COMMISSION DES COMMUNAUTÉS EUROPÉENNES

Bruxelles, le 26.1.2001
COM(2000) 890 final

COMMUNICATION DE LA COMMISSION AU CONSEIL, AU PARLEMENT EUROPEEN, AU COMITE ECONOMIQUE ET SOCIAL ET AU COMITE DES REGIONS

Créer une société de l'information plus sûre en renforçant la sécurité des infrastructures de l'information et en luttant contre la cybercriminalité

Sommaire

La transition de l'Europe vers la société de l'information est marquée par de profonds changements qui affectent tous les aspects de l'activité humaine: travail, éducation, loisirs, administration, industrie et commerce. Les nouvelles technologies de l'information et de la communication bouleversent et transforment profondément nos économies et nos sociétés. Le succès de la société de l'information, dont les répercussions économiques, sociales et juridiques sont considérables, est important pour la croissance, la compétitivité et la création d'emplois en Europe.

La Commission a lancé l'initiative eEurope en décembre 1999 pour permettre à l'Europe de tirer parti des avantages des technologies numériques et faire en sorte que la société de l'information naissante soit un facteur d'intégration sociale. En juin 2000, le Conseil européen de Feira a approuvé un plan global d'action sur l'initiative eEurope et a demandé sa mise en œuvre avant la fin 2002. Ce plan d'action souligne l'importance que revêtent la sécurité des réseaux et la lutte contre la cybercriminalité.

Les infrastructures de l'information et de la communication sont devenues une composante essentielle de nos économies, qui, malheureusement, n'est pas sans faiblesses et ouvre la voie aux comportements criminels . Ces activités criminelles peuvent prendre des formes très variées et franchir nombre de frontières. Bien qu'il n'existe, pour certaines raisons, aucune donnée statistique fiable, il ne fait aucun doute que ces infractions constituent une menace pour les investissements et les actifs des entreprises, ainsi que pour la sécurité et la confiance dans la société de l'information. On rapporte que certains exemples récents de refus de service et d'attaques de virus auraient causé d'importants préjudices financiers.

Plusieurs actions sont envisageables, tant par la prévention des activités criminelles en renforçant la sécurité des infrastructures de l'information qu'en dotant de moyens d'action appropriés les autorités chargées de l’application des lois, tout en respectant intégralement les droits fondamentaux de la personne.

L'Union européenne a déjà adopté un certain nombre de mesures pour lutter contre les contenus illicites et préjudiciables sur l'Internet, pour protéger les droits de propriété intellectuelle et les données à caractère personnel, pour promouvoir le commerce électronique et l'utilisation des signatures électroniques, et pour renforcer la sécurité des transactions. En avril 1998, la Commission a exposé devant le Conseil les résultats d'une étude (intitulée COMCRIME) sur la cybercriminalité. En octobre 1999, le Conseil européen de Tampere a conclu que les efforts visant à trouver un accord sur des définitions et des sanctions communes doivent aussi porter sur la criminalité utilisant les technologies avancées. Le Parlement européen a également invité à la mise au point de définitions de la criminalité informatique acceptables par tous et à un rapprochement efficace des législations, en particulier en matière de droit pénal positif. Le Conseil de l'Union européenne a adopté une position commune concernant les négociations relatives au projet de convention sur la criminalité informatique qui sont menées au sein du Conseil de l'Europe et a pris un certain nombre de mesures initiales dans le cadre de la stratégie de lutte de l'Union contre la criminalité utilisant de haute technologie. Certains États membres de l'Union européenne ont également exercé une action de premier plan dans les travaux du G8 en la matière.

La présente communication s'interroge sur la nécessité d'une initiative en vue de définir une politique globale et étudie les différentes formes qu'elle pourrait prendre, dans le contexte des objectifs plus larges que constituent la *société de l'information* et la *création d'un espace de liberté, de sécurité et de justice*, en vue d'améliorer la sécurité des infrastructures de

l'information et de lutter contre la criminalitécriminalité informatique, dans le respect des droits fondamentaux de la personne, conformément à l'engagement pris par l'Union européenne.

La Commission estime qu'à court terme, un instrument communautaire est indispensable pour permettre aux États membres de disposer de sanctions efficaces en vue de combattre la pornographie enfantine sur l'Internet. Elle présentera avant la fin de cette année une proposition de décision-cadre qui s'inscrira dans le contexte plus large des problèmes liés à l'exploitation sexuelle des enfants et à la traite des êtres humains, et comprendra des dispositions en vue d'un rapprochement des législations et des sanctions.

À terme, la Commission présentera des propositions législatives visant à rapprocher davantage les systèmes de droit pénal positif dans le domaine de la criminalité de haute technologie. Conformément aux conclusions du Conseil européen de Tampere d'octobre 1999, la Commission envisagera aussi les mesures possibles pour appliquer le principe de reconnaissance mutuelle aux injonctions préalables au procès dans le cadre d'enquêtes sur la cybercriminalité.

Parallèlement, la Commission entend promouvoir, au niveau national, la création d'unités de police spécialisées dans la lutte contre la criminalité informatique, là où elles n'existent pas encore, soutenir des actions de formation technique appropriées pour les agents de la force publique et encourager les actions européennes en matière de sécurité de l'information.

Sous l'angle technique et conformément au cadre juridique, la Commission favorisera les efforts de recherche et développement visant à comprendre et à corriger les faiblesses et incitera à la diffusion du savoir-faire.

Elle a également l'intention de créer un forum européen qui rassemblerait les autorités chargées de l'application des lois, les fournisseurs de services Internet, les entreprises de télécommunications, les organisations de défense des libertés publiques, les représentants des consommateurs, les autorités chargées de la protection des données et les autres parties intéressées, et qui aurait pour objectif d'améliorer la compréhension mutuelle et la coopération au niveau de l'Union européenne. Ce forum s'efforcera de sensibiliser le public aux risques liés à la criminalité sur l'Internet, de promouvoir les meilleures pratiques en matière de sécurité, de définir des outils et des procédures efficaces afin de lutter contre la criminalité informatique, ainsi que d'encourager les avancées en matière de mécanismes d'alerte rapide et de gestion des crises.

INVITATION À PRÉSENTER DES OBSERVATIONS SUR LA PRÉSENTE COMMUNICATION

La Commission européenne souhaite inviter toutes les parties intéressées à présenter des observations sur les points traités dans la présente communication. Les observations peuvent être envoyées jusqu'au 23 mars 2001 par courrier électronique à l'adresse suivante:

infso-jai-cybercrime-comments@cec.eu.int

Les observations seront en principe publiées sur l'Internet, sauf refus exprès des parties qui auront transmis ces observations. Les observations anonymes ne seront pas publiées. La Commission se réserve le droit de ne pas publier certaines observations (par exemple, si celles-ci contiennent des termes injurieux). Les observations pourront être consultées via un lien créé sur le site web suivant:

http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/crime1.html

Des suggestions technologies quant au format à utiliser, ainsi que les modalités de publication pourront être consultées sur ce même site. Il est conseillé de visiter ce site avant d'envoyer ses observations.

AUDITION PUBLIQUE

La Commission européenne organisera également une audition publique des parties intéressées sur les points traités dans la présente communication. Cette audition se tiendra le 7 mars 2001. Les demandes d'invitation à présenter des observations lors de cette audition peuvent être envoyées jusqu'au 20 février 2001 par courrier électronique à l'adresse suivante:

infso-jai-cybercrime-hearing@cec.eu.int

ou par la poste à l'adresse suivante:

Commission européenne
Bureau BU33-5/9
200 Rue de la Loi
B-1049 Bruxelles
Belgique

La Commission européenne se réserve le droit d'opérer une sélection des parties qui seront entendues. Cette éventuelle sélection dépendra du nombre de demandes reçues et sera motivée par le souhait d'entendre un large éventail des milieux intéressés.

TABLE DES MATIÈRES

Sommaire

1. OPPORTUNITES ET RISQUES DANS LA SOCIETE DE L'INFORMATION

L'accessibilité et l'utilisation croissantes des technologies de la société de l'information (TSI) ainsi que la mondialisation de l'économie sont caractéristiques de l'époque que nous vivons. Les progrès technologiques à venir et l'utilisation grandissante des réseaux ouverts, comme l'Internet, au cours des prochaines années créeront de nouvelles opportunités mais exposeront aussi à de nouveaux défis.

Le Conseil européen de Lisbonne, en mars 2000, a souligné toute l'importance que revêt la transition vers une économie compétitive, dynamique et fondée sur la connaissance, et a invité le Conseil et la Commission à établir un plan global d'action *e*Europe pour en tirer le meilleur parti[1]. Ce plan d'action, élaboré par la Commission et le Conseil et approuvé par le Conseil européen de Feira en juin 2000, comprend des actions visant à renforcer la sécurité des réseaux et prévoit le développement d'une approche coordonnée et cohérente de la criminalité informatique pour la fin 2002[2].

Les infrastructures de l'information sont devenues un maillon essentiel de nos économies. Les utilisateurs doivent pouvoir compter sur la disponibilité des services de l'information et être convaincus que leurs communications et leurs données sont préservées de tout accès et de toute modification non autorisés. La généralisation du commerce électronique et la réalisation intégrale de la société de l'information en dépendent.

Les nouvelles technologies numériques et sans fil sont déjà omniprésentes. Elles nous offrent la mobilité, tout en conservant une connexion à une myriade de services accessibles via des réseaux de réseaux. Elles nous donnent aussi la possibilité de participer, d'enseigner et d'apprendre, de jouer et de travailler ensemble, de prendre part à la vie politique. Toutefois, à mesure que les sociétés deviendront plus dépendantes de ces technologies, il leur faudra employer des moyens pratiques et juridiques efficaces pour pouvoir gérer les risques associés à cette évolution.

Les technologies de la société de l'information peuvent être utilisées, et le sont effectivement, pour perpétrer et faciliter diverses activités criminelles. Aux mains de personnes agissant de mauvaise foi, par malveillance ou par grave négligence, ces technologies peuvent servir d'instruments à des activités qui mettent en péril ou lèsent la vie, les biens ou la dignité des personnes, ou portent préjudice à l'intérêt général.

L'approche classique en matière de sécurité exigeait une stricte compartimentation, sous l'angle organisationnel, géographique et structurel, des informations en fonction de leur sensibilité et de leur catégorie. À l'ère numérique, cette approche est dépassée, puisque le traitement de l'information est réparti, que les services suivent des utilisateurs mobiles et que l'interopérabilité des systèmes est une condition indispensable. Des solutions innovantes, fondées sur les technologies naissantes, se substituent aux approches classiques des questions de sécurité. Elles comprennent l'utilisation de techniques de cryptage et de signatures numériques, de nouveaux outils de contrôle d'accès et d'authentification, ainsi que toutes sortes de filtres logiciels[3]. Pour sécuriser et fiabiliser les infrastructures de l'information, il

---

1 Conclusions de la présidence, Conseil européen de Lisbonne des 23 et 24 mars 2000, disponibles sur le site : http://ue.eu.int/fr/Info/eurocouncil/index.htm.

2 http://europa.eu.int/comm/information_society/eeurope/actionplan/index_fr.htm.

3 Les flux de l'information sont filtrés et contrôlés à tous les niveaux, depuis le pare-feu qui examine les paquets de données, en passant par le filtre qui recherche les éventuels logiciels malveillants, le filtre du

faut non seulement disposer de tout un éventail de technologies, mais aussi les déployer correctement et les utiliser efficacement. Certaines de ces technologies sont déjà disponibles, mais les utilisateurs ignorent souvent qu'elles existent, ne savent pas comment s'en servir ou ne connaissent pas les raisons pour lesquelles elles peuvent être nécessaires.

1.1. Réponses nationales et internationales

La criminalité informatique affecte le cyberespace tout entier, sans s'arrêter aux frontières traditionnelles des États. Ces infractions peuvent, en principe, être commises à partir de n'importe où et à l'encontre de n'importe quel utilisateur d'ordinateur, où qu'il se trouve. On s'accorde généralement à reconnaître qu'une action efficace pour lutter contre la criminalité informatiques'impose, tant au niveau national qu'à l'échelle internationale[4].

Au niveau national, il existe peu de réponses adéquates et qui tiennent compte de la dimension internationale pour pouvoir relever les nouveaux défis que constituent la sécurité des réseaux et la criminalité informatique. Dans la plupart des pays, les réactions à ce type de criminalité sont axées sur le droit national (en particulier le droit pénal) et négligent les autres mesures préventives.

En dépit des efforts d'organisations internationales et supranationales, les législations nationales continuent à souffrir de notables disparités, en particulier en ce qui concerne les dispositions de droit pénal sur le piratage informatique, la protection des secrets d'affaires et les contenus illicites. Il existe aussi d'importantes disparités quant aux pouvoirs de coercition des commissions nationales d'enquête (notamment en matière de données codées et d'enquêtes sur les réseaux internationaux), à l'étendue des compétences en matière pénale, ainsi qu'à la responsabilité des fournisseurs de services intermédiaires, d'une part, et des fournisseurs de contenu, d'autre part. La directive 2000/31/CE[5] sur le commerce électronique modifie cette situation en ce qui concerne la responsabilité des prestataires de services intermédiaires à l'égard de certaines activités d'intermédiaire. Cette directive interdit en outre aux États membres d'imposer à ces prestataires de services intermédiaires comme obligation générale de surveiller les informations qu'ils transmettent ou qu'ils stockent.

Au niveau international et supranational, la nécessité de lutter efficacement contre la criminalité informatique a été largement reconnue, et diverses organisations coordonnent ou essaient d'harmoniser les activités en la matière. Les ministres de la justice et de l'intérieur du G8 ont adopté un ensemble de principes et un plan d'action en dix points en décembre 1997, qui ont été approuvés par le sommet du G8 de Birmingham en mai 1998 et qui sont

---

courrier électronique qui élimine discrètement l'arrosage (courriers électroniques non sollicités ou spamming), jusqu'au filtre du navigateur qui empêche tout accès à des contenus préjudiciables.

4 Voir, par exemple, le plan global d'action sur l'initiative eEurope à l'adresse suivante: http://europa.eu.int/comm/information_society/eeurope/actionplan/index_fr.htm, ainsi que les déclarations d'António Vitorino, membre de la Commission, à l'adresse http://europa.eu.int/comm/commissioners/vitorino/speeches/2000/septembre/2000-19-09-en_brussels.pdf, et celles du premier ministre français, Lionel Jospin, à l'adresse http://www.france.diplomatie.fr/actual/evenements/cybercrim/jospin.html.

5 Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur ("directive sur le commerce électronique").

actuellement au stade de la mise en œuvre[6]. Le Conseil de l'Europe a commencé en février 1997 à élaborer une convention internationale sur la criminalité informatique et devrait avoir achevé ses travaux en 2001[7]. La lutte contre la criminalité informatique est aussi à l'ordre du jour de discussions bilatérales que la Commission européenne organise avec certains gouvernements (de pays tiers). C'est ainsi qu'a été mise en place une task force conjointe Communauté européenne/États-Unis sur la protection des infrastructures critiques (Joint EC/US Task Force on Critical Infrastructure Protection)[8].

Les Nations unies et l'OCDE ont également entrepris des actions dans ce domaine, qui fait aussi l'objet de discussions dans des forums internationaux tels que Global Business Dialogue et Trans-Atlantic Business Dialogue[9].

Au niveau de l'Union européenne, les mesures d'ordre législatif adoptées jusqu'à une date récente portaient surtout sur des aspects tels que le droit d'auteur, la protection des droits fondamentaux que constituent le respect de la vie privée et la protection des données, les services d'accès conditionnel ou à accès conditionnel, le commerce électronique, les signatures électroniques et, en particulier, la libéralisation du commerce des systèmes de codage, qui ont un lien indirect avec la criminalité informatique.

Un certain nombre de mesures importantes ne relevant pas du domaine législatif ont également été prises au cours des trois ou quatre dernières années. Il s'agit notamment du plan d'action contre les contenus illicites et préjudiciables sur l'Internet, qui cofinance des actions de sensibilisation, des expériences de filtrage et de classement du contenu, ainsi que des lignes directes ("hot-lines"), de même que des initiatives concernant la protection des mineurs et de la dignité humaine dans la société de l'information, la pornographie enfantine et l'interception des communications par les autorités chargées de l'application des lois[10].

---

6 Le Conseil JAI du 19 mars 1998 a fait siens les dix principes du G8 relatifs à la criminalité liée à la haute technologie et a invité les États membres de l'Union européenne qui ne sont pas membres du G8 à prendre des dispositions pour adhérer à ce réseau. Disponibles sur le site Internet du réseau judiciaire européen http://ue.eu.int/ejn/index.htm.

7 Le projet de convention est accessible sur la toile en deux langues: pour la version française, à l'adresse: http://conventions.coe.int/treaty/fr/projets/cybercrime.htm, et pour la version anglaise, à l'adresse: http://conventions.coe.int/treaty/en/projets/cybercrime.htm.

8 Sous l'égide du groupe consultatif conjoint institué en vertu de l'Accord de coopération scientifique et technologique entre la Communauté européenne et le gouvernement des États-Unis d'Amérique.

9 Les Nations unies ont produit un manuel détaillé intitulé "Manual on the prevention and control of computer-related crime," qui a été récemment mis à jour. En 1983, l'OCDE a réalisé une étude sur les possibilités d'une application et d'une harmonisation internationales des législations pénales afin de résoudre le problème de la criminalité informatique ou des abus informatiques. En 1986, elle a publié un rapport intitulé "Computer-Related Crime: Analysis of Legal Policy", passant en revue les législations existantes et les propositions de réforme dans certains États membres et recommandant une liste minimum des abus que les pays devaient envisager d'interdire et de sanctionner dans leur droit pénal. Enfin, en 1992, l'OCDE a mis au point un ensemble de Lignes directrices régissant la sécurité des systèmes de l'information, destinées à servir de base à l'établissement, par les États et le secteur privé, d'un cadre pour la sécurité des systèmes de l'information.

10 Recommandation 98/560/CE du Conseil du 24 septembre 1998 concernant le développement de la compétitivité de l'industrie européenne des services audiovisuels et de l'information par la promotion de cadres nationaux visant à assurer un niveau comparable et efficace de protection des mineurs et de la dignité humaine;Livre vert sur la protection des mineurs et de la dignité humaine dans les services audiovisuels et de l'information, COM(96) 483, octobre 1996, http://europa.eu.int/en/record/green/gp9610/protec.htm;
Communication de la Commission au Conseil, au Parlement européen, au Comité économique et social et au Comité des régions - Contenu illégal et préjudiciable sur le réseau Internet (COM(96) 487 final);
Résolution sur la communication de la Commission relative au contenu illégal et préjudiciable sur Internet (COM(96) 487 C4-0592/96);

L'Union européenne soutient de longue date les projets de recherche et développement qui visent à promouvoir la sécurité et la confiance dans les infrastructures de l'information et les transactions électroniques, et les dotations budgétaires à son programme TSI ont été récemment augmentées. Les projets de recherche et les projets opérationnels destinés à favoriser les actions de formation spécialisée des agents chargés de l'application des lois ainsi que la coopération entre ces services et les entreprises font également l'objet d'un soutien dans le cadre de programmes relevant du troisième pilier tels que STOP, FALCONE, OISIN et GROTIUS[11].

Le programme d'action relatif à la criminalité organisée, adopté par le Conseil JAI en mai 1997 et approuvé par le Conseil européen d'Amsterdam, invitait la Commission à réaliser une étude sur la criminalité informatique pour la fin 1998. Cette étude, connue sous son titre abrégé "étude COMCRIME", a été présentée en avril 1998 par la Commission au groupe multidisciplinaire du Conseil sur la criminalité organisée[12]. La présente communication est, en partie, un suivi de cette demande du Conseil JAI.

Avant de rédiger la présente communication, la Commission a jugé utile de mener des consultations informelles avec des représentants des services des États membres chargés de l'application des lois, des autorités de contrôle chargées de la protection des données[13] et des représentants d'entreprises européennes (en majorité des fournisseurs de services Internet et des entreprises de télécommunications)[14].

Sur la base de l'analyse réalisée pour cette étude et des recommandations qui y sont formulées, ainsi que des conclusions tirées du processus de consultation évoqué, des nouvelles possibilités offertes par le traité d'Amsterdam et des travaux déjà menés par l'Union européenne, le G8 et le Conseil de l'Europe, la présente communication s'attache à examiner les diverses actions complémentaires envisageables par l'Union européenne pour lutter contre la criminalité informatique. Au niveau de l'Union, les solutions retenues ne doivent pas avoir pour conséquence de faire obstacle à l'achèvement du marché intérieur ni de le fragmenter, ni déboucher sur des mesures qui compromettent la protection des droits fondamentaux[15].

Résolution du Conseil du 17 janvier 1995 relative à l'interception légale des télécommunications (JO C 329 du 4.11.1996, p. 1).

11 http://europa.eu.int/comm/justice_home/jai/prog_fr.htm.

12 "Legal Aspects of Computer-related Crime in the Information Society - COMCRIME." L'étude, commandée par la Commission européenne, a été réalisée par le Prof. U. Sieber de l'université de Wurtzbourg. Le rapport final est accessible à l'adresse http://europa.eu.int/ISPO/legal/en/crime/crime.html.

13 Au niveau de l'Union européenne, les autorités de contrôle de la protection des données font partie du groupe de travail "article 29" sur la protection des données, ce groupe étant un organe de l'Union européenne à caractère consultatif et indépendant, compétent pour les questions de protection de la vie privée et des données (voir articles 29 et 30 de la directive 95/46/CE).

14 Deux réunions ont eu lieu les 10 décembre 1999 et 1er mars 2000 avec les services répressifs. Il convient aussi de mentionner une réunion avec les représentants des entreprises spécialisées dans l'Internet le 13 mars 2000, une réunion avec un petit nombre d'experts de la protection des données à caractère personnel le 31 mars 2000 et une réunion finale avec tous les représentants et experts précités, le 17 avril 2000. Les comptes rendus de ces réunions peuvent être obtenus sur demande écrite envoyée à l'adresse suivante: Commission européenne, Unité INFSO/A4, Wetstraat/Rue de la Loi 200, 1049 Bruxelles, Belgique, ou à cette autre adresse: Commission européenne, Unité JAI/B2, Wetstraat/Rue de la Loi 200, 1049 Bruxelles, Belgique.

15 Charte des droits fondamentaux de l'Union européenne (http://europa.eu.int/comm/justice_home/unit/charte_fr.htm), article 6 du traité sur l'Union européenne et jurisprudence de la Cour de justice des Communautés européennes.

2. SECURITE DES INFRASTRUCTURES DE L'INFORMATION

Dans la société de l'information, les réseaux mondiaux contrôlés par l'utilisateur remplacent progressivement l'ancienne génération des réseaux de communication nationaux. L'une des raisons qui expliquent le succès de l'Internet est qu'il a donné aux utilisateurs l'accès aux technologies les plus modernes. La loi de Moore[16] prédit que la puissance de calcul doublera tous les 18 mois. Or, les technologies de communication connaissent des progrès encore plus rapides[17]. L'une des conséquences de cette évolution est que le volume de données transportées via l'Internet double à intervalles de moins d'un an.

Les réseaux téléphoniques traditionnels étaient construits et exploités par des organisations nationales. Les usagers avaient un choix de services limité et n'exerçaient aucun contrôle sur cet environnement. Les premiers réseaux de transmission de données qui ont été mis en place reposaient sur cette même philosophie, à savoir celle d'un environnement centralisé. Les systèmes de sécurité développés dans un tel environnement reflétaient cette centralisation.

L'Internet et les autres nouveaux réseaux sont très différents, de sorte que les besoins en matière de sécurité doivent être traités en conséquence. Dans ces réseaux, l'information et le contrôle sont situés surtout à la périphérie, là où se trouvent l'utilisateur et les services. Le noyau du réseau est simple et efficace, et a essentiellement pour tâche de transmettre des données. La vérification et le contrôle du contenu sont limités. Ils n'interviennent qu'en bout de chaîne, chez le destinataire final, là où les bits deviennent le son d'une voix, une radiographie ou la confirmation d'une opération bancaire. La sécurité est donc, dans une large mesure, la responsabilité de l'utilisateur, seul à même d'apprécier la valeur des bits de données qu'il envoie ou qu'il reçoit, et seul capable de déterminer le niveau de protection dont il a besoin.

L'environnement de l'utilisateur est donc un élément clé de l'infrastructure de l'information. C'est à cet endroit que les technique de sécurité doivent être mises en œuvre, avec l'autorisation et la participation de l'utilisateur et en respectant ses besoins. C'est d'autant plus important si on considère l'éventail de plus en plus large des activités que l'on peut mener à partir d'un même terminal. On peut en effet, à partir d'un même équipement, travailler, se distraire, regarder la télévision et autoriser des virements bancaires.

En matière de sécurité, plusieurs techniques ont déjà été mises au point, tandis que de nouvelles sont en cours de développement. On comprend mieux les avantages, sous l'angle de la sécurité, des logiciels libres ou ouverts (c'est-à-dire des logiciels dont le code source est ouvert). Beaucoup de travaux ont été menés pour la mise en forme de méthodes et la détermination de critères d'évaluation de la sécurité. Le recours aux techniques de cryptage et aux signatures électroniques tend à devenir indispensable, en particulier face à la croissance de l'accès sans fil. Il nous faut des mécanismes d'authentification de plus en plus variés pour couvrir nos différents besoins dans les environnements où nous évoluons. Dans certains cas, en effet, nous pouvons avoir besoin, ou envie, de conserver l'anonymat, tandis que dans d'autres, il arrive au contraire que nous devions faire la preuve d'une caractéristique déterminée, comme le fait d'être adulte, employé ou client d'une entreprise donnée, sans pour

---

[16] Cette observation a été formulée en 1965 par Gordon Moore, cofondateur de l'entreprise Intel, à propos du rythme de progression du nombre de transistors sur un circuit intégré. À l'heure actuelle, ce nombre double quasiment tous les dix-huit mois, ce qui a une influence directe sur le prix et les performances des puces informatiques. Nombre d'experts pensent que cette loi se vérifiera encore pendant les dix prochaines années au moins.

[17] Les plus récentes permettent, sur un seul et même câble à fibres optiques, d'acheminer simultanément l'équivalent de 100 millions de communications téléphoniques.

autant dévoiler notre identité. Dans d'autres situations, enfin, il nous faut prouver notre identité. En outre, les filtres logiciels étant de plus en plus perfectionnés, nous pouvons nous protéger, ainsi que les personnes à notre charge, des données dont nous ne voulons pas, telles que celles dont le contenu est indésirable, les courriers électroniques non sollicités, les logiciels malveillants ainsi que les autres formes d'attaque. La mise en œuvre et la gestion de ces exigences de sécurité à l'intérieur de l'Internet et des nouveaux réseaux entraînent aussi de lourdes dépenses pour les entreprises et les utilisateurs. C'est pourquoi il importe d'encourager l'innovation et l'utilisation commerciale des technologies et des services de sécurité.

Naturellement, l'infrastructure partagée des liaisons de télécommunications et des serveurs de noms de domaine pose également des problèmes de sécurité. La transmission de données dépend des liaisons physiques qu'empruntent les données lors de leur acheminement d'un ordinateur à l'autre. Ces liaisons doivent être mises en place et protégées de telle manière que la transmission reste possible malgré les accidents et les attaques et un volume de trafic qui ne cesse de croître. Les communications dépendent également de services cruciaux comme ceux que fournissent les serveurs de noms (de domaine), et en particulier, du petit nombre de serveurs de noms de domaine primaires, pour obtenir les adresses nécessaires. Il faudra aussi, pour chacun de ces composants, une protection appropriée, qui variera en fonction de la partie de l'espace de nom de domaine et de la clientèle à laquelle le service est fourni.

Guidées par l'objectif qui consiste à répondre avec plus de souplesse et à s'adapter plus rapidement aux besoins des personnes, les technologies utilisées dans les infrastructures de l'information sont devenues de plus en plus complexes, sans que soit accordée une attention suffisante aux problèmes de sécurité lors de la conception de ces technologies. En outre, cette complexité met en jeu des logiciels de plus en plus perfectionnés et interconnectés, qui présentent parfois des faiblesses et des failles sous l'angle de la sécurité qui peuvent être facilement exploitées en vue d'attaques. À mesure que la complexité du cyberespace et de ses composants se renforcera, il se peut que des faiblesses nouvelles et imprévues se fassent jour.

Plusieurs systèmes technologiques existent déjà, tandis que de nouveeaux sont en cours de développement en vue d'améliorer la sécurité dans le cyberespace. Ils comprennent des mesures:

- de sécurisation des éléments essentiels de l'infrastructure grâce au déploiement d'infrastructures à clé publique (ICP), au développement de protocoles de sécurité, etc.

- de sécurisation des environnements privés et publics par la mise au point de solutions de qualité (logiciels, protections, programmes antivirus, systèmes de gestion électronique des droits de propriété intellectuelle, systèmes de cryptage, etc.)

- d'authentification des utilisateurs autorisés, d'utilisation de cartes à puce, d'identification biométrique, ainsi que les signatures électroniques, les techniques de contrôle d'accès par la fonction, etc.

Ces mesures nécessitent le déploiement d'efforts supplémentaires pour mettre au point des technologies de sécurité, en faisant appel à la coopération afin d'assurer l'interopérabilité nécessaire entre les solutions proposées, grâce à des accords sur des normes internationales.

Il est également important que tout cadre conceptuel futur sur la sécurité fasse partie intégrante de l'architecture globale, en prévoyant des solutions face aux risques et à la vulnérabilité dès le début du processus de conception. Ce qui ne correspond plus aux approches traditionnelles qui consistent à développer des solutions de rattrapage pour essayer de combler les lacunes qu'exploitent des organisations malveillantes de plus en plus complexes, dotées de moyens de plus en plus perfectionnés.

Le programme communautaire sur les technologies de la société de l'information (TSI)[18], notamment les actions consacrées à la sécurité de l'information et des réseaux et aux autres technologies visant à susciter la confiance[19], constitue un cadre pour le développement des capacités et des technologies nécessaires pour comprendre et relever les défis que commence à poser la criminalité informatique. Ces technologies comprennent notamment des solutions techniques de protection contre les atteintes aux droits fondamentaux que sont le respect de la vie privée et la protection des données à caractère personnel, ainsi qu'aux autres droits de la personne, de même que des moyens de lutte contre la cybercriminalité. En outre, dans le contexte du programme TSI, une initiative sur la sécurité de fonctionnement a été lancée. Cette initiative contribuera à susciter la confiance dans des infrastructures de l'informationtrès étroitement interconnectées et dans des systèmes informatiques intégrés mis en réseau, par une sensibilisation au problème de la sécurité de fonctionnement et en encourageant les technologies qui la rendent possible. La coopération internationale fait intégralement partie de cette initiative. Le programme TSI a développé les relations de travail avec la DARPA et la NSF et a créé, en liaison avec le ministère américain des affaires étrangères, une task force conjointe Communauté européenne/États-Unis sur la protection des infrastructures critiques[20].

Enfin, la mise en œuvre des obligations en matière de sécurité qui découlent, en particulier, des directives de l'Union européenne sur la protection des données[21], contribue à renforcer la sécurité des réseaux et du traitement automatisé des données.

3. CRIMINALITE INFORMATIQUE

Les systèmes modernes de l'information et de communication offrent la possibilité d'exercer à tout moment des activités illicites à partir de n'importe quel lieu de la planète. Il n'existe pas de statistiques fiables sur la véritable étendue du phénomène de la criminalité informatique. Le nombre d'intrusions détectées et signalées à ce jour ne donne vraisemblablement pas une idée exacte de toute l'étendue du problème. La prise de conscience et l'expérience des administrateurs de systèmes et des utilisateurs étant encore limitées, nombre d'intrusions ne sont pas décelées. De surcroît, beaucoup d'entreprises ne sont pas disposées à signaler les cas de fraude informatique, par souci d'éviter toute mauvaise publicité et afin de ne pas s'exposer au risque de nouvelles attaques. Les services de police, dans leur majorité, ne tiennent pas encore de statistiques sur les utilisations d'ordinateurs et de systèmes de communication impliqués dans ce type de fraude et dans d'autres formes de criminalité. Or, il faut s'attendre à une augmentation du nombre d'activités illicites à mesure que s'intensifiera l'usage des

---

[18] Le Programme IST est géré par la Commission européenne. Il fait partie du 5ème programme-cadre, qui couvre la période 1998 à 2002. Pour plus de l'informations, consulter le site http://www.cordis.lu/ist.

[19] Dans l'action clé 2 - Nouvelles méthodes de travail et commerce électronique.

[20] Sous l'égide du groupe consultatif conjoint institué en vertu de l'Accord de coopération scientifique et technologique entre la Communauté européenne et le gouvernement des États-Unis d'Amérique.

[21] Voir l'article 4 de la directive 97/66/CE (qui prévoit aussi une obligation de l'information sur les risques qui subsistent en matière de sécurité) et l'article 17 de la directive 95/46/CE.

ordinateurs et des réseaux. Il faut donc impérativement recueillir des données fiables sur l'ampleur du phénomène de la criminalité informatique.

Dans la présente communication, la criminalité informatique est entendue dans un sens large, comme désignant toute infraction qui, d'une manière ou d'une autre, implique l'utilisation des technologies informatiques. Différentes conceptions s'opposent toutefois sur ce qui relève de la criminalité informatique. Les notions de "criminalité informatique", "délinquance informatique", "criminalité de hautes technologies" et de "cybercriminalité" sont souvent employées indifféremment. On peut établir une distinction entre la criminalité spécifiquement liée à l'informatique et les infractions classiques commises à l'aide des technologies informatiques. Un exemple d'actualité, qui illustre cette distinction, est celui de la douane, où l'Internet se révèle être un moyen de commettre des infractions traditionnelles à la législation douanière, telles que la contrebande, la contrefaçon, etc. Tandis que les infractions informatiques imposent une mise à jour des définitions des infractions dans les codes pénaux nationaux, les infractions traditionnelles commises à l'aide de l'ordinateur rendent nécessaires un renforcement et une amélioration de la coopération ainsi que l'adoption de mesures procédurales.

Toutes ces infractions ont cependant en commun d'exploiter les réseaux de l'information et de communication existants, qui ne connaissent pas de frontières, ainsi que la circulation de données qui sont intangibles et extrêmement volatiles Ces caractéristiques appellent un réexamen des mesures existantes afin de s'attaquer aux activités illicites qui s'exercent sur ces réseaux et ces systèmes ou grâce à eux.

De nombreux pays ont adopté une législation sur la criminalité informatique. Dans les États membres de l'Union européenne, un certain nombre d'instruments juridiques ont été adoptés. Même si, en dehors de la décision du Conseil sur la pornographie enfantine sur l'Internet, il n'existe à ce jour aucun instrument juridique communautaire qui traite directement de la criminalité informatique, il en existe un certain nombre qui sont indirectement applicables en la matière.

Les principaux problèmes dont traite la législation existante dans le domaine de la criminalité informatique, tant au niveau de l'Union européenne qu'à l'échelon des États membres, sont les suivants:

Atteintes à la vie privée: Plusieurs pays ont adopté une législation pénale concernant la collecte, le stockage, la modification, la divulgation et la diffusion illicites de données à caractère personnel. Au niveau de l'Union européenne, il existe deux directives qui rapprochent les législations nationales sur la protection de la vie privée dans le cadre du traitement des données à caractère personnel[22]. L'article 24 de la directive 95/46/CE oblige expressément les États membres à prendre les mesures appropriées pour assurer la pleine application des dispositions de cette directive, et à définir notamment les sanctions à appliquer en cas de violation des législations nationales de transposition. Les droits fondamentaux au respect de la vie privée et à la protection des données sont, en outre, inscrits dans la Charte des droits fondamentaux de l'Union européenne.

---

[22] Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications. L'article 24 de la directive 95/46/CE oblige les États membres à définir les sanctions à appliquer en cas de violation des dispositions relatives à la protection des données.

Infractions liées au contenu: La diffusion, en particulier sur l'Internet, d'images pornographiques, notamment la pornographe enfantine, de déclarations racistes et de l'informations incitant à la violence soulèvent la question de savoir jusqu'à quel point le droit pénal pourrait permettre de lutter contre de tels actes. La Commission a considéré que ce qui est illégal hors ligne doit l'être également en ligne. L'auteur ou le fournisseur de contenu[23] peut voir sa responsabilité pénale mise en cause. Le Conseil a adopté une décision visant à lutter contre la pornographie enfantine sur l'Internet[24].

La responsabilité des prestataires de services intermédiaires, dont les réseaux ou les serveurs sont utilisés pour transmettre ou stocker des informations émanant de tiers, est traitée par la directive sur le commerce électronique.

Infractions économiques, accès non autorisé et sabotage: De nombreux pays ont adopté une législation sur la criminalité informatique qui définit de nouvelles infractions liées à l'accès non autorisé aux systèmes informatiques (par exemple, piratage informatique, sabotage informatique et diffusion de virus, espionnage informatique, falsification informatique ou fraude informatique[25]) et de nouvelles formes d'infractions (par exemple, procéder à des manipulations informatiques au lieu de s'attaquer à une personne physique). L'objet de l'infraction est souvent intangible; il peut s'agir en effet d'argent déposé dans une banque ou de programmes d'ordinateurs. Il n'existe, à l'heure actuelle, aucun instrument communautaire traitant de ce type d'activités illicites. En matière de prévention, le règlement révisé sur les biens à double usage qui a été adopté récemment a contribué, de manière significative, à libéraliser l'accès aux produits de cryptage.

Atteintes à la propriété intellectuelle: Deux directives ont été adoptées, concernant la protection juridique des programmes d'ordinateur et des bases de données[26], qui concernent directement la société de l'information et prévoient des sanctions. Le Conseil a adopté une position commune sur une proposition de directive relative au droit d'auteur et aux droits voisins dans la société de l'information. Cette directive devrait être adoptée début 2001[27]. La violation du droit d'auteur et des droits voisins ainsi que la neutralisation des moyens technologiques mis au point afin de protéger ces droits doivent être sanctionnés. En ce qui concerne la contrefaçon et le piratage, la Commission présentera, avant la fin de l'année 2000, une communication qui fera le bilan du processus de consultation lancé avec la publication de son Livre vert de 1998 et annoncera un plan d'action en la matière. À mesure que l'Internet

---

23 Le fournisseur de contenu ne doit pas être confondu avec le prestataire ou fournisseur de services.

24 Décision du Conseil du 29 mai 2000 relative à la lutte contre la pornographie enfantine sur l'Internet (JO L 138 du 9.6.2000, p. 1).

25 Les médias ont accordé beaucoup d'attention aux attaques récentes de dénis de service distribués ou répartis, dont ont été victimes de grands sites Internet et à la diffusion du virus dénommé LoveBug. Il faut toutefois resituer le problème. Les attaques de déni de service, qu'elles soient délibérées ou accidentelles, de même que les virus transmis par le courrier électronique sont apparus il y a bien des années. Le ver d'Internet de Robert Morris et le virus de l'arbre de Noël en furent les premiers exemples. Il existe des produits et des procédures pour faire face à ces virus. Un bon esprit de coopération règne également au sein de la communauté Internet pour limiter les préjudices que peuvent provoquer de tels incidents au moment où ils se produisent. Il existe une coopération similaire pour limiter les abus liés à l'arrosage (diffusion de messages non sollicités).

26 Directive 91/250/CEE du Conseil du 14 mai 1991 concernant la protection juridique des programmes d'ordinateur (JO L 122 du 17.5.1991, p. 42).
Directive 96/9/CE du Parlement européen et du Conseil du 11 mars 1996 concernant la protection juridique des bases de données (JO L 77 du 27.3.1996, p. 20).

27 Position commune arrêtée par le Conseil en vue de l'adoption d'une directive du Parlement européen et du Conseil sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information (CS/2000/9512).

prend plus d'importance sur le plan commercial, émergent de nouveaux types de litiges portant sur l'enregistrement abusif de noms de domaine (cybersquattage et "warehousing") et le détournement inverse de noms de domaine ("reverse hijacking") et, naturellement, des voix se font aussi entendre pour réclamer l'adoption de règles et de procédures afin de résoudre ces problèmes[28].

La question du respect des obligations fiscales doit aussi être posée. Dans les transactions commerciales où le destinataire d'une prestation de services électroniques en ligne est situé dans l'Union européenne, l'obligation fiscale naît, dans la plupart des cas, sur le territoire dans lequel la consommation de ces services est réputée avoir lieu[29]. Le non-respect de ses obligations fiscales expose l'entreprise à des sanctions civiles (voire pénales dans certains cas), qui peuvent aller jusqu'à la saisie-arrêt sur des comptes bancaires ou sur d'autres avoirs. Même s'il est préférable que l'assujetti s'acquitte de ses obligations volontairement, ces obligations doivent en fin de compte avoir force exécutoire.

La coopération entre administrations fiscales est indispensable pour pouvoir atteindre cet objectif. Si la possibilité est donnée dans certains cas de protéger des opérations licites, les auteurs d'infractions pourront exploiter ces mêmes moyens pour protéger leurs transactions illicites. Les moyens technologiques qui sécurisent le commerce électronique peuvent donc aussi servir le trafic de stupéfiants. Il faudra déterminer des priorités et faire des choix.

La protection des victimes de la criminalité informatique passe aussi par l'examen des questions de responsabilité, des voies de recours et des réparations qui se posent lors d'infractions informatiques. La confiance dépend non seulement de l'utilisation de technologies appropriées, mais aussi des garanties juridiques et économiques qui sont données. Ces questions devront être examinées pour toutes les formes de criminalité informatique.

Il faut disposer d'instruments efficaces de droit positif et de droit procédural qui soient similaires, sinon au niveau mondial, du moins au niveau européen, afin de protéger les victimes de la criminalité informatique et de poursuivre les auteurs de ces infractions. Parallèlement, les communications à caractère personnel, le respect de la vie privée, la protection des données, l'accès à l'information et la diffusion de celle-ci sont des droits fondamentaux des démocraties modernes. C'est la raison pour laquelle il faudrait disposer et user de mesures de prévention efficaces de manière à pouvoir diminuer les mesures répressives. Toute mesure législative qui pourrait être nécessaire pour lutter contre la cybercriminalité devra trouver un juste équilibre entre ces intérêts majeurs.

---

[28] Communication de la Commission au Conseil et au Parlement européen, L'organisation et la gestion de l'Internet - Enjeux internationaux et européens 1998 -2000, avril 2000, COM(2000) 202.

[29] La Commission a proposé une série de modifications du régime communautaire de la TVA, destinées à clarifier le lieu d'imposition (COM(2000) 349 - Proposition de directive du Conseil modifiant la directive 77/388/CEE concernant le régime de taxe sur la valeur ajoutée applicable à certains services fournis par voie électronique) qui est en cours d'examen au Conseil et au Parlement européen. Dans certains cas, cependant, l'obligation fiscale peut incomber au fournisseur, même si ce dernier n'est pas physiquement établi dans la juridiction fiscale.

4. QUESTIONS DE DROIT POSITIF

Le rapprochement des dispositions de droit positif en matière de criminalité de hautes technologiesassurera un niveau de protection minimum aux victimes de la criminalité informatique (par exemple, aux victimes de la pornographie enfantine), aidera à satisfaire à l'exigence selon laquelle une activité doit d'abord constituer une infraction dans les deux pays considérés pour que ces derniers puissent s'entraider sur le plan judiciaire dans le cadre d'une enquête pénale (exigence de la double incrimination) et clarifiera davantage la situation pour les entreprises (par exemple, sur la définition d'un contenu illicite).

En fait, l'adoption d'un instrument législatif communautaire qui rapprocherait le droit pénalpositif en matière de criminalité informatique figure parmi les priorités de l'Union européenne depuis le Conseil européen de Tampere d'octobre 1999[30]. Ce Conseil a inscrit la criminalité de hautes technologies dans une liste limitée de secteurs dans lesquels des efforts doivent être déployés pour trouver un accord sur des définitions, des incriminations et des sanctions communes. Ce type de criminalité figure aussi dans la recommandation n° 7 de la stratégie de l'Union européenne sur la prévention et la répression de la criminalité organisée pour le prochain millénaire, qui a été adoptée par le Conseil "Justice et affaires intérieures" en mars 2000[31]. Il est également inscrit dans le programme de travail de la Commission pour l'année 2000 et dans le tableau de bord sur la création d'un espace de liberté, de sécurité et de justice, présenté par la Commission et adopté par le Conseil "Justice et affaires intérieures" le 27 mars 2000[32].

La Commission a suivi les travaux du Conseil de l'Europe consacrés à la convention sur la cybercriminalité, qui retient, dans sa version actuelle, quatre catégories d'infractions pénales: 1) infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques, 2) infractions informatiques, 3) infractions se rapportant au contenu et 4) infractions liées aux atteintes à la propriété intellectuelle et aux droits voisins.

Le rapprochement au niveau communautaire pourrait être plus important que celui que prévoit la convention du Conseil de l'Europe, qui représente un rapprochement international minimum. Elle pourrait être opérationnelle en moins de temps qu'il n'en faudrait pour que la convention du Conseil de l'Europe entre en vigueur[33]. Elle intégrerait la criminalité informatique dans le champ du droit communautaire et instaurerait des mécanismes communautaires de contrôle de l'application du droit.

La Commission attache une grande importance au fait de doter l'Union européenne de moyens d'action efficaces, en particulier contre la pornographie enfantine sur l'Internet. Elle se félicite de la décision du Conseil sur la lutte contre la pornographie enfantine dans ce secteur, mais partage l'avis du Parlement européen selon lequel des mesures complémentaires sont nécessaires afin de rapprocher les législations nationales. Elle entend présenter avant la fin de cette année une proposition de décision-cadre qui comprendra des dispositions en vue d'un rapprochement des lois et des sanctions applicables à la pornographie enfantine sur l'Internet[34].

---

30 http://db.consilium.eu.int/fr/info/eurocouncil/index.htm

31 Prévention et contrôle de la criminalité organisée: une stratégie de l'Union européenne pour le prochain millénaire (JO C 124 du 3.5.2000).

32 http://europa.eu.int/comm/dgs/justice_home/index_fr.htm.

33 La convention du Conseil de l'Europe ne pourra entrer en vigueur qu'après sa ratification.

34 Cette initiative fait partie d'un ensemble de propositions couvrant également des problèmes plus larges, liés à l'exploitation sexuelle des enfants et à la traite des êtres humains, comme cela avait été annoncé

Conformément aux conclusions du Conseil européen de Tampere, la Commission présentera une proposition législative en vertu du Titre VI du traité sur l'Union européenne afin de rapprocher les dispositions nationales en matière de criminalité de hautes technologies. Cette proposition tiendra compte des progrès des négociations au sein du Conseil de l'Europe et traitera en particulier de la nécessité de rapprocher les législations en matière de piratage et d'attaques par déni de service. Elle contiendra des définitions types pour l'Union européenne dans ce domaine. Elle pourrait aussi aller plus loin que le projet de convention du Conseil de l'Europe en garantissant que les cas graves de piratage et d'attaques de déni de service soient punis d'une peine minimum dans tous les États membres.

En outre, la Commission va étudier les possibilités de lutter contre le racisme et la xénophobie sur l'Internet afin de présenter, en vertu du titre VI du traité sur l'Union européenne, une proposition de décision-cadre du Conseil visant les activités racistes et xénophobes tant hors ligne qu'en ligne, en tenant compte des résultats de l'évaluation prochaine de la mise en œuvre, par les États membres, de l'actioncommune du 15 juillet 1996 concernant la lutte contre le racisme et la xénophobie[35]. Cette action commune a marqué une première étape sur la voie du rapprochement des infractions pénales liées au racisme et à la xénophobie, mais il est nécessaire d'augmenter le rapprochement au sein de l'Union européenne. L'importance et le caractère sensible de ces phénomènes ont été soulignés dans une ordonnance rendue par un tribunal français le 20 novembre 2000 et condamnant Yahoo à empêcher l'accès des internautes français à des sites vendant des objets nazis[36].

Enfin, la Commission réfléchira à la manière de renforcer l'efficacité des efforts de lutte contre le commerce de drogues illicites sur l'Internet, dont l'importance a été reconnue dans la Stratégie antidrogue de l'Union européenne (2000-2004) soutenue parle Conseil européen d'Helsinki a pris acte[37].

5. QUESTIONS DE DROIT PROCEDURAL

La nature même des infractions informatiques pose, sur les scènes nationale et internationale, le problème des procédures applicables, dans la mesure où des souverainetés, des compétences et des législations différentes s'opposent. Plus que pour toute autre forme de criminalité transnationale, la rapidité, la mobilité et la flexibilité de la criminalité informatique défient les règles existantes du droit pénal procédural.

Le rapprochement des pouvoirs en matière de droit procédural améliorera la protection des victimes en permettant aux autorités chargées de l'application des lois de disposer des pouvoirs dont ils ont besoin pour instruire les infractions sur leur propre territoire et qu'ils soient en mesure de répondre rapidement et efficacement aux demandes de coopération introduites par d'autres pays.

---

dans la communication de la Commission sur la traite des êtres humains de décembre 1998. Le texte de la proposition de décision-cadre du Conseil est annexé à la communication de la Commission au Conseil et au Parlement européen "relative à la lutte contre la traite des êtres humains et l'exploitation sexuelle des enfants: deux propositions de décision-cadre", qui est publiée parallèlement à la présente communication.

35 JO L 185 du 24.7.1996, p. 5. Disponible également sur le site Internet du réseau judiciaire européen http://ue.eu.int/ejn/index.htm.

36 Tribunal de grande instance de Paris, ordonnance de référé rendue le 20 novembre 2000, n RG 00/05308.

37 Plan d'action de l'Union européenne en matière de lutte contre la drogue (2000-2004), COM(1999) 239 final. http://europa.eu.int/comm/justice_home/unit/drogue_fr.htm.

Il faut également veiller à ce que les mesures prises sur la base de la législation pénale, qui relève généralement de la compétence des États membres, et du titre VI du traité sur l'Union européenne, soient conformes aux exigences du droit communautaire. En particulier, selon une jurisprudence constante, la Cour de justice considère que ces dispositions législatives ne peuvent opérer une discrimination à l'égard de personnes auxquelles le droit communautaire confère le droit à l'égalité de traitement, ni restreindre les libertés fondamentales garanties par le droit communautaire[38]. Les nouveaux pouvoirs qui seraient conférés aux autorités chargées de l'application des lois doivent être appréciés au regard du droit communautaire et de leurs répercussions sur la vie privée.

5.1. Interception des communications

Dans l'Union européenne, il existe un principe général de confidentialité des communications (et des données relatives au trafic). Les interceptions sont illégales, sauf autorisation prévue par la loi dans des cas précis où ces mesures sont nécessaires et justifiées par des finalités en nombre limité. Ce principe découle de l'article 8 de la Convention européenne des droits de l'homme, qui est mentionnée dans l'article 6 du traité sur l'Union européenne, et plus précisément des directives 95/46/CE et 97/66/CE.

Tous les États membres ont mis en place un cadre légal permettant aux autorités chargées de l'application des lois d'obtenir des ordonnances judiciaires (ou, lorsque deux États membres sont concernés, une autorisation délivrée personnellement par un ministre occupant un rang élevé dans la hiérarchie ministérielle) pour la mise sur écoute des communications sur le réseau public de télécommunications[39]. Cette législation, qui doit être conforme au droit communautaire pour autant que ce dernier s'applique, prévoit des garanties pour protéger le droit fondamental des personnes physiques au respect de leur vie privée, par exemple en limitant le recours à l'interception des communications à l'instruction de cas d'infractions graves, en exigeant que, dans chacune de ces enquêtes, l'interception soit nécessaire et proportionnée, ou en veillant à ce que la personne soit informée de cette interception dès que cela n'entrave plus le bon déroulement de l'enquête. Dans un grand nombre d'États membres, la législation sur l'interception des communications prévoit l'obligation pour les entreprises des télécommunications (assurant un service public) de donner la possibilité de procéder à ces écoutes. Une résolution du Conseil de 1995 avait pour objectif de coordonner les spécifications en matière d'interception[40].

---

38 Affaire C-274/96, Bickel & Franz, Recueil 1998, p. I-7637, point 17 des motifs et affaire C-186/87, Cowan, Recueil 1989, p. 195, point 19 des motifs. En particulier, les mesures administratives ou répressives ne doivent pas dépasser le cadre de ce qui est strictement nécessaire, les modalités de contrôle ne doivent pas être conçues de manière à restreindre la liberté voulue par le traité et il ne faut pas y rattacher une sanction si disproportionnée à la gravité de l'infraction qu'elle deviendrait une entrave à cette liberté (affaire C-203/80, Casati, Recueil 1981, p. 2595, point 27 des motifs).

39 Deux États membres ne reconnaissent pas les communications interceptées comme éléments de preuve dans les procédures pénales.

40 Résolution du Conseil du 17 janvier 1995 relative à l'interception légale des télécommunications (JO C 329 du 4.11.1996, p. 1). L'annexe contient une liste des spécifications des services autorisés en matière d'interception dont les États membres étaient invités à tenir compte lors de la définition et de la mise en œuvre des politiques et des mesures nationales applicables en la matière. En 1998, la présidence autrichienne a proposé une résolution du Conseil de l'Union européenne visant à étendre le champ d'application de la résolution de 1995 aux nouvelles technologies, notamment l'Internet et les communications par satellite. Cette question a fait l'objet d'un débat au sein de deux commissions du Parlement européen, à savoir la commission des libertés publiques et des affaires intérieures et la commission juridique et des droits des citoyens, qui sont toutes deux parvenues à des conclusions différentes. La première a en effet considéré cette résolution comme une clarification et une mise à jour

Les exploitants de réseaux traditionnels, en particulier ceux qui fournissent des services de téléphonie vocale, ont déjà noué par le passé des relations de travail avec les autorités chargées de l'application des lois afin de faciliter l'interception légale des télécommunications. La libéralisation des télécommunications et l'explosion de l'usage de l'Internet ont attiré nombre de nouvelles entreprises sur le marché, auxquelles on a imposé de nouveau des obligations en matière d'interception. Il faudra discuter, dans le cadre du dialogue entre les pouvoirs publics et les entreprises ainsi qu'avec toutes les autres parties concernées, notamment les autorités de contrôle chargées de la protection des données, des questions touchant à la réglementation, à la faisabilité technique, à la répartition des coûts et à l'impact commercial.

Les nouvelles technologies rendent indispensable une coopération entre les États membres s'ils veulent conserver la possibilité d'intercepter légalement les communications. La Commission estime que, si les États membres imposent aux entreprises de télécommunications et aux fournisseurs de services Internet de nouvelles obligations technologies en matière d'interception, ces normes devront faire l'objet d'une coordination internationale afin d'éviter les distorsions au sein du marché intérieur, de réduire au minimum le coût qu'elles impliquent pour les entreprises et de manière à respecter les exigences de respect de la vie privée et de protection des données. Ces normes devraient être transparentes et rendues publiques, le cas échéant, mais il ne faudrait pas qu'elles introduisent des faiblesses dans les infrastructures de communication.

Dans le cadre de la convention de l'Union européenne relative à l'entraide judiciaire en matière pénale[41], il a été convenu de faciliter la coopération en matière d'interception légale[42]. La convention contient des dispositions sur l'interception des communications téléphoniques par satellite[43] et sur l'interception des communications passées par une personne se trouvant sur le territoire d'un autre État membre[44]. La Commission est d'avis que les règles

---

de l'ancienne et l'a jugée acceptable. La seconde, en revanche, a formulé de vives critiques, tant sous l'angle des atteintes potentielles aux droits de l'homme que sous celui du coût économique pour les opérateurs, ce qui l'a amenée à rejeter la proposition du Conseil et à inviter la Commission à élaborer une nouvelle proposition dès que le traité d'Amsterdam serait entré en vigueur. Ce projet de résolution du Conseil n'a pas fait l'objet, au cours des derniers mois, d'un examen au fond par le Conseil ni par ses groupes de travail.

41 JO C 197 du 12.7.2000, p. 1. Elle a été adoptée le 29 mai 2000. Les dispositions de cette convention relatives à l'interception des communications ne s'appliquent qu'aux États membres de l'Union européenne et non aux pays tiers.

42 La convention prévoit des mesures de sauvegarde minimales en ce qui concerne la protection de la vie privée et des données à caractère personnel.

43 L'objet initial des négociations était de donner des possibilités d'interception de communications passées par des personnes utilisant un téléphone par satellite et se trouvant sur le territoire de l'État membre interceptant. Sous l'angle technique, le point stratégique pour intercepter ce type de communications est au niveau de la station terrestre. Il était donc nécessaire de demander l'assistance technique de l'État membre sur le territoire duquel est située cette station terrestre. La convention prévoit deux possibilités pour régler ce problème: une procédure accélérée d'entraide judiciaire, qui passe par des demandes d'assistance ponctuelles adressées à l'État membre qui possède cette station terrestre, et une solution technique reposant sur l'accès à distance à la station terrestre réalisé par l'État membre interceptant, qui ne requiert aucune demande.

44 La convention constitue également un cadre légal pour les demandes d'interception de communications passées par une personne se trouvant sur le territoire d'un autre État membre (l'État membre requis). Dans ce cas de figure, l'État membre interceptant et l'État membre requis doivent tous deux obtenir un ordre ou un mandat d'interception en vertu de leur droit national respectif. En dernier lieu, la convention fixe les règles applicables aux situations dans lesquelles l'État membre interceptant peut avoir la possibilité d'intercepter les communications d'une personne se trouvant sur le territoire d'un autre État membre sans avoir à solliciter l'assistance technique de cet État membre.

d'interception qui figurent dans cette convention d'entraide sont, pour l'heure, le maximum que l'on puisse envisager. Le texte de la convention est neutre sur le plan technologique. Il faudra donc la tester afin de savoir comment elle fonctionne en pratique avant d'envisager une quelconque amélioration. La Commission examinera les résultats de son application avec les États membres, les entreprises, les utilisateurs et les autorités de contrôle chargées de la protection des données, de manière à garantir l'efficacité, la transparence et le juste équilibre des initiatives prises en la matière.

Toute exploitation des possibilités d'interception faite de manière abusive et sans discernement, en particulier à l'échelle internationale, poserait des problèmes sous l'angle des droits de l'homme et saperait la confiance du citoyen dans la société de l'information. La Commission s'est alarmée de certains rapports dont elle a eu connaissance sur de prétendus abus des moyens d'interception[45].

5.2. Conservation des données relatives au trafic

Pour pouvoir instruire et poursuivre en justice des infractions impliquant l'utilisation des réseaux de communication, notamment l'Internet, les autoritéschargées de l'application des lois se servent fréquemment des données relatives au trafic lorsqu'elles sont stockées par les fournisseurs de services aux fins de facturation. Le prix des communications étant de moins en moins lié à la distance et à la destination, et les fournisseurs de services évoluant vers une facturation forfaitaire, le besoin de stocker les données sur le trafic aux fins de facturation va tendre à disparaître. Les autorités chargées de l'application des lois craignent de voir ainsi diminuer les éléments matériels potentiellement utiles pour les enquêtes pénales et réclament par conséquent que les fournisseurs de services conservent ces données pendant une période minimum afin de leur permettre de les utiliser à des fins d'application de la loi[46].

Conformément aux directives communautaires sur la protection des données à caractère personnel, et plus précisément au principe général de limitation des transferts à une finalité spécifique énoncé dans la directive 95/46/CE et aux dispositions particulières contenues dans la directive 97/66/CE, les données relatives au trafic doivent être effacées ou rendues anonymes dès que le service de télécommunications a été fourni, sauf lorsqu'elles sont nécessaires à des fins de facturation. Dans le cas d'un accès forfaitaire ou gratuit aux services de télécommunications, les fournisseurs de services ne sont pas autorisés, en principe, à conserver les données relatives au trafic.

En vertu de ces mêmes directives, les États membres peuvent adopter des mesures législatives visant à limiter la portée de cette obligation d'effacement des données relatives au trafic lorsqu'une telle limitation constitue une mesure nécessaire, entre autres, pour la prévention, la recherche, la détection et la poursuite d'infractions pénales ou pour l'utilisation non autorisée du système de télécommunications[47].

---

45 Un rapport long et très circonstancié de M. Campbell (http://www.gn.apc.org/duncan/stoa_cover.htm) sur un réseau d'interception de l'informations appelé ECHELON a fait l'objet d'une audition publique devant le Parlement européen. Le rapport précise que le système ECHELON a été conçu pour les besoins de la sécurité nationale mais a également servi à des actions d'espionnage industriel. Le Parlement européen a constitué une commission temporaire chargée d'étudier la question et présentera un rapport d'ici un an en séance plénière.

46 Cela inclut les enquêtes pénales dans des affaires qui n'ont pas de rapport avec l'informatique ou les réseaux de communication, mais dans lesquelles ces données peuvent aider à trouver l'auteur d'une infraction.

47 Article 14 de la directive 97/66/CE et article 13 de la directive 95/46/CE.

Cependant, toute mesure législative prise à l'échelon national qui prévoirait la conservation des données relatives au trafic pour les besoins de l'application des lois devrait remplir certaines conditions. Les mesures proposées devraient en effet être appropriées, nécessaires et proportionnées au but poursuivi, comme le prévoient le droit communautaire et le droit international, notamment la directive 97/66/CE et la directive 95/46/CE, la Convention de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950 et la Convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Le respect de ces conditions et de ces principes serait d'autant plus important pour les mesures qui impliquent la conservation systématique des données sur une large fraction de la population.

Certains États membres prennent des initiatives d'ordre législatif ou réglementaire afin d'obliger ou d'autoriser les fournisseurs de services à stocker certaines catégories de données relatives au trafic, après la prestation du service considéré, qui ne sont pas nécessaires aux fins de facturation, mais sont considérées comme utiles pour des enquêtes pénales.

La portée et la forme de ces initiatives varient beaucoup selon les États, mais elles reposent toutes sur l'idée qu'il faudrait que les autorités chargées de l'application des lois puissent disposer de davantage de données que ce ne serait le cas si les fournisseurs de services ne traitaient que les données strictement nécessaires à leurs prestations. La Commission examine actuellement ces mesures au regard du droit communautaire en vigueur.

Le Parlement européen est attentif aux problèmes de protection de la vie privée et s'est généralement déclaré favorable à un haut niveau de protection des données à caractère personnel. Toutefois, lors des débats sur la lutte contre la pornographie enfantine sur l'Internet, il s'est dit partisan d'une obligation générale de conservation des données relatives au trafic pendant une période de trois mois[48].

Cet avis illustre toute l'importance du contexte dans lequel s'inscrit l'examen d'un sujet aussi sensible que celui de la conservation des données relatives au trafic et le défi auquel doivent faire face les dirigeants dans leurs efforts de recherche d'un juste équilibre.

La Commission estime que toute solution apportée au problème complexe de la conservation des données relatives au trafic doit être bien fondée, proportionnée à son objectif et concilier de manière équitable les intérêts divergents en jeu. Seule une approche qui mettrait en commun les compétences et les capacités des pouvoirs publics, des entreprises, des autorités de contrôle chargées de la protection des données et des utilisateurs permettra d'atteindre ces objectifs. Il serait tout à fait souhaitable que tous les États membres adoptent une approche cohérente sur cette question complexe, si l'on veut réaliser les objectifs d'efficacité et de proportionnalité définis et éviter de créer une situation dans laquelle les autorités chargées de l'application des lois et la communauté de l'Internet se retrouveraient face à un patchwork de cadres techniques et juridiques disparates.

Il faut prendre en considération des intérêts importants, mais assez différents. Les autorités de contrôle chargées de la protection des données sont en effet d'avis que le moyen le plus efficace de réduire des risques inacceptables pour la vie privée tout en reconnaissant la nécessité d'une application efficace de la loi voudrait que les données relatives au trafic ne

---

[48] Résolution législative portant avis du Parlement européen sur le projet d'action commune - adopté par le Conseil sur la base de l'article K.3 du traité sur l'Union européenne - relative à la lutte contre la pornographie enfantine sur Internet, amendement 17 (JO C 219 du 30.7.1999, p. 68 et notamment p. 71).

soient pas en principe uniquement conservées à des fins de respect de la loi[49]. Les autorités chargées de l'application des lois, quant à elles, déclarent que la conservation d'un volume minimum de données sur le trafic pendant une durée minimum serait nécessaire pour faciliter les enquêtes pénales.

L'intérêt des entreprises est de coopérer à la lutte contre la criminalité du type piratage ou fraude informatique, mais pas au prix de mesures d'un coût exagéré. Les incidences économiques des mesures prises en la matière doivent être analysées avec attention et comparées à l'efficacité des mesures en question dans la lutte contre la criminalité informatique, de manière à éviter de rendre l'Internet plus coûteux et moins accessible aux utilisateurs. Il faudrait assurer une sécurité suffisante des données sur le trafic qui sont ainsi conservées.

Quoi qu'il en soit, les entreprises auront un rôle clé à jouer en contribuant au processus de création d'une société de l'information plus sûre. Il faudra que les utilisateurs aient confiance dans la sécurité de la société de l'information et se sentent à l'abri des infractions et des atteintes à leur vie privée.

La Commission soutient et encourage sans réserve l'établissement d'un dialogue constructif entre les services autorités de l'application des lois, les entreprises, les autorités de contrôle chargées de la protection des données, les organisations de consommateurs et les autres parties susceptibles d'être intéressées. Dans le cadre du forum européen proposé (voir point 6.4 de la présente communication), la Commission invitera toutes les parties concernées à procéder, en priorité, à un examen approfondi de la question complexe de la conservation des données relatives au trafic en vue de trouver en commun des solutions appropriées, équilibrées et proportionnées, qui respectent intégralement les droits fondamentaux au respect de la vie privée et à la protection des données[50]. Sur la base des résultats de cet examen, elle sera à même d'évaluer la nécessité d'adopter des mesures législatives ou autres au niveau de l'Union européenne.

5.3. Accès et utilisation anonymes

Les spécialistes des questions liées à l'application des lois ont exprimé la crainte que l'anonymat ne débouche sur l'absence de responsabilité et ne fasse dangereusement obstacle à l'arrestation de certains auteurs d'infractions. L'utilisation anonyme du téléphone mobile est possible dans certains pays (et pas dans d'autres) grâce aux cartes prépayées. L'accès et l'utilisation anonymes de l'Internet sont proposés par certains fournisseurs de services ou d'accès, notamment les réexpéditeurs anonymes et les cybercafés. Le système d'attribution dynamique des adresses IP, dans lequel les adresses ne sont pas affectées aux utilisateurs à

---

49 "Une surveillance exploratoire à grande échelle ou générale doit être prohibée. [..] le moyen le plus efficace de réduire des risques inacceptables pour la vie privée tout en reconnaissant la nécessité d'une application efficace de la loi voudrait que les données relatives au trafic ne soient pas en principe uniquement conservées à des fins de respect de la loi et que les législations nationales n'obligent pas les opérateurs de télécommunications, les fournisseurs de services de télécommunications et de services Internet à conserver des données relatives au trafic pendant une période plus longue qu'il n'est nécessaire à des fins de facturation", recommandation 3/99 du 7 septembre 1999 du groupe de travail "article 29" sur la protection des données. Voir le site http://europa.eu.int/comm/internal_market/fr/media/dataprot/wpdocs/index.htm.

50 Droits consacrés par la Convention européenne des droits de l'homme (article 8, droit au respect de la vie privée), par la Charte des droits fondamentaux de l'Union européenne, par le traité sur l'Union européenne et par les directives communautaires sur la protection des données.

titre permanent mais seulement pour la durée d'une session donnée, facilite aussi un certain degré d'anonymat.

Dans leurs discussions avec la Commission, certains représentants d'entreprises se sont montrés hostiles à un anonymat total, en partie pour des raisons liées à leur propre sécurité, à la lutte contre la fraude et à l'intégrité des réseaux. Le London Internet Exchange a signalé l'existence de lignes directrices qu'il a publiées sur les meilleures pratiques en la matière et qui se sont révélées utiles au Royaume-Uni[51]. Cependant, d'autres représentants d'entreprises et des spécialistes des questions relatives au respect de la vie privée ont déclaré que, sans anonymat, il est impossible de garantir les droits fondamentaux.

Le groupe de travail Article 29 sur la protection des données a publié une recommandation sur le thème de l'anonymat sur l'Internet[52]. Il considère que la question de l'anonymat sur l'Internet se trouve au centre d'un dilemme auquel les gouvernements et les organisations internationales doivent faire face. D'une part, la possibilité de rester anonyme est essentielle si l'on veut préserver les droits fondamentaux à la vie privée et à la liberté d'expression dans le cyberespace. D'autre part, la faculté de participer à des activités et de communiquer en ligne sans révéler son identité va à l'encontre d'initiatives lancées pour soutenir d'autres activités clés d'intérêt général telles que la lutte contre le contenu illégal et préjudiciable, contre les délits financiers ou contre les atteintes au droit d'auteur. Ce conflit apparent entre différents objectifs d'intérêt général n'est certes pas nouveau. Dans le contexte des modes de communication hors ligne plus traditionnels tels que les services postaux de courrier et de colis, le téléphone, les journaux ou les services de radio et de télédiffusion, un équilibre est atteint. Le défi que doivent relever aujourd'hui les dirigeants est de veiller à ce que cette approche équilibrée, qui garantit les droits fondamentaux tout en autorisant des restrictions proportionnées dans un nombre limité de situations spécifiques, soit préservée dans le nouveau contexte du cyberespace. La portée et les limites de l'anonymat des personnes s'exprimant en ligne seront déterminantes pour cet équilibre.

Dans la déclaration de clôture de la conférence ministérielle sur les réseaux d'information globaux qui s'est tenue à Bonn du 6 au 8 juillet 1997, le principe défendu était que l'utilisateur doit pouvoir choisir de rester anonyme en ligne lorsqu'il a le même choix hors ligne. Il existe donc un consensus clair sur le fait que les activités exercées sur les réseaux doivent être envisagées en appliquant les principes juridiques de base qui s'appliquent dans d'autres domaines. L'Internet n'est pas un ghetto anarchique, sans règles sociales. Toutefois, la capacité des administrations et des pouvoirs publics de limiter les droits des particuliers et de surveiller les comportements potentiellement illicites ne doit pas être plus grande sur les réseaux publics qu'elle ne l'est sur les activités hors ligne. L'exigence selon laquelle les restrictions aux libertés et droits fondamentaux doivent être dûment justifiées, nécessaires et proportionnées par rapport à d'autres objectifs d'intérêt général, doit aussi s'appliquer dans le cyberespace.

Dans la recommandation du groupe de travail Article 29, il est indiqué de façon détaillée la manière d'y parvenir dans des cas particuliers (par exemple, en ce qui concerne le courrier électronique, les forums de discussion, etc.)[53]. La Commission se rallie aux positions exprimées par le groupe.

---

51 http://www.linx.net/noncore/bcp/ .

52 Groupe de protection des personnes à l'égard du traitement des données à caractère personnel, recommandation 3/97 - L'anonymat sur l'Internet, adoptée par le groupe le 3 décembre 1997. http://europa.eu.int/comm/internal_market/fr/media/dataprot/wpdocs/index.htm.

53 http://europa.eu.int/comm/internal_market/fr/media/dataprot/wpdocs/index.htm.

5.4. Coopération concrète au niveau international

Récemment, des opérations de répression menées conjointement au niveau mondial, telles que "Starburst" et "Cathédrale" contre des réseaux pédophiles, ont démontré qu'il est utile que les autorités chargées de l'application des lois et le pouvoir judiciaire coordonnent leur action à l'échelon international, tant par l'échange d'informations au stade préliminaire qu'en empêchant les autres membres des réseaux d'être prévenus au moment des arrestations et des saisies. L'Internet également s'est avéré un outil précieux et efficace pour les enquêtes policières et douanières, là où il est utilisé comme moyen pour commettre des infractions traditionnelles, telles que la contrefaçon et la contrebande. D'autre part, ces opérations ont aussi mis en lumière les graves difficultés juridiques et opérationnelles auxquelles se sont heurtés les autorités chargées de l'application des lois et les autorités judiciaires en conduisant cette action, telles que la préparation d'une commission rogatoire internationale et l'identification des victimes, ainsi que le rôle des organisations intergouvernementales chargées des questions de police (Interpol et Europol en particulier).

Dans le domaine des mesures concrètes de coopération internationale, les réseaux internationaux d'échanges d'informations revêtent une importance croissante pour les autorités policières et douanières.

Au sein du G8, un réseau d' accessible vingt-quatre heures sur vingt-quatre et sept jours sur sept, regroupant des points de contact compétents en matière répressive a été créé et est déjà opérationnel. Sa mission consiste essentiellement à recueillir les demandes urgentes de coopération dans des affaires faisant intervenir des preuves électroniques et d'y répondre. Ceréseau a été utilisé avec succès dans un certain nombre d'affaires. Le Conseil JAI du 19 mars 1998 a approuvé les dix principes de lutte contre la criminalité de haute technologie, adoptés par le G8, et a invité les États membres de l'Union européenne non membres du G8 à adhérer à ce réseau[54]. Ces points de contact devraient travailler en collaboration directe, ce qui complétera les structures d'entraide et les canaux de communication existants[55].

Le projet de Convention du Conseil de l'Europe prévoit également la création d'un réseau de ce type. La mention d'un réseau de points de contact fonctionnant vingt-quatre heures sur vingt-quatre et sept jours sur sept figure aussi dans la décision du Conseil relative à la lutte contre la pornographie enfantine sur l'Internet et dans la position commune de l'Union européenne concernant le projet de convention du Conseil de l'Europe sur la criminalité dans le cyberespace[56], ainsi que dans la décision du Conseil approuvant le plan d'action du G8[57], mais l'Union européenne n'a pour l'instant pas pris de mesures concrètes dans ce domaine.

---

54 Hormis les membres du G8, cinq États membres de l'Union européenne ont adhéré à ce jour au réseau du G8 fonctionnant vingt-quatre heures sur vingt-quatre et sept jours sur sept.

55 Lors du congrès mondial contre l'exploitation sexuelle des enfants à des fins commerciales, qui s'est tenu à Stockholm le 28 août 1996, des propositions ont été avancées en vue d'intégrer INTERPOL dans les réseaux cités. La décision du Conseil de l'UE relative à la lutte contre la pornographie enfantine sur l'Internet prévoit également l'intervention d'Interpol dans ce domaine.

56 Article 1er, paragraphe 4, de la position commune: "Les États membres devraient soutenir la définition de dispositions qui faciliteront la coopération internationale, notamment des dispositions concernant une entraide judiciaire aussi étendue que possible. La convention devrait faciliter la coopération rapide en matière de criminalité informatique et de criminalité assistée par ordinateur. Cette forme de coopération peut inclure la création de points de contact des autorités chargées de l'application des lois fonctionnant vingt-quatre heures sur vingt-quatre, qui complètent les structures existantes d'entraide judiciaire."

57 Disponible sur le site Internet du réseau judiciaire européen http://ue.eu.int/ejn/index.htm.

Étant donné que ce domaine requiert des compétences appropriées et une action rapide, il est urgent, selon la Commission, de mettre en application les intentions du Conseil. Pour pouvoir fonctionner de manière efficace, ce réseau devra toutefois disposer d'un personnel juridiquement et techniquement compétent, ce qui nécessitera des mesures de formation correspondantes.

Il est tout aussi nécessaire d'intensifier la coopération et l'échange d'information entre les autorités douanières. Les formes de coopération existantes devraient être améliorées et il convient de développer de nouveaux moyens pour diriger des opérations communes et échanger des informations. Eu égard aux exigences requises par la protection des données, les autorités douanières s'accordent de plus en plus sur la nécessité de constituer des réseaux d'information internationaux pour faciliter davantage les échanges d'informations. Il est également nécessaire de consentir des investissements plus importants dans ce domaine, tant en ce qui concerne la modernisation des systèmes informatiques qu'en matière de formation du personnel, afin que les autorités douanières parviennent à une plus grande efficacité dans l'exécution de leurs tâches.

5.5. Pouvoirs et compétences en matière de droit procédural

Au niveau national, et lorsque les conditions légales nécessaires sont remplies, les autorités chargées de l'application des lois doivent être en mesure de rechercher et de saisir des données stockées dans des ordinateurs assez rapidement pour empêcher la destruction des preuves de l'infraction pénale. Les autorités chargées de l'application des lois considèrent qu'elles devraient disposer de pouvoirs de coercition suffisants pour être capables, dans le cadre de leurs compétences, de procéder à des perquisitions dans des systèmes informatiques et de saisir des données, d'enjoindre à des personnes de communiquer des données informatiques déterminées, d'ordonner ou d'obtenir la conservation rapide de données précises, conformément aux garanties et procédures légales normales. À l'heure actuelle, cependant, les garanties et les procédures ne font pas l'objet d'un rapprochement.

Des problèmes risquent de se poser si, lors de leurs recherches sur un ordinateur, les autorités chargées de l'application des lois découvrent qu'un certain nombre d'ordinateurs et de réseaux répartis dans tout le pays sont impliqués. Ces questions se compliquent bien davantage si, au moment d'une perquisition sur un ordinateur ou d'une simple enquête, un service répressif constate qu'il est en train de consulter, ou qu'il doit consulter, des données localisées dans un ou plusieurs pays. Dès lors que d'importants intérêts sont en jeu au niveau de la souveraineté, des droits de l'homme et de la répression, il conviendra de les concilier au mieux.

Les instruments légaux existants en matière de coopération internationale dans des affaires pénales (entraide judiciaire) pourraient s'avérer inadaptés ou insuffisants, car leur application prend en temps normal plusieurs jours, plusieurs semaines voire plusieurs mois. Il faut créer un mécanisme par lequel, dans le cas de procédures pénales transfrontières, les états pourront, avec rapidité et efficacité, enquêter sur des infractions et recueillir des preuves ou, tout au moins, ne pas perdre des preuves importantes, d'une manière compatible avec les principes de souveraineté nationale, les droits constitutionnels et les droits de l'homme, y compris la protection de la vie privée et des données à caractère personnel.

Les nouvelles propositions envisagées par le projet de convention du Conseil de l'Europe sur la criminalité informatique pour s'attaquer à ces problèmes comprennent des injonctions en matière de conservation de données afin de faciliter des enquêtes déterminées. Toutefois, d'autres aspects, tels que les perquisitions et les saisies transfrontières comportent des questions de fond difficiles qui, pour l'instant, n'ont pas été résolues. Toutes les parties

concernées devront de toute évidence procéder à un examen plus approfondi avant que des initiatives concrètes puissent être envisagées.

Le sous-groupe du G8 chargé de la criminalité liée aux hautes technologies a débattu de la question des perquisitions et saisies transfrontalières et a obtenu un consensus sur des principes provisoires, en attendant la conclusion ultérieure d'un accord à caractère plus permanent[58]. Des questions importantes se posent toutefois, notamment sur les conditions dans lesquelles il est possible de mener des perquisitions et des saisies dans le cadre d'une procédure accélérée, avant d'en informer l'État à l'intérieur duquel celles-ci ont lieu, et des garanties appropriées devront être instituées afin que les droits fondamentaux soient respectés. Dans leur position commune concernant le projet de convention du Conseil de l'Europe sur la criminalité informatique, les ministres du Conseil de l'Union européenne ont arrêté une position ouverte[59].

Dans les affaires de criminalité informatique transfrontière, il importe également de disposer de règles explicites déterminant quel est le pays compétent pour exercer des poursuites. Il convient notamment d'éviter que l'infraction ne relève de la compétence d'aucun pays. Le projet de convention du Conseil de l'Europe propose principalement qu'un État reconnaisse sa compétence lorsque l'infraction pénale est commise sur son territoire ou par un de ses ressortissants. Lorsque plusieurs États sont compétents, les États concernés devraient se concerter afin de décider quel est le mieux à même de mener des poursuites. Ces principes sont bons, mais leur application dépendra pour beaucoup de l'efficacité des consultations bilatérales ou multilatérales. La Commission poursuivra l'examen de cette question pour déterminer si des mesures supplémentaires s'imposent au niveau de l'Union européenne.

La Commission, qui a pris part aux discussions du Conseil de l'Europe comme à celles du G8, reconnaît la complexité des questions de droit procédural et les difficultés qui s'y attachent. Il est toutefois vital qu'au sein de l'Union européenne, la lutte contre la cybercriminalité soit menée dans le cadre d'une coopération efficace, si l'on veut rendre la société de l'information plus sûre et créer un espace de liberté, de sécurité et de justice.

La Commission va poursuivre ses consultations avec toutes les parties concernées au cours des prochains mois, afin d'exploiter ces travaux. Cette question sera également examinée dans le contexte plus large de ses actions visant à mettre en œuvre les conclusions du Conseil européen de Tampere d'octobre 1999. Le Sommet de Tampere a en particulier demandé au Conseil et à la Commission d'adopter, d'ici décembre 2000, un programme de mesures destinées à mettre en œuvre le principe de reconnaissance mutuelle des décisions judiciaires. La Commission a déjà publié une communication sur la reconnaissance mutuelle des décisions finales en matière pénale[60]. Dans le cadre de sa contribution à la mise en œuvre de la partie du programme de mesures qui concerne l'exécution des injonctions préalables au procès, la Commission va examiner les possibilités de reconnaissance mutuelle de ces

---

58 Communiqué de la conférence ministérielle des pays du G8 sur la lutte contre le crime organisé transnational - Moscou, 19-20 octobre 1999 (voir http://www.usdoj.gov/criminal/cybercrime/action.htm et également http://www.usdoj.gov/criminal/cybercrime/principles.htm)

59 JO L 142, p. 2: "Sous réserve de principes constitutionnels et de garanties spécifiques destinées à assurer, comme il se doit, le respect de la souveraineté, de la sécurité, de l'ordre public ou d'autres intérêts essentiels des États, les recherches informatiques transfrontalières pour les besoins d'une enquête relative à une infraction pénale grave, à définir de manière plus précise dans la convention, peuvent être envisagées dans des cas exceptionnels, notamment en cas d'urgence, par exemple, pour éviter si nécessaire que ne soit commise une infraction risquant d'entraîner la mort ou de porter gravement atteinte à l'intégrité physique d'une personne".

60 COM(2000) 495, Bruxelles, le 26 juillet 2000.

injonctions liées à des enquêtes en matière de cybercriminalité, en vue de présenter une proposition législative en vertu du titre VI du traité sur l'Union européenne.

5.6. Force probante des données informatiques

Même lorsqu'ils ont accès à des données informatiques qui semblent constituer des preuves d'une infraction pénale, les autorités chargées de l'application des lois doivent être en mesure de les récupérer et de les authentifier, afin de pouvoir les utiliser pour des enquêtes et des poursuites pénales. Leur tâche est ardue, étant donné le caractère volatil des données électroniques et la facilité avec laquelle elles peuvent être manipulées ou falsifiées, protégées par des moyens technologiques ou détruites. Ce travail est confié aux services de recherches en matière de criminalité informatique, chargés de développer et d'utiliser des protocoles et des procédures scientifiques pour rechercher des preuves informatiques, analyser et préserver l'authenticité des données qui ont été récupérées.

L'organisation internationale des preuves informatiques (International Organisation of Computer Evidence - IOCE) a accepté, à la demande des experts du G8, d'élaborer des recommandations de normes, comprenant la définition de termes communs, de méthodes et de technologies d'identification communes et la création d'un format commun pour les demandes en matière légale. Il faudrait que l'Union européenne soit associée à ces travaux, tant au niveau des organismes des États membres spécialisés dans les enquêtes sur la criminalité informatique, qu'au niveau de la recherche et développement financée par le 5è programme-cadre (programme IST).

6. MESURES AUTRES QUE LEGISLATIVES

La mise en œuvre d'une législation appropriée au niveau national et international est nécessaire, mais ne suffit pas en soi pour lutter efficacement contre la criminalité informatique et l'utilisation frauduleuse des réseaux. Un certain nombre de conditions autres que législatives doivent compléter le cadre législatif. La plupart d'entre elles figurent dans les recommandations de l'étude COMCRIME, le G8 a proposé des conditions identiques dans son plan d'action en dix points et celles-ci ont emporté l'adhésion de toutes les parties ayant participé au processus de consultation informel qui a précédé la rédaction de la présente communication. Ces conditions comprennent:

- la création au niveau national d'unités de police spécialisées dans la lutte contre la criminalité informatique, là où elles n'existent pas encore;

- l'amélioration de la coopération entre les autorités chargées de l'application des lois, les entreprises, les organisations de consommateurs et les autorités chargées de la protection des données;

- des mesures visant à encourager les entreprises et le milieu associatif à prendre des initiatives pertinentes, y compris en matière de produits de sécurité.

Dans ce contexte, la question du chiffrement restera probablement importante. Il s'agit d'une technique indispensable pour faciliter la mise en œuvre et l'adoption de nouveaux services, y compris le commerce électronique, et il peut jouer un rôle non négligeable dans la prévention des actes délictueux sur Internet. La politique de la Commission en matière de chiffrement a

été exposée dans sa communication de 1997[61] sur la sécurité et la confiance dans la communication électronique, dans laquelle la Commissionn a déclaré qu'elle s'efforcerait de lever toutes les restrictions à la libre circulation de la totalité des produits de chiffrement au niveau de la Communauté européenne. La communication indique par ailleurs que les restrictions internes à la libre circulation des produits de chiffrement doivent être compatibles avec le droit communautaire et que la Commission examinera si ces restrictions nationales sont justifiées et proportionnées, notamment au regard des dispositions du traité relatives à la libre circulation, de la jurisprudence de la Cour de justice des Communautés européennes et des exigences des directives concernant la protection des données. Néanmoins, la Commission reconnaît que la technique du chiffrement pose aussi des problèmes nouveaux et difficiles à résoudre aux autorités chargées de l'application des lois.

La Commission se félicite par conséquent de l'adoption récente du nouveau règlement sur les biens à double usage, qui a fortement contribué à libéraliser l'accès aux produits de chiffrement, tout en admettant que ce mouvement doit aller de pair avec un renforcement du dialogue entre les utilisateurs, les entreprises et les autorités chargées de l'application des lois. La Commission a l'intention, pour sa part, d'encourager ce dialogue au niveau communautaire en proposant la création du forum de l'Union européenne. La diffusion de produits de sécurité dans l'ensemble de l'Union européenne, y compris de produits de chiffrement résistants, certifiés, au besoin, sur la base de critères d'évaluation acceptés par tous, renforcerait à la fois les possibilités de prévention d'actes criminels et la confiance des utilisateurs dans les technologies de la société de l'information.

6.1. Unités nationales spécialisées

Étant donné la complexité juridique et technique de certaines infractions informatiques, il est indispensable de constituer des unités spécialisées au niveau national. Ces unités pluridisciplinaires (autorités chargées de l'application des lois et autorités judiciaires), dotées d'un personnel bien formé, devraient être équipées d'installations techniques adéquates et fonctionner en tant que points de contact rapides, en vue:

- de répondre rapidement aux demandes de renseignements sur des infractions présumées. Il conviendra de définir des formats communs pour échanger ces renseignements, même si les discussions entre les experts du G8 ont démontré que les différences nationales en matière de cultures juridiques risquaient de rendre cette tâche difficile;

- d'agir comme interface répressive au niveau national et international pour les lignes directes[62] qui reçoivent des plaintes d'utilisateurs d'Internet signalant des contenus illicites;

- d'améliorer et/ou de développer des technologies spécialisées en matière d'investigation informatique, afin de détecter, d'instruire et de poursuivre les crimes informatiques;

---

61 COM(97) 503.

62 À ce jour, il n'existe de lignes directes que dans un nombre limité de pays. Parmi elles, citons Cybertipline aux États-Unis et Internet Watch Foundation (IWF) au Royaume-Uni, qui a mis en place, depuis décembre 1996, une ligne téléphonique et une messagerie électronique directes pour que les utilisateurs signalent des documents rencontrés sur Internet, qu'ils estiment illicites. L'IWF se prononce sur le caractère illicite du document, informe les fournisseurs de services Internet et la police. D'autres organismes de surveillance existent également en Norvège (Redd Barna), aux Pays-Bas (Meldpunt), en Allemagne (Newswatch, FSM et Jugendschutz), en Autriche (ISPAA) et en Irlande (ISPAI). Dans le cadre du programme communautaire Daphne, Childnet International mène actuellement un projet directement lié à cette question ("International Hotline Providers in Europe Forum"). De même, les experts de l'UNESCO réunis à Paris en janvier 1999 ont soutenu et encouragé la création de lignes directes nationales, leur mise en réseau ou l'établissement d'une "veille électronique" internationale.

- de jouer le rôle de centre d'excellence sur les questions de cybercriminalité en vue de partager les meilleures pratiques et les expériences.

Au sein de l'Union européenne, certains États membres ont déjà mis en place ces unités spécialisées dans la criminalité informatique. La Commission estime que la création de ces unités est une prérogative des États membres et encourage vivement ces derniers à prendre des mesures dans ce sens. Le coût que représentent l'achat des tout derniers matériels et logiciels pour ces unités ainsi que la formation de leur personnel est élevé et suppose au préalable que les pouvoirs publics, au niveau compétent, fixent des priorités et prennent les décisions politiques qui s'imposent[63]. Les expériences des unités existant déjà dans quelques États membres pourraient être particulièrement précieuses et la Commission prendra des mesures pour encourager l'échange de ces expériences.

La Commission pense également qu'Europol peut apporter une valeur ajoutée supplémentaire au niveau communautaire, par des actions de coordination, d'analyse et d'autres formes d'assistance menées auprès des unités nationales spécialisées. Elle soutiendra par conséquent l'extension du mandat d'Europol à la cybercriminalité.

6.2. Formation spécialisée

Des efforts considérables doivent être déployés dans le secteur de la formation permanente et spécialisée du personnel de police comme du personnel judiciaire. Les technologies et moyens en matière de crimes informatiques changent plus rapidement que dans les secteurs plus classiques de l'activité criminelle.

Certains États membres ont mis sur pied des initiatives pour former le personnel des autorités chargées de l'application des lois aux hautes technologies . Ils pourraient dispenser des conseils et donner des orientations aux États membres qui n'ont pas encore pris de mesures similaires.

Divers projets allant dans ce sens, qui se présentent sous la forme d'échanges d'expériences, de séminaires consacrés aux défis communs auxquels se heurtent les catégories de professionnels concernées, ont été lancés avec le soutien de programmes gérés par la Commission (en particulier, les programmes STOP, FALCONE et GROTIUS).

Celle-ci va proposer d'autres activités dans ce domaine, notamment en ce qui concerne la formation en informatique et en ligne.

Europol a pris l'initiative d'accueillir, en novembre 2000, une session de formation d'une semaine destinée au personnel des autorités chargées de l'application des lois des États membres, qui a eu notamment pour thème la pornographie enfantine. Le champ de ce type d'action pourrait être élargi de manière à englober la criminalité informatique en général. Interpol est également présente dans ce secteur depuis plusieurs années. Elle pourrait faire bénéficier un plus grand nombre de participants de ses initiatives en la matière.

---

63 En ce qui concerne l'expérience américaine dans ce domaine, voir Michael A. Sussmann "The Critical Challenges from International High-Tech and Computer-Related Crime at the Millennium", Duke Journal of Comparative and International Law, Vol. 9 printemps 1999, p. 464.

Le G8 a organisé des actions permettant l'échange d'expériences entre autorités chargées de l'application des lois et l'élaboration de technologies d'investigation communes à partir de cas concrets. Une mesure de formation supplémentaire devrait être lancée au second semestre 2001. Les États membres de l'Union européenne faisant partie du G8 pourraient partager ces expériences avec les autres États membres.

Dans le domaine de la lutte contre la pornographie enfantine sur l'Internet, plus précisément, la création et la gestion, au niveau international, d'une bibliothèque centrale numérique des images de pornographie enfantine (à laquelle les unités de police nationale spécialisées auraient accès par Internet, moyennant la mise en place des conditions et restrictions nécessaires en matière d'accès et de protection de la vie privée) faciliteraient la recherche des victimes et des coupables, contribueraient à qualifier les infractions et à former des officiers de police spécialisés[64].

6.3. Amélioration de l'information et création de règles de comptabilisation communes

L'harmonisation des règles de comptabilisation en matière policière et judiciaire ainsi que la création d'instruments adaptés pour l'analyse statistique de la criminalité informatique aideraient les autorités chargées de l'application des lois et les autorités judiciaires à améliorer le stockage, l'analyse et l'évaluation des informations officielles recueillies dans ce domaine encore mouvant.

De même, du point de vue du secteur privé, ces statistiques sont nécessaires pour apprécier correctement les risques en cause et analyser le rapport coût-bénéfice de leur gestion. Il s'agit d'une question importante, non seulement pour des raisons opérationnelles (décider, par exemple, des mesures à prendre en matière de sécurité), mais également pour des motifs d'assurance.

Une base de données contenant des textes législatifs sur la cybercriminalité, qui faisait partie de l'étude COMCRIME, est en cours d'actualisation et sera mise à la disposition de la Commission. Celle-ci envisage d'améliorer son contenu (en y incluant des législations, la jurisprudence et des publications) et son utilisation.

---

64 Dans ce contexte, le projet "Excalibur" lancé par la direction nationale suédoise des renseignements criminels avec l'aide de la Commission européenne dans le cadre du programme STOP, a donné de très bons résultats. Cette initiative a été mise sur pied en collaboration avec les forces de police allemandes, britanniques, néerlandaises et belges, conjointement avec Europol et Interpol. Il a aussi été dûment tenu compte d'autres projets entrepris par le BKA allemand (le "Perkeo") et le ministère français de l'intérieur (projet "Surfimage", cofinancé également dans le cadre du programme STOP).

6.4. Coopération entre les différents acteurs: le forum européen

L'efficacité de la coopération entre les pouvoirs publics et les entreprises, à l'intérieur du cadre légal, est considérée comme un élément fondamental de toute politique publique de lutte contre la criminalité informatique[65]. Les représentants des autorités chargées de l'application des lois ont concédé qu'ils avaient parfois manqué de clarté et de précision pour indiquer aux fournisseurs de services ce dont ils avaient besoin. Les industriels se sont montrés dans l'ensemble favorables à l'amélioration de la coopération avec les autorités chargées de l'application des lois, tout en soulignant la nécessité de trouver un juste équilibre entre la protection des libertés et droits fondamentaux des citoyens, notamment leur droit au respect de la vie privée[66], la nécessité de lutter contre la criminalité et les contraintes économiques imposées aux fournisseurs.

Les entreprises et les autorités chargées de l'application des lois peuvent, en conjuguant leurs efforts, sensibiliser le public aux risques posés par la criminalité sur l'Internet, encourager les meilleures pratiques en matière de sécurité et élaborer des instruments et des procédures efficaces de lutte contre la criminalité. Des initiatives allant dans ce sens ont déjà été prises par un certain nombre d'États membres, dont la plus ancienne et la plus ambitieuse est sans doute le forum britannique de la criminalité sur Internet (UK Internet Crime Forum)[67].

La Commission se félicite de ces initiatives et estime qu'elles doivent être encouragées dans tous les États membres. Elle a l'intention de créer un forum européen qui rassemblerait les chargées de l'application des lois, les fournisseurs de services Internet, les entreprises de télécommunications, les organisations de défense des libertés publiques, les représentants des consommateurs, les autorités chargées de la protection des données et d'autres parties intéressées, et qui aurait pour objectif d'améliorer pleinement la coopération au niveau de l'Union européenne. Dans un premier temps, les États membres nommeront des fonctionnaires, le groupe de travail Article 29 sur la protection des données désignera des experts en technologie et des spécialistes des questions relatives au respect de la vie privée, et des représentants des entreprises et des consommateurs seront choisis en étroite liaison avec leurs organisations représentatives. Ultérieurement, participeront également à ce forum des représentants d'initiatives nationales prises en la matière.

Le forum européen fonctionnera d'une manière ouverte et transparente, les documents s'y rapportant seront publiés sur un site Internet et toutes les parties intéressées seront conviées à présenter leurs observations.

---

65 Dans le communiqué adopté à Washington les 9 et 10 décembre 1997 sur les principes et le plan d'action en dix points de la lutte contre la criminalité liée aux hautes technologies, les ministres de la justice et de l'intérieur du G8 ont déclaré: "ce sont les entreprises qui conçoivent, mettent place et gèrent ces réseaux mondiaux et elles sont les principales responsables du développement des normes techniques. Il leur appartient donc de jouer leur rôle dans l'élaboration et la distribution de systèmes de sécurité conçus pour aider à déceler les cas de malveillance informatique, à préserver les preuves électroniques et pour faciliter la localisation et l'identification des auteurs d'infractions". La décision du Conseil relative à la lutte contre la pornographie enfantine sur l'Internet souligne qu'il est nécessaire que les États membres entament un dialogue constructif avec les entreprises et coopèrent avec elles en partageant leurs expériences.

66 Tel que précisé dans les directives communautaires relatives à la protection des données, la Convention du Conseil de l'Europe sur les droits de l'homme et la Convention du Conseil de l'Europe n°108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et la législation nationale correspondante.

67 Créé en 1997, le "Internet Crime Forum" regroupe des officiers de police, des fonctionnaires du ministère britannique de l'intérieur, des responsables de la protection des données et des représentants du secteur de l'Internet; ce forum tient des réunions plénières trois ou quatre fois par an et dispose d'un certain nombre de groupes de travail permanents.

Le forum européen sera invité à réfléchir, en particulier, aux actions suivantes:

- créer, s'il y a lieu, des points de contact fonctionnant vingt-quatre heures sur vingt-quatre entre les pouvoirs publics et les entreprises;

- développer un formulaire type approprié pour les demandes de renseignements adressées par les autorités chargées de l'application des lois aux entreprises, renforcer l'utilisation d'Internet par les autorités chargées de l'application des lois lorsqu'ils communiquent avec les fournisseurs de services;

- encourager l'élaboration et/ou l'application de codes de conduite et des meilleures pratiques, ainsi que leur mise en commun entre les entreprises et les pouvoirs publics[68];

- promouvoir l'échange d'informations entre les diverses parties, en particulier les entreprises et les autorités chargées de l'application des lois, sur les tendances en matière de criminalité utilisant de hautes technologies;

- examiner les préoccupations des autorités chargées de l'application des lois sur le développement des nouvelles technologies;

- encourager les avancées concernant les mécanismes d'alerte rapide et de gestion des crises pour prévenir, identifier et traiter les menaces et les perturbations sur les infrastructures de l'information;

- apporter, selon les besoins, une valeur ajoutée, en termes d'expertise, aux travaux en cours au sein du Conseil et d'autres enceintes internationales, comme le Conseil de l'Europe et le G8;

- encourager les coopérations entre les parties intéressées, comprenant les principes communs aux autorités chargées de l'application des lois, aux entreprises et aux utilisateurs (par exemple, protocole d'accord, codes de bonnes pratiques, en conformité avec le cadre légal).

6.5. Actions menées directement par les entreprises

La lutte contre la criminalité informatique est, dans une large mesure, dans l'intérêt de l'ensemble de la collectivité. Si l'on veut que les consommateurs aient confiance dans le commerce électronique, les mesures de prévention de la criminalité informatique doivent être acceptées comme un élément de bonne pratique commerciale. Dans de nombreux domaines, services bancaires, communications électroniques, cartes de crédit et droits d'auteur, les entreprises et leurs clients sont des victimes potentielles de la criminalité informatique.

Les sociétés protègent naturellement leurs propres enseignes et marques commerciales et jouent par conséquent un rôle dans la prévention de la fraude. Certains organismes représentant le secteur des logiciels et celui des phonogrammes (British Phonographic Industry, BPI, par exemple) disposent d'équipes chargées d'enquêter sur le piratage (y compris sur Internet). Dans un certain nombre d'États membres, les fournisseurs de services Internet

---

[68] Dans la mesure où il s'agit de codes de conduite au sens de l'article 27 de la directive 95/46/CE (ils pourraient traiter, par exemple, de questions relevant de la directive 97/66/CE, telles que les interceptions), le groupe de travail Article 29 sur la protection des données et les autorités de contrôle nationales chargées de la protection des données sont associés.

ont mis en place des lignes directes permettant aux utilisateurs de dénoncer les messages à contenu illicite et préjudiciable.

La Commission apporte son soutien à certaines de ces initiatives en encourageant leur participation au programme-cadre communautaire de recherche et développement, au plan d'action Internet[69] et aux programmes relevant du titre VI tels que STOP et DAPHNE.

Le forum européen permettra l'échange des meilleures pratiques dans ces domaines.

6.6. Projets de RDT financés par l'Union européenne

Le programme de RDT sur les technologies de la société de l'information (TSI), qui fait partie du 5e programme-cadre (1998 - 2002), met l'accent sur le développement et l'utilisation de technologies propres à susciter la confiance. Comme telles, ces dernières comprennent à la fois la sécurité des informations et des réseaux, ainsi que les moyens technologies et les méthodes pour se protéger contre les atteintes au droit fondamental à la protection de la vie privée et des données à caractère personnel et aux autres droits individuels, et pour lutter contre la cybercriminalité.

Le programme IST, en particulier les travaux relatifs à la *Sécurité des informations et des réseaux et autres technologies visant à susciter la confiance* figurant dans l'action clé 2 - *Nouvelles méthodes de travail et commerce électronique*, fournit un cadre permettant de développer des ressources et des techniques pour comprendre et relever les nouveaux défis technologiques liés à la prévention et à la répression de la criminalité informatique, et de garantir que les exigences en matière de sécurité et de protection de la vie privée peuvent être satisfaites aux niveaux de l'Union européenne, des communautés virtuelles et de l'individu.

En outre, afin d'aborder correctement ces problèmes de confiance, y compris la prévention et l'instruction des cas de criminalité informatique, une initiative sur la sûreté de fonctionnement a également été lancée dans le cadre du programme IST. Celle-ci vise à renforcer et à garantir la confiance dans des infrastructures informatiques très étroitement interconnectées et dans des systèmes informatiques intégrés mis en réseau, en sensibilisant aux problèmes de la sécurité de fonctionnement et en encourageant les technologies qui la rendent possible. La coopération internationale fait intégralement partie de cette initiative. Le programme IST a noué des relations de travail avec la DARPA et la NSF et créé, en collaboration avec le ministère américain des affaires étrangères, une task force conjointe sur la protection des infrastructures critiques, sous l'égide du groupe consultatif conjoint institué en vertu de l'accord de coopération scientifique et technologique Communauté européenne/États-Unis[70].

Le centre commun de recherche de la Commission (CCR), qui soutient l'initiative sur la sécurité de fonctionnement dans le cadre du programme IST, s'emploiera surtout à mettre au point, en liaison avec d'autres parties intéressées, y compris Europol, des mesures, des indicateurs et des statistiques adaptés et harmonisés. Il s'agira, par ces moyens, de classer et de comprendre correctement les activités illégales, leur répartition géographique, leur rythme de progression et l'efficacité des actions entreprises pour les combattre. Le CCR fera appel, si besoin est, à d'autres groupes de recherche et intégrera leurs travaux et leurs résultats. Il

---

69 De plus amples renseignements sur le plan d'action visant à promouvoir une utilisation plus sûre d'Internet sont disponibles à l'adresse suivante: http://158.169.50.95:10080/iap/.

70 De plus amples renseignements relatifs au programme TSI sont disponibles à l'adresse suivante: http://www.cordis.lu/ist.

gérera un site Internet sur cette question et rendra compte au forum européen des progrès accomplis en la matière.

7. CONCLUSIONS ET PROPOSITIONS

Pour prévenir la criminalité informatique et lutter efficacement contre ce phénomène, l'existence préalable d'un certain nombre de conditions est nécessaire:

- disponibilité des technologies en matière de prévention. Ceci requiert un cadre réglementaire adapté qui laisse le champ libre à l'innovation et à la recherche et les encourage. Le recours au financement public peut se justifier pour soutenir le développement et l'utilisation de technologies de sécurité appropriées;

- sensibilisation aux risques potentiels liés à la sécurité et aux moyens de les combattre;

- dispositions législatives adéquates en matière de droit positif et procédural, en ce qui concerne les activités délictueuses tant nationales que transnationales. Au niveau du droit pénal positif, les législations nationales devraient être suffisamment détaillées et efficaces pour incriminer les atteintes informatiques graves et prévoir des sanctions dissuasives, contribuer à résoudre les problèmes de double infraction[71] et faciliter la coopération internationale. Lorsqu'il est pleinement justifié que les autorités chargées de l'application des lois recherchent, saisissent et fassent rapidement une copie en toute sécurité de données informatiques à l'intérieur de leur territoire national, afin de pouvoir enquêter sur un crime informatique, le droit procédural devrait le permettre, conformément aux principes et aux exceptions prévus par le droit communautaire ainsi qu'à la Convention européenne des droits de l'homme. La Commission pense que l'accord conclu sur les dispositions en matière d'interception dans le cadre de la convention relative à l'entraide judiciaire en matière pénale représente le maximum de ce qu'il est possible d'obtenir actuellement. La Commission continuera à en contrôler l'application, avec l'aide des États membres, les entreprises et des utilisateurs, afin de garantir que les initiatives correspondantes sont efficaces, transparentes et équilibrées;

- mise à disposition d'un personnel répressif, en nombre suffisant, bien formé et correctement équipé. Une collaboration étroite avec les fournisseurs de services Internet et les entreprises de télécommunications en matière de formation sera davantage encouragée;

- renforcement de la coopération entre tous les acteurs concernés: utilisateurs et consommateurs, entreprises, autorités chargées de l'application des lois et autorités chargées de la protection des données. Cette condition est essentielle pour enquêter sur la criminalité informatique et protéger la sûreté publique. Les entreprises doivent disposer de règles et obligations clairement définies. Les pouvoirs publics doivent reconnaître que les besoins des autorités chargées de l'application des lois peuvent faire peser des contraintes sur les entreprises et, par conséquent, prendre des mesures raisonnables pour les diminuer le plus possible. Parallèlement, les entreprises devraient intégrer dans leurs pratiques commerciales des considérations de sûreté publique. La coopération et le soutien actifs de l'utilisateur et du consommateur individuels seront à cet égard de plus en plus nécessaires;

---

[71] Lorsque des enquêtes pénales nécessitent l'assistance des autorités dans d'autres pays, de nombreux systèmes juridiques posent comme condition préalable à certains types d'entraide judiciaire et à l'extradition que l'infraction soit répréhensible dans les deux pays.

- actions permanentes des entreprises et du milieu associatif. Les lignes directes, qui fonctionnent déjà pour dénoncer les contenus illicites ou préjudiciables, pourraient être étendues à d'autres catégories d'infractions. Des mesures recommandées par les industries elles-mêmes et un protocole d'accord pluridisciplinaire pourraient associer le plus grand nombre possible de parties intéressées et jouer un rôle multiple dans la prévention de la cybercriminalité et la lutte contre ce phénomène, ainsi que dans une meilleure sensibilisation et une plus grande confiance du public;

- il convient de tirer parti au maximum des résultats et des potentialités de la recherche et du développement. La stratégie consistera essentiellement à faire coïncider l'évolution des technologies de sécurité accessibles et efficaces et d'autres moyens de favoriser la confiance avec les actions entreprises au niveau communautaire.

Toutefois, toute mesure adoptée à l'avenir par l'Union européenne devrait prendre en compte la nécessité d'amener progressivement les pays candidats à participer à la coopération communautaire et internationale dans ce domaine et d'éviter qu'ils ne deviennent des refuges pour la cybercriminalité. L'association des représentants de ces pays à certaines ou à toutes les réunions communautaires sur ce sujet devra être envisagée.

Les propositions de la Commission se répartissent comme suit.

7.1. Propositions législatives

La Commission présentera des propositions législatives en vertu du titre VI du traité sur l'Union européenne:

- pour rapprocher les législations des États membres dans le domaine des infractions relatives à la pornographie enfantine. Cette initiative fera partie d'un ensemble de propositions couvrant également des problèmes plus larges liés à l'exploitation sexuelle des enfants et au trafic d'êtres humains, ainsi que la Commission l'avait annoncé dans sa communication de décembre 1998 sur la lutte contre la traite des femmes. Cette proposition sera pleinement conforme aux efforts déployés par le Parlement européen pour transformer l'initiative autrichienne en vue de l'adoption d'une décision du Conseil relative à la pornographie enfantine en une décision-cadre requérant le rapprochement des législations. Ceci est également cohérent avec les conclusions de Tampere et la stratégie de lutte contre le crime organisé définie par l'Union européenne pour le nouveau millénaire. Cette initiative figure déjà dans le tableau de bord mis en place pour la création d'un espace de liberté, de sécurité et de justice;

- pour rapprocher davantage les systèmes de droit pénal matériel dans le domaine de la criminalité utilisant de hautes technologies. Ceci pourrait englober les infractions concernant, entre autres, le piratage et les attaques par déni de service. La Commission va également étudier les possibilités de lutter contre le racisme et la xénophobie sur l'Internet afin de présenter, en vertu du titre VI du traité sur l'Union européenne, une décision-cadre s'appliquant aux activités racistes et xénophobes tant hors ligne qu'en ligne. Enfin, le problème des drogues illicites sur l'Internet sera également examiné;

- pour appliquer le principe de la reconnaissance mutuelle aux injonctions préalables au procès liées aux enquêtes en matière de cybercriminalité et faciliter les enquêtes pénales touchant à l'informatique, qui impliquent plus d'un État membre, moyennant les garanties appropriées en ce qui concerne les droits fondamentaux. Cette proposition est compatible avec les grandes lignes du programme de mesures en faveur de la reconnaissance mutuelle,

qui mentionne la nécessité d'examiner des propositions relatives à la production et à la saisie de preuves.

La Commission évaluera s'il y a lieu de prendre une initiative, en particulier de nature législative, sur la question de la conservation de données relatives au trafic, à partir, entre autres consultations, des résultats des travaux qui seront menés par le futur forum européen dans ce domaine.

7.2. Propositions autres que législatives

Des mesures sont envisagées dans un certain nombre de domaines:

- la Commission va créer et présider un forum européen regroupant des autorités chargées de l'application des lois, des fournisseurs de services, des opérateurs de réseaux, des associations de consommateurs et des autorités chargées de la protection des données, dans le but d'intensifier la coopération au niveau communautaire en sensibilisant le public aux risques que pose la criminalité sur Internet, de promouvoir les meilleures pratiques en matière de sécurité informatique, de développer des instruments et des procédures efficaces pour lutter contre la criminalité informatique, ainsi que d'encourager les avancées dans les mécanismes d'alerte rapide et de gestion des crises. Il s'agira d'une version communautaire de forums similaires qui fonctionnent avec succès dans certains États membres. La Commission incitera les États membres qui n'en disposent pas à en créer. La structure communautaire encouragera et facilitera la coopération entre ces divers forums;

- la Commission va continuer à œuvrer en faveur de la sécurité et de la confiance dans le cadre de l'initiative *e*Europe, du plan d'action Internet, du programme IST et du prochain programme-cadre de RDT. Ces actions consisteront notamment à faciliter la mise à disposition de produits et de services présentant un niveau de sécurité satisfaisant et à encourager la libéralisation de l'usage du chiffrement résistant par un dialogue entre toutes les parties intéressées;

- la Commission va lancer d'autres projets dans le cadre de programmes existants pour soutenir la formation du personnel répressif sur les questions relatives à la criminalité utilisant de hautes technologies et la recherche en matière de criminalité informatique;

- la Commission envisage de financer des mesures destinées à améliorer le contenu et l'utilisation de la base de données des législations nationales des États membres fournie par l'étude COMCRIME; elle va en outre lancer une étude pour avoir une vision plus précise de la nature et de l'ampleur de la criminalité informatique dans les États membres.

7.3 Actions menées au sein d'autres enceintes internationales

La Commission continuera à jouer pleinement son rôle en veillant à ce que les États membres coordonnent leur action dans d'autres enceintes internationales où la question de la cybercriminalité est examinée, telles que le Conseil de l'Europe et le G8. Les initiatives que prendra la Commission au niveau de l'Union européenne tiendront dûment compte des progrès réalisés au sein d'autres enceintes internationales, tout en s'attachant à rapprocher les positions à l'intérieur de l'Union européenne.

* * * * *

FICHE FINANCIÈRE

1. INTITULE DE L'ACTION

« Créer une société de l'information plus sûre en renforçant la sécurité des infrastructures d'information et en luttant contre la cybercriminalité ».

2. LIGNE(S) BUDGETAIRE(S) CONCERNEE(S)

B5 302

B5 820

B6 1110, B6 2111, B6 1210

3. BASE JURIDIQUE

Articles 95, 154 et 155 du traité CE et articles 29 et 34 du traité UE.

4. DESCRIPTION DE L'ACTION

4.1 Objectif général de l'action

La Commission a l'intention de créer et de présider un forum de l'Union européenne, qui rassemblera les services de police, les fournisseurs de services internet, les entreprises de télécommunications, les organisations de défense des libertés publiques, les associations de consommateurs, les autorités chargées de la protection des données et toute autre partie intéressée, dans le but d'améliorer la compréhension mutuelle et d'intensifier la coopération au niveau communautaire. Ce forum s'efforcera de sensibiliser le public aux risques liés à la criminalité sur l'Internet, de promouvoir les meilleures pratiques en matière de sécurité informatique, de définir des outils et des procédures efficaces afin de lutter contre la délinquance informatique, ainsi que d'encourager les avancées en matière de mécanismes d'alerte rapide et de gestion des crises. Les documents s'y rapportant seront publiés sur un site web.

4.2 Période couverte par l'action et modalités prévues pour son renouvellement

Le programme est prévu pour une durée de deux ans (2001-2002). L'opportunité de poursuivre le forum sera examinée en 2002.

5. CLASSIFICATION DE LA DEPENSE/RECETTE

5.1. DNO (dépense non obligatoire)

5.2. CD (crédit dissocié)

6. TYPE DE LA DEPENSE/RECETTE

Réunions: remboursement des frais de déplacement des experts			
B5 302A	2001		27 000 euros
B5 302A	2002		40 500 euros
Gestion du forum et d'un site web			
B6 1110	2001	Missions du JRC	10 000 euros
B6 2111	2001	Frais spécifiques du JRC (divers)	15 000 euros
B6 1210	2001	Frais généraux JRC	50 000 euros
B6 1110	2002	Missions JRC	10 300 euros
B6 2111	2002	Frais spécifiques du JRC (divers)	15 450 euros
B6 1210	2002	Frais généraux JRC	51 500 euros
Études sur des questions spécifiques			
B6 2111	2001	Frais spécifiques du JRC (études)	25 000 euros
B6 2111	2002	Frais spécifiques du JRC (études)	25 750 euros
Total	2001 + 2002		270 500 euros

7. INCIDENCE FINANCIERE

Mode de calcul du coût total de l'action (lien entre les coûts individuels et le coût total):

Remboursement des frais de déplacement des participants aux réunions, lesquelles devraient être au nombre de deux en 2001 et de trois en 2002. Un remboursement sera accordé à 15 experts par réunion. Le coût moyen des remboursements est estimé à 900 euros par personne.

Les coûts d'infrastructure et d'aide administrative et technique, en termes tant de personnel que de frais spécifiques, sont proportionnels au nombre de postes affectés aux activités concernées. Le budget consacré aux études est calculé sur la base de deux études par an représentant environ un mois-personne chacune.

8. DISPOSITIONS ANTI-FRAUDE PREVUES

Contrôles de routine. Aucune autre disposition anti-fraude n'est envisagée.

9. ÉLEMENTS D'ANALYSE COUT-EFFICACITE

9.1. Objectifs spécifiques quantifiables, population visée

Améliorer la compréhension mutuelle et intensifier la coopération au niveau communautaire entre les différents groupes d'intérêts. Sont visés les services de police, les fournisseurs de services internet, les entreprises de télécommunications, les organisations de défense des libertés publiques, les associations de consommateurs, les autorités chargées de la protection des données, ainsi que toute autre partie intéressée.

9.2. Justification de l'action

Le forum a pour objectif d'améliorer la compréhension mutuelle et d'intensifier la coopération au niveau communautaire entre les différents groupes d'intérêts. Il s'efforcera de sensibiliser le public aux risques que pose la criminalité sur l'Internet, de promouvoir les meilleures pratiques en matière de sécurité informatique, de développer des instruments et des procédures efficaces pour lutter contre la délinquance informatique, ainsi que d'encourager les avancées dans les mécanismes d'alerte rapide et de gestion des crises.

9.3. Suivi et évaluation de l'action

La Commission organisera et présidera les réunions du forum et prendra part aux débats. Elle gérera le site web se rapportant audit forum. Elle examinera en 2002 s'il convient de le maintenir en 2003 et au-delà.

10. DEPENSES ADMINISTRATIVES

Les besoins en ressources humaines et administratives seront couverts par le personnel existant.

10.1. Incidence sur le nombre d'emplois

Types d'emplois	Effectifs à affecter à la gestion de l'action		dont		Durée
	emplois permanents	emplois temporaires	par utilisation des ressources existantes au sein de la DG	par recours à des ressources supplémen-taires	
Fonctionnaires A ou agents B temporaires C	 0,05	1,75 0,15	1,75 0,15 0,05		Par an pendant 2 ans
Autres ressources					
Total	0,05	1,9	1,95		

10.2. Incidence financière globale des ressources humaines

	Montants	Mode de calcul (2001 -2002)
Fonctionnaires	421 200 euros	2 ans x 108 000 euros x 1,95 poste