



**Éléments de langage de M. Brice HORTEFEUX,
ministre de l'intérieur,
de l'outre-mer et des collectivités territoriales**

forum international sur la cybercriminalité

**prononcé par Jean-Michel BERARD, Préfet de la région Nord – Pas
de Calais, Préfet du Nord**

Lille, mercredi 31 mars 2010

– Seul le prononcé fait foi –

Mesdames et Messieurs,

Si je n'ai pu être présent parmi vous, aujourd'hui, à l'occasion de cette 4^{ème} édition du forum international sur la cybercriminalité, j'ai tenu à vous faire parvenir ces quelques mots.

Vous entamez aujourd'hui deux journées de réflexion et de travail. Les questions de sécurité, de justice et de défense seront évoqués, ainsi que les enjeux du développement de la société numérique pour nos collectivités territoriales et les moyens de protéger nos entreprises face aux risques numériques *[diffusion du guide pratique du chef d'entreprise face au risque numérique dont vous avez signé la préface]*.

Le réseau internet est, en effet, devenu un vecteur de communication d'une puissance jamais atteinte. Il donne lieu au développement d'une économie, favorise les échanges et l'émergence d'une culture, notamment au travers des blogs et des nouveaux services interactifs.

Ces aspects positifs ont cependant un revers : l'émergence et la facilitation, dans un total anonymat, de nombreuses formes de délinquance qui se jouent des frontières et des législations : escroqueries, usurpation d'identité, vols de numéros de cartes bancaires, piratage, mais aussi pédopornographie, terrorisme, pénétration de réseaux ou prise de contrôle à distance de systèmes d'informations stratégiques.

Enjeu fondamental pour la sécurité nationale, les nouvelles technologies de l'information doivent donc être à la fois protégées et maîtrisées sous peine d'être infiltrées ou dévoyées.

I. Où en sommes-nous de la lutte contre la cybercriminalité ?

(1) Le constat reste, aujourd'hui, préoccupant.

La cybercriminalité est essentiellement une criminalité transnationale. Concrètement, une action commise par une personne dans un pays peut affecter des milliers de personnes dans plusieurs autres pays.

Les acteurs économiques sont des cibles de choix, tout comme les administrations publiques et les citoyens. Il faut le dire : il existe encore, en France comme dans les pays industrialisés, de nombreuses infrastructures extrêmement vulnérables à la criminalité informatique, susceptibles de déstabiliser l'économie entière d'un pays. Je pense notamment à ce pirate informatique, « hacker-croll », interpellé la semaine dernière à Clermont-Ferrand, grâce à la coopération des autorités américaines, et qui était en mesure d'infiltrer le réseau social Twitter.

(2) Face à cette menace, il est non seulement nécessaire d'accroître la coopération avec tous les acteurs de l'économie numérique mais aussi de renforcer l'action internationale

→ Pour être pleinement efficaces, les enquêtes de cybercriminalité requièrent, tout d'abord, une coopération accrue avec les fournisseurs d'accès et de services sur Internet.

Dans les faits, la lutte contre la cybercriminalité se heurte parfois à des obstacles en raison de la complexité des réseaux informatiques, de la rapidité avec laquelle les infractions sont commises et de la difficulté à rassembler les preuves, généralement électroniques et volatiles.

Je sais que forces de l'ordre et fournisseurs d'accès ont chacun un rôle bien précis : les uns doivent faire respecter la loi, les autres doivent offrir à leurs clients la capacité de communiquer. Mais nous poursuivons tous le même but : rendre Internet plus sûr.

C'est tout le sens de ce forum international auquel vous participez, que vous soyez élus, responsables des collectivités territoriales, universitaires, issus du monde de l'entreprise, ou représentants des forces de sécurité et des pouvoirs publics.

Je tiens d'ailleurs à féliciter tous ses organisateurs, la gendarmerie, l'union européenne, les pays partenaires, les collectivités et les grandes sociétés, qui ont permis de réunir plus de 1 500 participants, acteurs publics, fournisseurs d'accès, juristes, clients, pendant ces 2 jours pour débattre de ce sujet et proposer de nouveaux partenariats.

→ Vos travaux vont vous conduire à réfléchir sur la mobilisation européenne et internationale nécessaire pour améliorer la lutte contre la cybercriminalité.

Votre rendez-vous intervient quelques jours après la conférence de Strasbourg sur la coopération contre la cybercriminalité [23 au 25 mars 2010] et quelques jours avant le congrès des Nations Unies sur la prévention de la

criminalité et la justice pénale [12 au 19 avril 2010]. Celui-ci sera l'occasion, pour le Conseil de l'Europe, de lancer un appel en faveur d'un soutien mondial pour permettre aux Etats de répondre aux défis liés à la cybercriminalité, en s'appuyant au mieux sur les outils et les instruments existants, dont sa Convention sur la cybercriminalité [adoptée à Budapest en 2001], aujourd'hui ratifiée par de nombreux pays [29 pays, avec l'adhésion du Monténégro, du Portugal et de l'Azerbaïdjan lors de la conférence de Strasbourg la semaine dernière].

Vous évoquerez notamment la plate-forme européenne de signalement des contenus illicites sur Internet. Cette plate-forme européenne, dont l'annonce avait été faite lors de la présidence française de l'Union européenne, mobilise toutes les énergies. De nombreux pays, déterminés à voir aboutir ce projet, se mettent en ordre de bataille. Je vous le dis : je souhaite que tout soit mis en œuvre afin que ce projet aboutisse le plus rapidement possible. La protection de nos enfants des prédateurs sexuels sur Internet est une priorité qui ne peut attendre.

II. La mobilisation des pouvoirs publics contre la cybercriminalité est une priorité et la France y associe étroitement les acteurs privés.

(1) Il faut développer la politique nationale de sécurité des entreprises.

Les acteurs économiques et les utilisateurs d'Internet ont pris conscience qu'ils constituent des cibles pour les cybercriminels.

J'ai demandé aux services du ministère de continuer d'apporter aux entreprises un soutien actif dans l'évaluation du « cyber-risque » et dans la préparation des plans de protection de leurs implantations.

Des plans triennaux de promotion de l'intelligence économique ont été mis en place par chaque préfet de région. Ils ont pour objectif la promotion des mesures les plus adaptées pour mieux sécuriser la circulation de l'information au sein des entreprises implantées dans leur région.

Je rappelle que des observatoires zonaux de sécurité des systèmes d'information ont également été créés, récemment, sous l'autorité des préfets de zone. Ils s'adressent notamment aux chambres professionnelles et servent, entre autre, à sensibiliser les responsables économiques, à les aider à mieux protéger leurs informations sensibles et à maintenir leur activité.

C'est, d'ailleurs, l'objet du « guide du chef d'entreprise face au risque numérique » que vous avez reçu en participant à ce forum. Fruit de la réflexion commune d'acteurs publics et privés, il permet à l'entrepreneur de prendre connaissance des risques que court son entreprise dans le domaine numérique et de découvrir les solutions mises à sa disposition.

(2) Outre les entrepreneurs, les fournisseurs d'accès ont un rôle majeur à jouer pour l'information des utilisateurs.

Les fournisseurs d'accès et de services à Internet doivent continuer de protéger le mieux possible leurs clients dans le cadre du projet d'accord qui lie le ministère de l'intérieur et l'association des fournisseurs d'accès et de services Internet (AFA).

Il est évidemment normal que les utilisateurs soient informés sur les risques que peut présenter Internet pour leurs droits, leur sécurité et leur vie privée. Il est aussi nécessaire qu'ils soient informés sur les outils et les logiciels disponibles à utiliser pour une meilleure protection.

(3) Nos forces de sécurité s'investissent également totalement dans la lutte contre la cybercriminalité

450 enquêteurs spécialisés dans la lutte contre la cybercriminalité ont déjà été formés au sein de la police et de la gendarmerie. J'ai fixé à 600 le nombre de personnels formés d'ici 2012. Ces enquêteurs sont notamment chargés de la recherche et de la préservation des preuves numériques des infractions.

Depuis l'été dernier, des policiers et gendarmes effectuent des cyber-patrouilles. Cette nouvelle forme d'investigation, basée sur l'infiltration, favorise l'administration de la preuve pour une plus grande efficacité des enquêtes. A ce jour, plusieurs dizaines de dossiers ont été menés à terme avec interpellation des prédateurs qui ont été déférés devant la justice. J'ai demandé que le nombre des personnels, habilités à effectuer ces cyber-patrouilles, soit augmenté dès 2010.

Outre ces enquêteurs, la plate-forme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (P.H.A.R.O.S.), composée de policiers et de gendarmes, a pour objectif le recueil et le traitement des signalements des contenus illicites d'Internet. En 2009, elle a reçu près de **53 000 signalements**, soit plus de 1 000 signalements par semaine. La moitié concernaient des escroqueries commises sur Internet ; 28% des

atteintes sur les mineurs et 5% des actes relatifs à la xénophobie et discrimination. Depuis le 1er janvier 2010, ce sont déjà **18 355 signalements** qui ont été reçus, dont 4 296 concernent des atteintes contre les mineurs *[soit plus de 23%]*.

Enfin, une plate-forme téléphonique « info-escroqueries », dédiée à l'information du public, a également été mise en place l'année dernière. Elle a déjà traité plus de **20 000 appels** dont près de la moitié concernaient des victimes d'infraction.

III. Aujourd'hui, une part importante de la solution passe par une législation claire et adaptée qui définisse les responsabilités de chacun. C'est l'enjeu de la LOPPSI.

(1) J'entends, en premier lieu, bloquer les sites et contenus à caractère pédopornographiques.

Le Gouvernement n'a pas l'intention de bouleverser l'équilibre d'ensemble établi par la loi du 21 juin 2004 pour la confiance dans l'économie numérique, qui a établi le droit sur Internet. Il n'est absolument pas dans ses intentions de restreindre l'accès des citoyens à Internet. Cependant, Internet ne peut devenir un espace de non-droit.

Or, un nombre croissant d'infractions sont commises par son biais, notamment la pédopornographie. C'est une obligation morale que d'adapter la réponse de l'Etat à cette violence. Derrière les contenus pédopornographiques, nous le savons, il y a la prostitution infantile, des viols et la criminalité organisée.

C'est la raison pour laquelle, à l'instar de ce qui existe dans de nombreuses démocraties voisines, la LOPPSI crée un dispositif autorisant le blocage de l'accès aux sites et contenus à caractère pédopornographique.

Le principe est simple : le ministère de l'Intérieur indique aux fournisseurs d'accès à Internet la liste noire des sites et contenus à bloquer, et ce sont les fournisseurs qui empêchent l'accès à ces sites et à ces contenus depuis un ordinateur en France.

J'entends les voix qui s'élèvent pour dire, en même temps, que la lutte contre la pédopornographie rassemble et ne fait pas débat, et que les mesures proposées par le Gouvernement ne sont pas efficaces et seront très vite contournées en faisant peser une menace de blocage sur Internet.

J'entends aussi, et ce sont souvent les mêmes, ceux qui considèrent que les policiers et les gendarmes, dont c'est le métier, ne seraient pas capables, sans porter atteinte aux libertés fondamentales, d'identifier les sites en infraction pour en dresser la liste, alors que les internautes le font sans difficulté.

Car il faut le constater, les internautes sont de plus en plus matures et responsables, y compris lorsqu'ils sont mineurs, et reconnaissent de mieux en mieux les infractions. Moins de 7% des signalements reçus en 2009 par la plate-forme PHAROS étaient infondés. C'est également le constat que fait l'AFA, qui a reçu près de 8 000 signalements sur son site en 2009 [*pointdecontact.net*] et qui agit, comme d'autres acteurs privés, en parfaite complémentarité avec la plate-forme de signalement du Gouvernement. Cette association constate, d'ailleurs, qu'en 2009, les sites signalés par les

internauts comme présentant un contenu pédopornographique sont en augmentation de plus de 30% par rapport à 2008.

A tous, je réponds qu'il est urgent d'agir pour limiter préventivement l'accès des internautes à de tels sites. A tous, je réponds que l'efficacité est dans le pragmatisme et qu'il ne faut pas renoncer parce que la solution n'est pas absolument parfaite. C'est bien l'addition de plusieurs mesures – le renforcement de la coopération internationale, avec la création de la plateforme européenne de signalement, et les techniques de blocage des fournisseurs d'accès - qui nous permettra de faire reculer la pédopornographie sur Internet.

(2) Je suis aussi totalement déterminé à lutter contre l'usurpation d'identité sur les réseaux de télécommunications

Aujourd'hui, l'usage d'éléments d'identité d'un tiers sur un réseau de télécommunications n'est réprimé que lorsqu'il en résulte un préjudice financier.

Cela ne suffit pas. L'engouement pour les réseaux sociaux, par exemple, comme « facebook » ou « twitter », où l'on expose sa vie privée sans toujours en maîtriser les conséquences, que vous avez évoqué pendant ces 2 jours, nous invite à mettre en place des dispositifs de régulation.

C'est pourquoi j'ai souhaité que le fait d'usurper l'identité d'une personne sur internet, même s'il n'y a pas de préjudice financier, soit désormais condamnable. Il n'est plus question de nier le préjudice moral que représente l'utilisation de l'identité d'une personne sur des forums de toute

nature ou encore son inscription, à son insu ou contre son gré, sur des réseaux sociaux. C'est à la loi de protéger ces victimes et c'est mon rôle de faire voter ces lois.

X

La mission que m'a confié le Président de la République, celle de protéger tous les Français, suppose un engagement total de ma part pour améliorer, au quotidien, le dispositif de sécurité dans notre pays. Assurer la sécurité des Français et des acteurs économiques sur Internet n'est pas une mission simple.

Face aux atteintes, parfois extrêmement violentes, que peuvent subir nos entreprises ou des personnes vulnérables, vous ne m'entendrez jamais dire « *nous n'y pouvons rien – on a tout essayé* ».

Ceux qui rejettent toute amélioration du dispositif actuel se trompent. C'est mon devoir de responsable politique de rechercher et de proposer toutes les pistes d'amélioration possibles.

Loin de tout sensationnalisme, je souhaite avancer avec sérénité et conviction sur ce dossier majeur. Et je sais que je ne suis pas seul. La collaboration entre usagers, fournisseurs d'accès et autorités publiques, au niveau national et international, constitue la clé du succès.

Soyez assurés de mon entière détermination à répondre au défi que constitue la lutte contre la cybercriminalité.