



COMMISSION DES COMMUNAUTÉS EUROPÉENNES

Bruxelles, 15.11.2006  
COM(2006) 688 final

**COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN, AU  
CONSEIL, AU COMITÉ ÉCONOMIQUE ET SOCIAL EUROPÉEN ET AU COMITÉ  
DES RÉGIONS**

**sur la lutte contre le pourriel, les espioniciels et  
les logiciels malveillants**

**COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN, AU  
CONSEIL, AU COMITÉ ÉCONOMIQUE ET SOCIAL EUROPÉEN ET AU COMITÉ  
DES RÉGIONS**

**sur la lutte contre le pourriel, les espioniciels et  
les logiciels malveillants**

**(Texte présentant de l'intérêt pour l'EEE)**

**1. OBJET DE LA COMMUNICATION**

On constate chaque jour davantage à quel point les réseaux et services modernes de communications électroniques font partie de la vie quotidienne, au bureau ou à la maison. Et, pour être largement adoptés, ces services doivent reposer sur des technologies fiables, sûres et performantes. La communication de la Commission relative à une stratégie pour une société de l'information sûre<sup>1</sup> vise à accroître la sécurité des réseaux et de l'information en général, et invite le secteur privé à corriger les failles des réseaux et systèmes informatiques qui peuvent être exploitées pour la diffusion de pourriel et de logiciels malveillants. La communication de la Commission concernant le réexamen du cadre réglementaire de l'UE propose de nouvelles règles pour renforcer la sécurité et la protection de la vie privée dans le secteur des communications électroniques<sup>2</sup>.

La présente communication traite de l'évolution du pourriel<sup>3</sup> et des menaces que constituent les espioniciels et logiciels malveillants. Elle fait le point des efforts déployés jusqu'à maintenant pour faire face à ces menaces et recense les autres mesures qui peuvent être prises comme, par exemple:

- renforcement de la législation communautaire
- application de la loi
- coopération dans et entre les États membres
- dialogue politique et économique avec les pays tiers
- initiatives des entreprises
- activités de R&D.

---

<sup>1</sup> COM(2006) 251 final

<sup>2</sup> COM(2006) 334 final

<sup>3</sup> COM(2004) 28 final

## 2. LE PROBLEME: LE CARACTERE CHANGEANT DES MENACES

Le pourriel<sup>4</sup> a considérablement augmenté au cours des cinq dernières années<sup>5</sup>. Des sources professionnelles indiquent qu'il représente désormais entre 50 et 80% des messages envoyés aux utilisateurs finals<sup>6</sup>. Même si la majeure partie du pourriel provient de l'extérieur de l'UE, les pays européens relayent aujourd'hui 25% des messages non sollicités<sup>7</sup>. Au niveau mondial, le coût du pourriel a été estimé à 39 milliards d'euros. En Europe, il a été estimé à environ 3,5 milliards d'euros en Allemagne, 1,9 milliards d'euros au Royaume-Uni et 1,4 milliards d'euros en France<sup>8</sup>. Le pollupostage est désormais considéré comme une activité à part entière, les polluposteurs louant ou vendant à des sociétés, aux fins de prospection, les listes d'adresses électroniques qu'ils ont récoltées. Et le pourriel sur internet est particulièrement lucratif. Cela tient à la portée de ce moyen de communication et au faible coût qu'implique l'envoi massif de messages. Parallèlement, investir ne serait-ce que modérément dans la lutte antipourriel peut aussi donner des résultats significatifs. Par exemple, aux Pays-Bas, on est parvenu à réduire le pourriel néerlandais de 85% en investissant **570 000 euros** dans des dispositifs de lutte antipourriel.

Le courrier électronique non sollicité a cessé d'être une simple nuisance et devient peu à peu une activité de nature frauduleuse et délictueuse. Un exemple patent en est le recours aux courriels hameçons qui persuadent l'utilisateur final de révéler des données confidentielles à l'aide d'une imitation de site censée représenter de véritables sociétés, ce qui fait craindre des cas éventuels d'usurpation d'identité et d'atteinte à la réputation des entreprises. La diffusion d'espioniciels, par courrier électronique ou par logiciel, afin de suivre et rapporter le comportement en ligne d'utilisateurs se poursuit. Les espioniciels peuvent également permettre de recueillir des informations personnelles comme les mots de passe et numéros de carte de crédit.

L'envoi massif de messages électroniques non sollicités est grandement facilité par la diffusion de codes malveillants comme les vers et virus. Une fois installés, ils permettent à un agresseur de prendre le contrôle du système informatique infecté et de le transformer en «botnet»<sup>9</sup> en dissimulant l'identité du véritable polluposteur. Les botnets sont loués par les polluposteurs, hameçonneurs et fournisseurs d'espioniciels à des fins frauduleuses et délictueuses. Les experts du secteur estiment que les botnets relayent plus de 50% des messages abusifs<sup>10</sup>. La diffusion d'espioniciels et d'autres types de codes malveillants dont sont victimes particuliers et entreprises a un impact économique considérable. Ainsi l'impact financier global des logiciels malveillants a été estimé à environ 11 milliards d'euros en 2005<sup>11</sup>.

---

<sup>4</sup> On entend par pourriel l'envoi de messages non sollicités par courrier électronique, à des fins commerciales notamment. Toutefois, les messages électroniques non sollicités peuvent aussi contenir des logiciels malveillants et espions.

<sup>5</sup> En 2001, le pourriel représentait 7% du trafic mondial de courrier électronique.

<sup>6</sup> Symantec 54%; Messagelabs 68,6%; MAAWG 80-85%.

<sup>7</sup> Q1 2006 (Sophos) Asie 42,8%, Amérique du Nord 25,6%, Europe 25%, Amérique du Sud 5,1%, Australasie 0,8%, Afrique 0,6%, Autres 0,1%.

<sup>8</sup> Ferris research, 2005.

<sup>9</sup> Les botnets sont des ordinateurs compromis que les polluposteurs utilisent pour envoyer des messages en vrac après installation d'agents logiciels cachés qui transforment les ordinateurs en serveurs de courrier à l'insu de leur utilisateur.

<sup>10</sup> Symantec (Q 3-4 2005) Principaux pays infectés par les botnets: États-Unis 26%, Royaume-Uni 22%, Chine 9%, France, Corée du Sud, Canada 4%, Taïwan, Espagne, Allemagne 3%, Japon 2%.

<sup>11</sup> Computer Economics: the 2005 Malware Report.

### 3. LE TRAVAIL DEJA ACCOMPLI: ACTIONS ENTREPRISES DEPUIS 2004

En 2002, l'UE a adopté une **directive sur la vie privée et les communications électroniques** qui **interdit le pourriel**<sup>12</sup> en instaurant le principe de la prospection basée sur le consentement des personnes physiques. En janvier 2004, la Commission a présenté une communication sur le pourriel qui énumère les actions destinées à compléter la directive<sup>13</sup>. Cette communication soulignait la nécessité de diverses actions en matière de sensibilisation, d'autorégulation, de solutions techniques, de coopération et d'application de la loi. La Commission a commencé à aborder la question de la lutte contre le pourriel, les espioniciels et les logiciels malveillants dans ses discussions avec les pays tiers. En outre, la directive sur les pratiques commerciales déloyales<sup>14</sup> protège les consommateurs contre les pratiques commerciales agressives, la coopération transfrontière pour lutter contre ces pratiques relevant du règlement relatif à la coopération en matière de protection des consommateurs<sup>15</sup>.

#### 3.1. Actions de sensibilisation

La communication de la Commission a contribué à sensibiliser les utilisateurs au problème du pourriel aux niveaux national et international. Au niveau de l'UE, le **programme Safer Internet plus** vise à promouvoir une utilisation plus sûre d'internet et des nouvelles technologies en ligne, notamment par les enfants, dans le cadre d'une approche cohérente de l'Union européenne.

Les États membres ont lancé ou soutenu des **campagnes** de sensibilisation des utilisateurs au problème du pourriel et aux moyens d'y remédier. En général, les FSI se sont chargés de prodiguer à leurs clients conseils et assistance sur la façon de se protéger contre les espioniciels et les virus. La Commission a accueilli un **atelier** de l'OCDE consacré au pourriel en février 2004. Elle a aussi contribué activement à la mise au point de la **Boîte à outils anti-spam** de l'OCDE qui constitue un ensemble complet d'approches réglementaires, de solutions techniques et d'initiatives des entreprises pour lutter contre le pourriel.

Au Sommet mondial sur la société de l'information (SMSI) des Nations unies<sup>16</sup>, il a été **reconnu** que la question du pollupostage devait être traitée aux niveaux national et international appropriés. En 2004 et 2005, des réunions thématiques du SMSI ont été organisées par l'UIT. Enfin, l'agenda de Tunis, adopté lors de la deuxième phase du SMSI en novembre 2005, préconise de «traiter efficacement le problème toujours plus préoccupant du spam»<sup>17</sup>.

#### 3.2. Coopération internationale

Le pourriel étant un problème transfrontière, plusieurs initiatives de coopération et mécanismes d'application transfrontière de la loi ont été mis en place. La Commission a créé un **Réseau de contact des autorités antis spam** (CNSA) qui se réunit régulièrement, échange les meilleures pratiques et coopère en matière d'application transfrontière de la loi. Le CNSA

---

<sup>12</sup> Article 13 de la directive 2002/58/CE.

<sup>13</sup> Supra 3.

<sup>14</sup> Point 26 de l'annexe 1 de la directive 2005/29/CE.

<sup>15</sup> Règlement (CE) n° 2006/2004.

<sup>16</sup> SMSI, Genève, décembre 2003.

<sup>17</sup> Agenda de Tunis, paragraphe 41.

a établi une procédure de coopération<sup>18</sup> visant à faciliter le traitement transfrontière des plaintes relatives au pourriel. Les services de la Commission apportent leur soutien et participent, à titre d'observateurs, au **Plan d'action de Londres (PAL)** qui regroupe les autorités chargées de faire appliquer la loi de vingt pays et a également arrêté une procédure de coopération transfrontière. Un atelier conjoint CNSA UE – PAL s'est tenu en novembre 2005. L'**OCDE** a adopté, en avril 2006, une recommandation relative à la coopération transfrontière dans l'application des législations contre le spam invitant les autorités chargées de faire appliquer la loi à s'échanger leurs informations et à collaborer<sup>19</sup>.

La Commission encourage également les **initiatives de coopération internationale**. Par exemple, les États-Unis et l'Union européenne sont convenus de coopérer pour s'attaquer au problème du pourriel par des initiatives conjointes d'application de la loi, et d'étudier les moyens de lutte contre les logiciels illicites, espions et malveillants. La Commission prend également part au groupe de travail sur le pourriel dans le cadre de la collaboration internationale du Canada. Des discussions sont engagées avec les principaux partenaires internationaux comme la Chine et le Japon. Concernant l'Asie, la Commission a pris l'initiative d'une déclaration conjointe sur la coopération internationale antipourriel qui a été adoptée à la conférence de l'ASEM sur le commerce électronique en février 2005<sup>20</sup>.

L'agenda de Tunis, adopté en novembre 2005 par le Sommet mondial sur la société de l'information, souligne que la sécurité d'internet est un domaine exigeant une meilleure collaboration internationale et que cette question devra être abordée dans le cadre du modèle de coopération accrue pour la gouvernance de l'internet qui sera mis en œuvre au titre du suivi du sommet<sup>21</sup>.

### **3.3. Recherche et développement technologique**

En vertu du 6<sup>e</sup> programme-cadre de RDT, la Commission a lancé des projets afin d'aider les parties intéressées à lutter contre le pourriel et d'autres formes de logiciel malveillant. Ces projets<sup>22</sup> vont du contrôle général de réseau et de la détection des attaques à la mise au point de techniques spécifiques de filtrage pour repérer le pourriel, l'hameçonnage et les logiciels malveillants. Parmi les réalisations, on peut citer la création d'une communauté scientifique spécialisée dans la maîtrise des logiciels malveillants, et la mise au point d'une infrastructure européenne pour contrôler le trafic internet. Les activités récemment entamées portent sur les filtres adaptatifs contre l'hameçonnage qui permettent de détecter les menaces inconnues et les cyberattaques. L'effort financier consacré à ces activités s'élève à 13,5 millions d'euros.

### **3.4. Actions des entreprises**

Le Commission se réjouit du rôle moteur joué par les entreprises en matière de pourriel. Les fournisseurs de services ont, en général, pris des **mesures techniques** pour s'attaquer au pourriel, notamment à l'aide de filtres antipourriel. Les FSI disposent d'un **service de support technique** et fournissent aux utilisateurs des logiciels contre le pourriel, les

---

18

[http://europa.eu.int/information\\_society/policy/ecommerce/doc/todays\\_framework/privacy\\_protection/spam/cooperation\\_procedure\\_cnsa\\_final\\_version\\_20041201.pdf](http://europa.eu.int/information_society/policy/ecommerce/doc/todays_framework/privacy_protection/spam/cooperation_procedure_cnsa_final_version_20041201.pdf)

19

<http://www.oecd-antispam.org/>

20

<http://www.asemec-london.org/>

21

Agenda de Tunis, paragraphes 39-47. <http://www.itu.int/wsis/docs2/tunis/off/6rev1-fr.doc>

22

<http://www.diademhttp://cordis.europa.eu/fp6/projects.htm#search>

espiogiciels et logiciels malveillants. Nombre de ces FSI ont prévu des **clauses contractuelles** qui interdisent les malversations en ligne. Récemment, un tribunal britannique a ainsi infligé une amende de 68 800 euros à un polluposteur pour rupture de contrat. Les associations professionnelles ont adopté de bonnes pratiques afin de prévenir l'hameçonnage en ligne et d'améliorer les méthodes de filtrage<sup>23</sup>.

Les opérateurs de téléphonie mobile ont également agi et les codes de conduite professionnels prévoient d'entamer une action contre les messages non sollicités. L'association GSM a publié, en 2006, un code de bonnes pratiques concernant le pourriel mobile. Actuellement, la Commission cofinance l'initiative Spotsam, partenariat entre organismes privés et publics qui vise à construire une base de données facilitant les enquêtes et l'application transfrontière de la loi en cas de pourriel<sup>24</sup>.

### 3.5. Actions pour faire appliquer la loi

Il est clair qu'engager la lutte contre le pourriel donne des résultats. Les mesures de filtrage imposées en Finlande ont permis de réduire la proportion de pourriel dans les messages électroniques de 80% à environ 30%. Un grand nombre d'autorités chargées de faire appliquer la loi ont déployé des efforts pour mettre un frein au pollupostage<sup>25</sup>.

Il existe toutefois de grandes différences entre les États membres quant au nombre réel de poursuites. Certaines autorités ont ouvert au moins une centaine d'enquêtes qui ont été menées à bien et conduit à sanctionner des activités de pollupostage. Dans d'autres États membres, le nombre d'affaires instruites n'a pas dépassé cinq, voire parfois zéro.

La plupart des actions visaient des **formes «traditionnelles»** de pourriel. **Les autres menaces signalées ont rarement donné lieu à des poursuites** même si elles font courir de grands risques.

## 4. LA VOIE A SUIVRE: TRAVAIL RESTANT A ACCOMPLIR

### 4.1. Actions au niveau des États membres

Cette partie couvre les actions incombant aux pouvoirs publics et autorités nationales, notamment en ce qui concerne l'application de la loi et la coopération.

#### 4.1.1. Facteurs clés du succès

La persistance et le caractère changeant du problème exigent des États membres qu'ils s'impliquent davantage et fixent des priorités. Les actions doivent viser en particulier les polluposteurs «professionnels», les hameçonneurs et la diffusion d'espiogiciels et de logiciels malveillants. À cet égard, les facteurs clés du succès sont les suivants:

- un engagement résolu de l'administration centrale à lutter contre les malversations en ligne;

---

<sup>23</sup> <http://www.maawg.org/home/>

<sup>24</sup> <http://www.spotspam.net>

<sup>25</sup> Une enquête du CNSA a révélé que quinze des dix-huit membres y ayant répondu avaient engagé des poursuites sur la période 2003-2006.

- une responsabilité organisationnelle claire concernant l’application de la loi;
- des moyens appropriés pour les autorités chargées de faire appliquer la loi.

Actuellement, ces facteurs n’existent pas dans tous les États membres.

#### 4.1.2. *Coordination et intégration au niveau national*

En vertu de la directive Vie privée et communications électroniques et de la directive générale sur la protection des données<sup>26</sup>, les autorités nationales ont le pouvoir d’agir contre les pratiques illicites suivantes:

- envoyer des communications non sollicitées (**spam**)<sup>27</sup>;
- accéder illégalement à un équipement terminal pour y stocker des informations, comme des **logiciels publicitaires** ou **espions**, ou consulter des informations qui y sont stockées<sup>28</sup>;
- infecter un équipement terminal en y introduisant des **logiciels malveillants** tels que vers et virus et transformer des ordinateurs en **botnets** ou les utiliser à d’autres fins<sup>29</sup>;
- tromper les utilisateurs afin qu’ils révèlent des informations confidentielles<sup>30</sup>, telles que mots de passe et numéros de carte de crédit, par des messages dits d’**hameçonnage**.

Certaines de ces pratiques peuvent aussi relever du droit pénal, y compris de la décision-cadre relative aux attaques visant les systèmes d’information<sup>31</sup>. Conformément à cette dernière décision, les États membres doivent prévoir une peine d’emprisonnement d’au moins trois ans, ou de cinq ans si l’infraction a été commise dans le cadre d’une organisation criminelle.

Au niveau national, ces dispositions peuvent être appliquées par des juridictions administratives et/ou pénales. Le cas échéant, les **responsabilités** des différentes autorités et les procédures de coopération doivent être clairement définies. Cela peut exiger que des décisions soient prises à haut niveau par les autorités nationales.

**Jusqu’à maintenant, l’imbrication accrue des aspects pénaux et administratifs du pourriel et des autres menaces ne s’est pas traduite, dans les États membres, par une multiplication des procédures de coopération permettant de conjuguer les compétences techniques et d’investigation des différents organismes.** Il est donc nécessaire d’établir des protocoles de coopération en matière d’échange d’informations et de renseignements, de coordonnées, d’assistance et de transfert des dossiers.

Une étroite coopération entre les autorités chargées de faire appliquer la loi, les opérateurs de réseau et les FSI au niveau national est également favorable à l’échange d’informations et d’expertise technique et aux poursuites contre les malversations en ligne. Les autorités

---

<sup>26</sup> Directive 95/46/CE.

<sup>27</sup> Article 13 de la directive 2002/58/CE.

<sup>28</sup> Article 5, paragraphe 3, de la directive 2002/58/CE.

<sup>29</sup> Supra 28.

<sup>30</sup> Article 6, point a), de la directive 95/46/CE.

<sup>31</sup> Décision-cadre du Conseil 2005/222/JHA.

norvégiennes et néerlandaises ont apporté la preuve de l'utilité de tels partenariats public-privé.

#### 4.1.3. *Ressources*

Il est nécessaire de disposer de ressources pour rassembler les preuves, procéder aux enquêtes et engager les poursuites. Les autorités ont besoin de moyens techniques et juridiques et doivent se familiariser avec le mode opératoire des contrevenants pour mener leurs actions à bien.

À cet égard, les mécanismes de plainte en ligne associés à des systèmes permettant de consigner et d'analyser les malversations signalées peuvent constituer un outil précieux. L'expérience a montré que des **investissements modérés** pouvaient donner des **résultats significatifs**. L'autorité néerlandaise (OPTA) est ainsi parvenue à réduire le pourriel néerlandais en créant une équipe spécialisée de cinq personnes à plein temps et en lui fournissant pour **570 000 euros** de dispositifs de lutte antipourriel. Grâce à cet investissement, l'expérience acquise dans la lutte antipourriel est désormais mise à profit pour traiter d'autres aspects du problème.

#### 4.1.4. *Coopération transfrontière*

Le pourriel est un problème mondial. Il arrivera souvent qu'une autorité nationale doive s'en remettre à des autorités étrangères pour poursuivre des polluposteurs et, à l'inverse, qu'elle soit priée de conduire des enquêtes ouvertes dans d'autres pays.

Même s'il peut y avoir une certaine réticence à consacrer des ressources nationales limitées aux problèmes d'autrui, il est important que les États membres comprennent qu'une coopération transfrontière effective est un élément essentiel de la lutte antipourriel. Récemment, les autorités antipourriel australiennes et néerlandaises ont œuvré de concert pour faire échouer une opération de pollupostage de grande envergure.

Aujourd'hui, vingt-et-une autorités européennes ont approuvé la procédure de coopération du CNSA<sup>32</sup> sur le traitement transfrontière des plaintes, et les autres autorités sont invitées à en faire de même au cours des prochains mois. Les États membres et autorités compétentes sont notamment invitées à promouvoir activement le recours:

- aux documents pro forma de l'atelier conjoint CNSA-PAL;
- la recommandation et la boîte à outils de l'OCDE sur l'application des législations contre le spam.

---

<sup>32</sup> Supra 18.

#### 4.1.5. *Actions proposées*

Les États membres et autorités compétentes sont priées:

- de délimiter clairement les responsabilités des organismes nationaux concernés par la lutte antipourriel;
- d'assurer une coordination effective entre les autorités compétentes;
- d'impliquer les acteurs économiques au niveau national en tirant parti de leur expertise et des informations à leur disposition;
- de faire en sorte que les ressources nécessaires soient consacrées à l'application de la loi;
- d'adopter les procédures de coopération internationale et de répondre aux demandes d'assistance transfrontière.

## 4.2. **Actions des entreprises**

Cette partie couvre les mesures que les entreprises peuvent prendre pour susciter la confiance des consommateurs et limiter l'envoi de messages abusifs.

### 4.2.1. *Fourniture et installation de logiciels*

Les logiciels espions représentent une menace sérieuse pour la vie privée des utilisateurs. Les offres de logiciel en ligne constituent désormais une méthode très employée de **fourniture et d'installation d'espions** sur l'équipement terminal de l'utilisateur. Les logiciels espions peuvent également se cacher dans les logiciels distribués par d'autres moyens, comme les téléchargements d'installation. Aussi des programmes non sollicités peuvent-ils s'installer, en même temps que le logiciel acheté par le consommateur, sur l'ordinateur de ce dernier.

Pour éviter que les logiciels espions n'atteignent l'utilisateur final, des actions spécifiques sont énumérées ci-après.

### 4.2.2. *Information du consommateur*

Les offres logicielles peuvent comprendre l'installation de programmes supplémentaires. Lorsque ces logiciels supplémentaires fonctionnent comme des logiciels espions en surveillant le comportement des utilisateurs (à des fins de prospection, par exemple), cela implique le traitement de données à caractère personnel, pratique illicite sans le consentement éclairé de l'utilisateur. Bien souvent, le consentement de l'utilisateur concernant l'installation de tels logiciels n'est pas obtenu ou alors se cache dans les petits caractères d'une interminable licence d'utilisation.

Les sociétés qui proposent des produits logiciels sont donc encouragées à exposer clairement tous les termes du contrat et conditions de l'offre, en particulier s'il y a traitement de données à caractère personnel par un quelconque dispositif de surveillance intégré aux logiciels.

L'autorégulation et le recours à une sorte de label de qualité pourraient fournir un moyen de distinguer les sociétés fiables des autres. Les codes de conduite qui visent à informer

l'utilisateur des conditions impliquant le traitement de données à caractère personnel peuvent être soumis à l'approbation du Groupe de travail «article 29» sur la protection des données.

#### 4.2.3. *Clauses contractuelles dans la chaîne logistique*

Souvent, les sociétés **ignorent** comment les annonces publicitaires concernant leurs produits et services sont techniquement présentées au public. Des logiciels licites peuvent donc être conditionnés avec des logiciels destinés à accéder à des données sensibles telles que numéros de carte de crédit, documents confidentiels, etc.

Les sociétés qui vendent des produits ou en font la publicité doivent s'assurer que les activités de leurs partenaires commerciaux sont légales. Elles doivent comprendre comment fonctionne la chaîne de relations contractuelles, vérifier le respect de la législation et faire des malversations un motif de rupture de contrat d'un bout à l'autre de la chaîne afin de pouvoir mettre immédiatement terme à toute autre affiliation avec des entreprises convaincues de malversation.

#### 4.2.4. *Mesures de sécurité à la charge des fournisseurs de services*

Une **enquête de l'ENISA de 2006**<sup>33</sup> confirme que les fournisseurs de services ont, en général, pris des mesures pour s'attaquer au pourriel. Elle indique toutefois que lesdits fournisseurs pourraient contribuer encore à la sécurité globale du réseau et recommande de mettre davantage l'accent sur le filtrage du courrier électronique quittant le réseau d'un fournisseur de services (**filtrage à la sortie**). La Commission encourage les fournisseurs de services à mettre en œuvre cette recommandation.

Le Groupe de travail «article 29» sur la protection des données a émis un avis sur les problèmes de protection de la vie privée liés à la fourniture de services de filtrage du courrier électronique<sup>34</sup>, qui donne des orientations concernant la question de la confidentialité des communications électroniques et, plus précisément, le filtrage des communications en ligne contre les virus, le pourriel et le contenu illicite.

#### 4.2.5. *Actions proposées*

La Commission invite:

- les sociétés à s'assurer que le critère applicable aux informations fournies à l'achat d'applications logicielles est conforme à la législation sur la protection des données;
- les sociétés à interdire contractuellement l'utilisation illicite de logiciels dans les publicités, contrôler comment les annonces publicitaires parviennent aux consommateurs et donner suite aux malversations;
- les fournisseurs de services de courrier électronique à appliquer une politique de filtrage qui garantisse la conformité avec les recommandations et orientations en la matière.

<sup>33</sup> [http://www.enisa.eu.int/doc/pdf/deliverables/enisa\\_security\\_spam.pdf](http://www.enisa.eu.int/doc/pdf/deliverables/enisa_security_spam.pdf)

<sup>34</sup> Avis 2/2006, GT 118.

### 4.3. Action au niveau européen

La Commission continuera à aborder les problèmes relatifs au pourriel, aux espioniciels et aux logiciels malveillants dans les enceintes internationales, dans les réunions bilatérales et, le cas échéant, par des accords avec les pays tiers, et continuera à promouvoir la coopération entre parties intéressées, notamment les États membres, autorités compétentes et entreprises. En matière de législation et de recherche, elle prendra aussi de nouvelles initiatives visant à relancer la lutte contre les malversations qui sapent la société de l'information. La Commission poursuit actuellement l'élaboration d'une politique cohérente concernant la lutte contre la cybercriminalité. Cette politique sera présentée dans une communication dont l'adoption est prévue pour le début de 2007.

#### 4.3.1. Réexamen du cadre réglementaire

La communication de la Commission<sup>35</sup> sur le cadre réglementaire applicable aux communications électroniques propose de renforcer les règles en matière de protection de la vie privée et de sécurité. En vertu de cette proposition, les opérateurs de réseau et fournisseurs de services seraient tenus:

- de notifier à l'autorité compétente d'un État membre tout manquement à la sécurité ayant entraîné la perte de données à caractère personnel et/ou des interruptions de service;
- de notifier à leurs clients tout manquement à la sécurité entraînant la perte, la modification, la révélation ou la destruction de données à caractère personnel les concernant.

Les autorités réglementaires nationales auraient la responsabilité de faire en sorte que les opérateurs appliquent les politiques de sécurité adaptées, et de nouvelles règles pourraient être établies concernant des **solutions spécifiques** ou le **niveau de sanctions** à prévoir pour les infractions.

#### 4.3.2. Rôle de l'ENISA (Agence européenne chargée de la sécurité des réseaux et de l'information)

Dans les propositions, figure aussi une disposition reconnaissant le rôle consultatif de l'ENISA en matière de sécurité. Les autres tâches prévues pour l'ENISA sont exposées dans la communication de la Commission relative à une stratégie pour une société de l'information sûre<sup>36</sup> et consistent notamment à:

- développer un partenariat de confiance avec les États membres et les parties prenantes en vue d'élaborer un **cadre approprié pour la collecte de données** concernant les incidents de sécurité et le niveau de confiance des consommateurs. À propos de ce cadre, l'ENISA collaborera étroitement avec Eurostat dans l'optique des statistiques communautaires concernant la société de l'information et le cadre d'évaluation comparative i2010<sup>37</sup>;
- examiner la **faisabilité d'un système européen de partage d'informations et d'alerte** permettant de répondre efficacement aux menaces existantes et émergentes pour les réseaux électroniques.

---

<sup>35</sup> [http://europa.eu.int/information\\_society/policy/ecommm/tomorrow/index\\_en.htm](http://europa.eu.int/information_society/policy/ecommm/tomorrow/index_en.htm)

<sup>36</sup> Supra I.

<sup>37</sup> Cadre d'évaluation comparative du groupe à haut niveau i2010 du 20 avril 2006.

#### 4.3.3. Recherche et développement

Le prochain 7<sup>e</sup> programme-cadre vise à poursuivre le développement de connaissances et de technologies pour sécuriser les services et systèmes d'information en étroite coordination avec les initiatives politiques. Les thèmes en rapport avec les logiciels malveillants devraient couvrir les botnets et virus cachés ainsi que les attaques contre les services mobiles et vocaux.

#### 4.3.4. Coopération internationale

Comme internet est un réseau mondial, l'engagement à lutter contre le pourriel, les espioniciels et les logiciels malveillants doit être pris par tous à travers le monde. Aussi la Commission entend-elle développer le dialogue et la coopération avec les pays tiers concernant la lutte contre ces menaces et les activités criminelles qui y sont associées. À cet effet, la Commission veillera à faire en sorte que la question du pourriel, des espioniciels et des logiciels malveillants soit abordée dans les accords entre l'UE et les pays tiers, à obtenir un engagement ferme des pays tiers les plus concernés à collaborer avec les États membres de l'UE pour lutter plus efficacement contre ces menaces, et à vérifier de près le respect des engagements communs.

#### 4.3.5. Actions proposées

La Commission:

- poursuivra son effort de sensibilisation et de promotion de la coopération entre parties intéressées;
- continuera à établir des accords avec les pays tiers abordant la question de la lutte contre le pourriel, les espioniciels et les logiciels malveillants;
- visera à soumettre, au début de 2007, de nouvelles propositions législatives renforçant les règles en matière de protection de la vie privée et de sécurité dans le secteur des communications, et une politique relative à la cybercriminalité;
- fera appel à l'expertise de l'ENISA en matière de sécurité;
- soutiendra la recherche et développement au titre de son 7<sup>e</sup> programme-cadre.

## 5. CONCLUSION

Les menaces que représentent le pourriel, les espioniciels et les logiciels malveillants entament la confiance du public dans la société de l'information, nuisent à la sécurité de celle-ci et ont un impact financier important. Malgré les initiatives de certains États membres, **les actions entreprises** au sein de l'UE dans son ensemble **sont insuffisantes pour faire face à cette évolution**. La Commission joue son rôle de médiateur afin de mieux faire comprendre qu'un engagement politique plus résolu est nécessaire pour faire face à ces menaces.

**Il faut intensifier les efforts pour faire appliquer la loi afin d'arrêter ceux qui l'enfreignent sciemment. Pour compléter les activités visant au respect de la loi, d'autres actions doivent être menées par les entreprises. Une coopération s'impose au niveau national, tant au sein de l'administration qu'entre l'administration et les entreprises. La Commission développera le dialogue et la coopération avec les pays tiers et étudiera**

**aussi la possibilité de soumettre de nouvelles propositions législatives, de même qu'elle entreprendra des actions de recherche pour renforcer encore la protection de la vie privée et la sécurité dans le secteur des communications électroniques.**

Une mise en œuvre intégrée et, si possible, en parallèle des actions énumérées dans la présente communication peut contribuer à limiter les menaces qui, actuellement, portent préjudice à la société et à l'économie de l'information.

La Commission supervisera la mise en œuvre de ces actions et, d'ici à 2008, déterminera si des actions supplémentaires sont nécessaires.