette fois, l'heure fatidique est toute proche !

Depuis octobre 1999, lors de l'élaboration du projet de loi sur la société de l'information, le Parlement européen cherchait à détruire une idée bien ancrée dans les esprits, idée selon laquelle Internet serait une zone libre de droit !

À l'époque, les textes proposés semblaient trop rigides, pas assez réalistes par rapport au contexte du net, encore mal défini. Il restait

des zones d'ombres, des litiges difficiles à régler faute de règlement adapté et suffisamment précis. Les états membres ont analysé les phénomènes qui se produisaient sur leurs territoires respectifs, ils ont remanié en conséquence leurs propositions. Un texte définitif n'était pas envisagé à court terme, compte tenu de la difficulté à harmoniser les législations. Dans ce petit monde, les attentats aux

États-Unis ont bousculé la machine bureaucratique.

Les mesures prises en urgence le 20 septembre 2001 par le Conseil des ministres européens de la Justice et des Affaires intérieures, la nécessité de fixer rapidement une définition et des dispositions communes concernant la cybercriminalité semblèrent une évidence. Le cybercrime est donc dorénavant défini comme suit : les infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques, les infractions informatiques, les infractions liées à la pédophilie, celles relatives aux atteintes à la propriété intellectuelle et aux droits connexes. Ainsi, a-t-il été d'abord proposé que les infractions, au nombre de treize, seraient sanctionnées selon leur gravité entre deux ans de prison (pour vol) jusqu'à vingt ans (pour infraction terroriste). Le dessein du Parlement européen avec la signature de cette convention, première du genre au niveau mondial, vise à garantir la sécurité du réseau Internet qui compte près de 400 millions d'utilisateurs, qu'ils soient simple individu ou personne morale. Par conséquent, si l'on considère le coût de la cybercriminalité, dont le chiffre est représenté comme un trou noir, tant il est difficile de pouvoir l'estimer, on agrée forcément leur position. On suppose qu'il représente plus de 1 600 milliards de dollars dans le cadre seulement des attaques de sécurité aux entreprises, selon un sondage réalisé par *Information Week Research*. On ignore ce qu'il en est pour les personnes physiques, mais on imagine aisément la détresse des

victimes de hackers malveillants. On y répond d'autant plus favorablement quand on apprend qu'il aura fallu la participation de 19 pays, dix mois d'enquête, pour arrêter un réseau de 130 personnes dont l'activité portaient atteinte à l'intégrité d'enfants. 10 000 utilisateurs, amateurs d'images pédophiles ont été découverts, connectés sur plus de 30 sites web diffusant sans scrupule ces photographies. Selon l'*UNICEF*, il y aurait dans le monde, 200 000 clients pour ce type de commerce et près de 150 000 sites pédocriminels.

Ca fait frémir !

On enrage aussi à l'idée de ne pouvoir obtenir réparation, lorsque l'on est victime d'une arnaque bien huilée, réalisée par de jeunes internautes venus d'un pays très peu regardant en matière de criminalité en ligne.

Le principe est simple : se faire passer pour un citoyen américain désireux de vendre à un coût réduit un objet (un téléphone portable par exemple), rassurer l'acheteur en lui transmettant des documents UPS permettant de traquer le colis soi-disant envoyé afin que ce dernier accepte d'adresser sans délai la moitié de la somme convenue en attendant la livraison, qui n'arrivera jamais à destination. Les brigades de police d'Interpol ne sont pas suffisamment formées, ni même qualifiées pour pouvoir réagir sans perte de temps et un Cyberpol n'est pas encore envisagé. La technologie évolue plus vite que les décisions institutionnelles, surtout quand elles engagent la responsabilité de nombreux États.

CECI-DIT...

ADIJ ?

L'Association pour le Développement de l'Informatique Juridique a pour vocation de suivre l'actualité juridique de la nouvelle société de l'information au travers d'ateliers, de colloques et de publications.

On peut citer comme sujets traités, outre la responsabilité des hébergeurs :

Droit d'auteur et Internet, e-commerce, preuve électronique, Droit du travail et NTIC...

www.adij.asso.fr



CECI-DIT...

GFII ?

Le Groupement Français de l'Industrie de l'Information (GFII) fédère les acteurs tant publics que privés de l'information électronique professionnelle. Par la définition d'objectifs communs, les membres du GFII constituent un groupe d'influence pour faire valoir et défendre le point de vue des professionnels de l'information électronique auprès des pouvoirs publics et institutionnels français et communautaires.

www.gfii.asso.fr



Aussi fallait-il rapidement prendre des dispositions radicales afin d'endiguer le flot de cybercriminalité, en attendant une révision des mesures, prévue d'ici trois ans, une fois que le système aura été mis en application et affichera ses faiblesses et ses qualités.

Trop vite ?

Malheureusement, la précipitation est souvent mauvaise conseillère. Bon nombre de mesures importantes ont été omise ou sont maintenant en contradiction avec les textes dans leur application. En effet, plusieurs points de discordance font leur apparition.

Jusqu'ici les données relatives au trafic internet et tous les enregistrements des événements survenus sur les forums et salons ne devaient être conservés que pour une durée allant de 15 à 90 jours. Afin d'enrayer le problème du « cybervandalisme », dorénavant, les fournisseurs d'accès et les responsables de site devront pouvoir présenter ses informations sur demande officielle des institutions désignées et ce pendant un an. Autant déclarer immédiatement forfait pour certains petits sites, tant le coût de l'investissement supplémentaire est important. Malheureusement, les États, s'ils souhaitent voir se mettre en place une barrière de sécurité, ne donnent pas les moyens financiers à leurs partenaires pour parvenir

à un travail en partenariat qui pourrait être constructif à défaut d'être unanime.

Le problème se pose également quant aux données personnelles. Les responsables de sites sont tenus de respecter certains principes qui garantissent la protection de ces dites données. Selon la loi « Informatique et Liberté » du 6 janvier 1978, on est normalement assuré qu'au bout d'un an, elles ne seront pas oubliés dans le coin d'un registre et de ce fait, à la disposition de celui qui les découvrira. Le respect de la vie privée est également touché puisque les services de Police cybernétique sont autorisés à intercepter des messages, même cryptés, s'ils leurs semblent suspects.

Personne n'est à l'abri d'une erreur et ainsi n'importe quel courriel qu'il s'agisse d'une simple liste de courses à un message de menace pourra être épluché. L'humain a parfois du mal à garder le secret, et l'on imagine aisément que le principe de confidentialité sera bafoué presque aussi souvent qu'un message croustillant sera intercepté.

Or, les infractions de confidentialité sont qualifiées de Cybercrime. Oups ! Personne n'a d'ailleurs l'assurance que certains messages dignes d'intérêt pour la sûreté des États ne passeront pas au travers des mailles du filet, tant le volume d'informations à traiter est gigantesque.

En attendant, si chacun surveille son troupeau, les bêtes seront bien gardées ! •

POUR EN SAVOIR PLUS

Isijolie

www.isijolie.net

Le point sur Iris

www.iris.sgdg.org/les-iris/lbi/index.html

SERKET
serket@free.fr