Document
mis en distribution
le 17 décembre 2004

N° 1978

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

DOUZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 8 décembre 2004.

RAPPORT

FAIT

AU NOM DE LA COMMISSION DES AFFAIRES ÉTRANGÈRES SUR LE PROJET DE LOI n° 905 *autorisant l'approbation de la* **convention** *sur la* **cybercriminalité**,

PAR M. JEAN–MARC NESME,

Député

SOMMAIRE

—

Pages

Mesdames, Messieurs,

L'Assemblée nationale est saisie du projet de loi autorisant l'approbation de la convention sur la cybercriminalité (projet n° 905). Cette convention a été adoptée dans le cadre du Conseil de l'Europe à Budapest le 23 novembre 2001 et signée par la France le jour même. Le projet de loi s'y rapportant a été déposé à l'Assemblée nationale le 11 juin 2003.

Le Conseil de l'Europe a par ailleurs adopté le 7 novembre 2002 un protocole additionnel à la convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques. Ce protocole additionnel a été ouvert à la signature le 28 janvier 2003, date à laquelle il a été signé par la France.

Alors que l'Assemblée nationale avait été saisie de la convention de base, le Gouvernement a choisi de déposer le projet de loi autorisant l'approbation du protocole additionnel s'y rapportant au Sénat (projet n° 182, session ordinaire 2003-2004). Pour des raisons de cohérence et de lisibilité du travail parlementaire, votre Rapporteur propose de joindre l'examen de la convention et du protocole additionnel, dont il présentera ici le contenu. Une telle démarche permettra par ailleurs aux pouvoirs publics français d'approuver plus rapidement les deux textes qui nous sont soumis et dont l'essentiel des stipulations ont d'ores et déjà été introduites dans notre droit interne.

I – LA CYBERCRIMINALITE : UN PHENOMENE GRAVE QUI APPELLE DES REPONSES FORTES DES POUVOIRS PUBLICS

A - Eléments de définition

La cybercriminalité peut se définir comme l'ensemble des infractions pénales commises sur le réseau internet. Elle correspond à trois catégories distinctes d'infractions : les infractions de contenu, les atteintes à la propriété intellectuelle et les infractions informatiques.

Les **infractions de contenu** correspondent à la diffusion intentionnelle par internet de textes ou d'images contraires à la loi. On range parmi ces infractions, la diffusion de matériels, d'insultes, de menaces ou de considérations de nature raciste, xénophobe ou négationniste. Y figurent également les infractions pédopornographiques.

Internet constitue par ailleurs un moyen privilégié pour porter **atteinte à la propriété intellectuelle** par le vol ou la copie de contenus et de procédés. Les sites mettant en ligne des fichiers musicaux gratuits sans l'accord des auteurs, des interprètes ou des producteurs constituent une illustration de ce type d'infractions.

La cybercriminalité recoupe également l'ensemble des **infractions informatiques**. Celles-ci concernent les atteintes délibérées aux réseaux informatiques, à l'intégrité et à la disponibilité des données, les accès illicites ou les interceptions de données, ainsi que l'entrave au fonctionnement des systèmes. Enfin, ces infractions concernent aussi la diffusion de programmes tels que les virus ou les chevaux de Troie, ainsi que les trafics relatifs aux mots de passe ou aux codes d'accès.

Cette liste n'est pas exhaustive dans la mesure où internet peut également être utilisé pour préparer des opérations criminelles, qui auraient tout aussi bien pu être préparées au moyen d'autres modes de communication. Enfin, certaines escroqueries sont facilitées par l'internet, comme par exemple les fraudes aux cartes bancaires ou le recueil frauduleux des données bancaires. Aussi, les services de police judicaire français opèrent une classification des actes de cybercriminalité en distinguant les infractions spécifiques aux technologies de l'information et de la communication, les infractions liées à ces technologies et celles qui sont facilitées par elles.

Parmi les **infractions spécifiques aux technologies de l'information et de la communication**, on trouve les atteintes aux systèmes de traitement automatisé de données, les atteintes aux traitements de données à caractère personnel, les infractions aux cartes bancaires, le chiffrement non autorisé ou non

déclaré, ainsi que les interceptions des correspondances émises par voie de télécommunication.

S'agissant des **infractions liées aux technologies de l'information et de la communication**, elles concernent la pédopornographie, les infractions à la loi sur la presse (racisme, négationnisme, provocation aux crimes et délits), les atteintes aux personnes et aux biens.

Enfin, les **infractions dont la commission est facilitée par l'utilisation des technologies de l'information et des communications** comprennent les escroqueries en lignes, les atteintes à la propriété intellectuelle, les jeux de hasard, les atteintes aux personnes et aux biens.

La cybercriminalité, qui est en plein développement, concerne donc un nombre extrêmement varié d'infractions. Alors que le nombre d'internautes est estimé à 25 millions en France aujourd'hui, il est essentiel de pouvoir les protéger des atteintes rendues possibles par le réseau. De même, les entreprises et les services publics doivent être prémunis face aux dangers de la cybercriminalité, dont le coût est potentiellement exorbitant.

A l'heure actuelle la France se dote d'instruments statistiques spécifiques pour pouvoir comptabiliser cette délinquance d'un nouveau type. A titre d'exemple, en 2003, 464 faits de pédopornographie et 156 faits de haine raciale ont été constatés.

B - Les institutions chargées de lutter contre la cybercriminalité

1) Au niveau national

La cheville ouvrière de la lutte contre la cybercriminalité est l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), créé par un décret du 15 mai 2000. Rattaché à la direction générale de la police nationale au sein de la direction de la police judiciaire, cet office a succédé à la Brigade centrale de Répression informatique.

Comme les autres offices centraux spécialisés (répression du banditisme, lutte contre le trafic de stupéfiants, lutte contre la délinquance financière, le faux monnayage…), il a une compétence nationale et une vocation interministérielle. Ses interlocuteurs privilégiés sont la Brigade d'enquête sur les fraudes aux technologies de l'information (rattachée à la Préfecture de police de Paris), la DST, la Gendarmerie nationale et les douanes.

L'Office est investi d'une double mission:

— au niveau opérationnel, il réalise des enquêtes judiciaires de haut niveau ou fournit une assistance technique à l'occasion d'enquêtes judiciaires menées par d'autres services ;

— au niveau stratégique, il forme, anime et coordonne les services répressifs compétents en matière d'infractions liées aux technologies de l'information et de la communication ; il est par ailleurs le point de contact pour la coopération policière internationale.

L'Office dispose d'un effectif de 35 policiers et de 3 gendarmes. A l'échelon territorial, les services de Police judiciaire disposent de 51 enquêteurs spécialisés en criminalité informatique (ESCI). Les services de gendarmerie ont pour leur part un effectif de 50 enquêteurs « N-TEC » dans les sections de recherche. Les services territoriaux ont la possibilité de confier les expertises informatiques les plus complexes à la police technique et scientifique ou à l'Institut de recherche criminelle de la gendarmerie nationale (IRCGN).

Les pouvoirs publics français ont entrepris un important effort en matière de lutte contre la cybercriminalité et le doublement des effectifs des enquêteurs est envisagé. L'harmonisation des matériels utilisés par la police et par la gendarmerie constitue par ailleurs un enjeu très important et il convient d'y consacrer les moyens nécessaires.

2) Au niveau international et européen

La coopération policière internationale est réglée par l'accès à des centres de ressources qui fournissent une aide à l'enquêteur. Ces centres ont notamment pour finalité de coordonner l'action des services répressifs internationaux et de leur apporter toute l'assistance utile en terme de rapprochement, de recherches et d'échanges d'informations. Ils facilitent en outre la lutte contre le crime et la délinquance en offrant leur expertise aux services d'enquête et en mutualisant les ressources. Cette coopération est mise en œuvre au moyen des outils suivants : Interpol, Europol, Schengen et Eurojust.

— Interpol :

En 1946, la conférence de Bruxelles a fait renaître la communauté internationale de police criminelle créée en 1929 en adoptant un nouveau statut. Les buts de l'OIPC-Interpol (Organisation internationale de police criminelle) sont d'assurer et de développer l'assistance réciproque des autorités de police judiciaire dans le cadre des lois existant dans les divers pays et dans l'esprit de la Déclaration Universelle des Droits de l'Homme, d'établir et développer toutes les

institutions capables de contribuer efficacement à la prévention et à la répression des infractions de droit commun.

L'OIPC - Interpol ne dispose pas de pouvoirs supranationaux pour effectuer des missions opérationnelles. En revanche, elle coordonne les polices des Etats membres, agissant à la fois comme fournisseurs et demandeurs d'informations et de services. Elle met également en œuvre des échanges d'expérience et définit des principes d'action communs, organise des sessions de formation ou encore élabore des guides recensant les meilleures pratiques.

Afin d'apporter un soutien immédiat aux enquêteurs chargés de mener des investigations sur une ou plusieurs infractions perpétrées sur ou au moyen d'Internet, Interpol a décidé la mise en œuvre de points de contact fonctionnant 24 heures sur 24 et 7 jours sur 7 dans les services de police des Etats associés.

Au sein de l'Union européenne le rôle d'Interpol est limité, puisque les canaux Schengen et Europol sont privilégiés par les Etats membres. Interpol n'est donc en général sollicité que pour les affaires ayant une relation avec un ou plusieurs Etats situés en dehors de l'espace de l'Union européenne. Pour autant, il n'existe pas de clivage entre Europol et Interpol et des relations étroites ont été tissées entre les deux structures. Le sous-groupe haute technologie du groupe de Lyon existant au sein du G8 constitue également un lieu de réflexion et d'orientation des politiques de sécurité des Etats. Son influence n'est pas négligeable au sein des instances internationales.

— Europol :

L'office européen de police Europol dont l'organisation et les missions sont prévues par la convention du 26 juillet 1995, est chargé du traitement des renseignements relatifs aux activités criminelles au sein de l'Union européenne. Il constitue un point central de coordination et de coopération chargé de soutenir les services enquêteurs afin de rationaliser leurs efforts et compléter leurs moyens en matière de prévention et de lutte contre les formes graves de criminalité internationale organisée. Europol intervient en facilitant l'échange d'informations, en fournissant des analyses opérationnelles et stratégiques, en apportant son expertise et son assistance techniques aux enquêtes.

Europol dispose d'un système d'informations qui n'a pas encore atteint sa pleine maturité. A ce titre, un fichier d'analyse concernant la pédophilie sur Internet a été créé. Par ailleurs, les échanges directs et rapides de données peuvent également intervenir entre les officiers de liaison des Etats membres. Pour traiter les dossiers, les services répressifs de l'Union européenne pourront à l'avenir constituer des équipes conjointes et mener des actions spécifiques d'enquête, y compris des actions opérationnelles conjointes, comprenant en appui des représentants d'Europol. Dans l'immédiat, les équipes communes d'enquête n'ont toujours pas été mises en œuvre.

— Schengen :

Le système d'information Schengen permet l'échange d'informations entre les Etats signataires et la consultation automatisée de données sur les personnes, les véhicules terrestres et les objets signalés. La coopération entre les Etats de l'Union porte sur l'assistance mutuelle aux fins de la prévention et de la recherche de faits punissables, ainsi que l'intensification de la coopération policière dans les régions frontalières.

Pour assurer une meilleure sécurité de l'espace Schengen par suite de l'absence de la Suisse des instances de coopération Schengen, un accord de coopération policière judiciaire et douanière a été signé entre la France et la Suisse en mars 1998.

— Eurojust :

Eurojust a été intégré au traité de l'Union européenne par le conseil européen de Nice en décembre 2000. Il s'agit d'une unité de coopération opérationnelle chargée de lutter contre toutes les formes de criminalité. Organe de l'Union européenne, il est chargé de promouvoir et d'améliorer la coordination et la coopération entre les autorités judiciaires compétentes des Etats membres. Il peut demander aux Procureurs nationaux de faire procéder à une enquête ou de faire engager des poursuites, de dénoncer des infractions aux autorités compétentes d'un autre Etat membre, de participer à la mise en place d'équipes communes d'enquête. Eurojust peut également s'appuyer sur le mandat d'arrêt européen pour obtenir l'extradition rapide de criminels recherchés par un Etat membre de l'Union.

II – DE NOUVEAUX INSTRUMENTS DE DROIT INTERNATIONAL

A - La convention sur la cybercriminalité

Le Conseil de l'Europe a adopté une première recommandation sur la criminalité informatique en 1989, suivie en 1995 d'une seconde, consacrée aux aspects procéduraux. Ces textes recommandaient l'élaboration d'une convention internationale sur la cybercriminalité. Le conseil de l'Europe a élaboré cette convention entre 1997 et 2000. Ouverte à la signature le 23 novembre 2001, elle constitue le premier texte de droit international visant à garantir la sécurité du réseau internet et de ses utilisateurs.

Trente huit Etats européens ont participé à la négociation de la convention. Parallèlement, le G 8 s'est saisi de cette question et a adopté le 21 juillet 2000 la Charte d'Okinawa sur la société mondiale de l'information, qui affirme la nécessité d'une co-régulation face au développement des nouvelles technologies de l'information et de la communication. Cette convergence du Conseil de l'Europe et du G 8 a abouti à la participation des Etats-Unis, du Japon et du Canada aux travaux du Conseil de l'Europe sur la cybercriminalité. L'Afrique du Sud s'est également jointe aux négociations. Ces quatre pays ont signé la convention le 23 novembre 2001 aux côtés de 34 des 46 membres du Conseil de l'Europe.

Les objectifs de la Convention sont les suivants :

— l'harmonisation des éléments des infractions ayant trait au droit pénal matériel national et les dispositions connexes en matière de cybercriminalité ;

— la modification des procédures pénales en vigueur dans les Etats, afin de leur donner les pouvoirs nécessaires à l'instruction et à la poursuite d'infractions de ce type, ainsi que d'autres infractions commises au moyen d'un système informatique ou pour lesquelles les preuves existent sous forme électronique ;

— la mise en place d'un régime rapide et efficace de coopération internationale.

La convention définit tout d'abord les notions de « système informatique », de « données informatiques », de « fournisseurs de services » et de « données relatives au trafic ». Elle ne définit en revanche pas la notion de cybercriminalité, laissant ainsi aux Etats le soin de le faire dans leurs législations.

La convention invite les Parties à prendre les mesures nécessaires pour donner une qualification pénale à différentes infractions ressortant de la criminalité informatique. Elle définit les infractions suivantes : accès illégal, interception illégale, atteinte à l'intégrité des données, atteinte à l'intégrité du système, abus de dispositifs, falsification informatique, fraude informatique, infractions se rapportant à la pornographie enfantine et infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes.

En matière de procédure, la Convention énonce les mesures que les Parties doivent prendre. Il s'agit de la conservation rapide de données stockées dans un système informatique, de la conservation et de la divulgation rapides de données relatives au trafic, de l'injonction de produire, de la perquisition et saisie de données informatiques stockées, de la collecte en temps réel des données relatives au trafic et de l'interception de données relatives au contenu.

La Convention définit ensuite les dispositions relatives à l'entraide entre Etats, ainsi que les règles d'extradition. Pour permettre aux Etats de faire connaître leurs demandes et afin d'y répondre avec célérité, la convention a prévu, en plus des voies de communication traditionnelles, un réseau de points de contact disponibles 24 heures sur 24 et 7 jours sur 7. Pour la France, ce service est géré par l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication de la direction générale de la police nationale.

Enfin, les clauses finales de la convention sont conformes aux dispositions types des Traités émanant du Conseil de l'Europe. Pour entrer en vigueur, le texte doit avoir été ratifié par cinq Etats, dont au moins trois membres du Conseil de l'Europe. A ce jour, la convention a été ratifiée par **l'Albanie, la Croatie, l'Estonie, la Hongrie, la Lituanie, l'ex-République yougoslave de Macédoine, la Roumanie, et la Slovénie**. Celle-ci est entrée en vigueur le 1er juillet 2004. Sur les 38 Etats signataires de la Convention, 30 n'ont à ce jour pas déposé leurs instruments de ratification. Il importe donc que la France soit en mesure de le faire rapidement.

Enfin, il est à noter que les Etats suivants n'ont toujours pas signé la Convention : **Andorre, l'Azerbaïdjan, la Bosnie-Herzégovine, la Géorgie, le Liechtenstein, Monaco, la République Tchèque, la Russie, Saint-Marin, La Serbie-Montenegro, la Slovaquie et la Turquie**.

B - Le protocole additionnel relatif à l'incrimination d'actes racistes et xénophobes

Lors de la négociation de la convention sur la cybercriminalité, les délégations des Etats-Unis, du Canada et du Japon, se sont opposées à l'incrimination des comportements racistes et xénophobes sur internet. Les Etats-Unis ont pour leur part considéré qu'une telle incrimination contreviendrait au premier amendement de leur Constitution qui garantit la liberté d'expression. Afin de dépasser ce blocage, la France a demandé que soit négocié de manière séparée un protocole additionnel portant sur l'incrimination des actes de nature raciste et xénophobe commis par le biais de systèmes informatiques. Ce protocole a été ouvert à la signature par le Conseil de l'Europe en janvier 2003.

L'objet du protocole est de mettre en place une approche coordonnée entre Etats, afin de lutter contre la diffusion de matériels racistes et xénophobes sur les réseaux informatiques. Faute d'une telle approche, les législations nationales en vigueur risquent en effet d'être contournées en permanence. A cette fin, le protocole vise à harmoniser le droit pénal matériel en vigueur dans les différents Etats Parties. Il leur permet également d'utiliser les moyens procéduraux mis en œuvre en application de la convention sur la cybercriminalité.

Le protocole définit la notion de « matériel raciste et xénophobe », comme « *tout matériel écrit, toute image ou toute autre représentation d'idées ou de théories qui préconise ou encourage la haine, la discrimination ou la violence, contre une personne ou un groupe de personnes, en raison de la race, de la couleur, de l'ascendance ou de l'origine nationale ou ethnique, ou de la religion, dans la mesure où cette dernière sert de prétexte à l'un ou l'autre de ces éléments ou qui incite à de tels actes.* »

Cette définition permet de compléter utilement l'article 10 de la Convention européenne des droits de l'Homme, qui reconnaît le droit à la liberté d'expression, ce qui inclut la liberté d'avoir une opinion et de recevoir et de transmettre des informations et des idées. Comme l'a précisé la Cour dans sa jurisprudence cet article « *vaut non seulement pour les "informations" ou "idées" accueillies avec faveur ou considérées comme inoffensives ou indifférentes, mais aussi pour celles qui heurtent, choquent ou inquiètent l'Etat ou une fraction quelconque de la population*[1] ». Toutefois, la Cour a établi que les actions des Etats visant à restreindre le droit à la liberté d'expression étaient justifiées au regard du paragraphe 2 de l'article 10, notamment lorsque ces idées et ces expressions portent atteinte aux droits des tiers. Le Protocole additionnel établit dans quelle mesure la diffusion d'expressions et d'idées racistes et xénophobes porte atteinte aux droits des individus.

[1] Voir l'arrêt de la CEDH, *Handyside,* du 7 décembre 1976

Le texte définit ensuite la liste des faits qui doivent faire l'objet d'une incrimination au niveau national : la diffusion de matériel raciste et xénophobe par internet ; la menace avec une motivation raciste et xénophobe ; l'insulte avec une motivation raciste et xénophobe ; la négation, la minimisation grossière, l'approbation ou la justification du génocide ou des crimes contre l'humanité ; l'aide et la complicité à perpétrer les infractions énumérées par le protocole.

Le protocole prévoit expressément la possibilité pour les Parties de mettre en œuvre les procédures prévues par la convention sur la cybercriminalité, comme la perquisition en ligne, la conservation rapide de données informatiques stockées ou la collecte en temps réel de données informatiques. Il prévoit également l'application des mécanismes d'entraide judiciaire prévus par la Convention.

A ce jour, 23 Etats ont signé le protocole et seuls **l'Albanie et la Slovénie** ont procédé à sa ratification. Il est à noter que plusieurs membres de l'Union européenne n'ont pas signé le protocole : **Chypre, l'Espagne, la Hongrie, l'Irlande, l'Italie, la Lituanie, la République Tchèque, le Royaume Uni et la Slovaquie**. Pour entrer en vigueur, il doit avoir été ratifié par cinq Etats. Une ratification rapide de ce protocole par la France s'impose d'autant plus, qu'elle est à l'origine du texte ; elle constituerait par ailleurs un signal pour obtenir un plus grand nombre de signatures.

III – D'IMPORTANTES REFORMES LEGISLATIVES

La France n'a pas attendu l'entrée en vigueur de la convention sur la cybercriminalité et du protocole additionnel pour mettre en place un arsenal législatif adapté aux enjeux de la cybercriminalité. Les problèmes les plus importants qui se posent demeurent liés à l'application de la loi française dans l'espace et devraient être résolus par la convention sur la cybercriminalité.

A - Les instruments nationaux en matière de lutte contre la cybercriminalité

Depuis 1997 les pouvoirs publics ont procédé à d'importantes réformes améliorant les instruments de lutte contre la cybercriminalité. Le législateur est ainsi intervenu à plusieurs reprises dans ce domaine avec la loi n° 2001-1062 du 15 novembre 2001 pour la sécurité quotidienne, la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure, la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique et la loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité. Parmi les mesures adoptées figurent des dispositifs de droit pénal spécial, de procédure pénale et de droit pénal général destinées à lutter contre la criminalité en facilitant les investigations judiciaires.

1) Le droit pénal spécial

Le code pénal français incrimine les infractions suivantes :

— le non respect de la confidentialité, de l'intégrité et de la disponibilité des données et systèmes informatiques (articles 323-1 à 323-7 du code pénal) ;

— les infractions se rapportant à la pornographie enfantine (articles 227-22 à 227-24 du code pénal) ; par ailleurs, le code pénal sanctionne plus gravement le viol (article 222-24) et les agressions sexuelles autre que le viol (222-28), lorsque la victime a été mise en contact avec l'auteur des faits grâce à un réseau de télécommunication ;

— les infractions de nature raciste et xénophobe (Loi de 1881 sur la presse, articles 24 alinéa 6 et 32 alinéa 2) ; cette loi prévoit des règles procédurales dérogatoires au droit commun notamment en matière de prescription, de responsabilité pénale et de nullité, afin de préserver la liberté d'expression.

Pour sa part, le code de la propriété intellectuelle réprime les infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes.

Par ailleurs, des mesures nouvelles portant à la fois sur l'aggravation des peines, la mise en œuvre d'incriminations et la prise en compte de circonstances aggravantes sont venues renforcer le dispositif existant. La peine est désormais aggravée dans les cas suivants : utilisation d'un moyen de cryptologie pour faciliter, préparer ou commettre un crime ou un délit ; absence de réponse à une réquisition dans les meilleurs délais ; contrefaçon ; jeux de hasard ; atteintes aux systèmes automatisés de données.

La loi pour la confiance dans l'économie numérique modifie partiellement les dispositions de l'article 227-23 du code pénal. Le premier alinéa de cet article punit désormais de 3 ans et de 45 000 euros d'amende le fait de fixer, d'enregistrer ou de transmettre l'image de la représentation d'un mineur en vue de sa diffusion, lorsque cette image ou cette représentation présente un caractère pornographique. Sera dorénavant punie des mêmes peines la tentative de commettre ces mêmes faits. En outre, le deuxième alinéa de l'article 227-23 punit des mêmes peines la diffusion, l'importation et l'exportation, directe ou indirecte, de l'image d'un mineur présentant un caractère pornographique. Le fait d'offrir de telles images est également puni des mêmes peines. Cette modification est destinée à mettre en conformité le droit français avec les dispositions de la convention du conseil de l'Europe sur la cybercriminalité et des articles 3 et 4 de la décision –cadre du conseil européen du 22 décembre 2003 relative à la lutte contre l'exploitation sexuelle des enfants et de la pédopornographie.

Le législateur a également créé de nouvelles infractions, comme la diffusion de procédés permettant la fabrication d'engins de destruction par l'utilisation d'un réseau de télécommunication. Il a de plus renforcé la loi dite Godfrain (article 323-3-1 du code pénal) en vue de réprimer l'importation, la détention, l'offre, la cession ou la mise à disposition sans motif légitime d'équipements, instruments, ou programmes informatiques destinés à permettre une intrusion dans un système automatisé de données.

Enfin, la loi sanctionne toute personne physique ou morale qui n'aurait pas respecté les dispositions portant sur les règles de mise en œuvre, d'acquisition, et de mise à disposition de moyens de cryptologie.

2) Le droit pénal général

Les articles L 32-3-1 et L 32-3-2 du code des Postes et télécommunications disposent que les opérateurs de télécommunication ont une obligation d'effacer ou de rendre anonyme toutes données techniques relatives à une communication. Ce principe général connaît trois exceptions qui concernent :

— d'une part les données techniques nécessaires à la facturation et au paiement des prestations de télécommunications permettant la conservation facultative dans la limite d'un an qui correspond au délai de prescription prévu par l'article 126 du code des postes et télécommunications ;

— les données techniques susceptibles d'être utilisées pour la recherche, la constatation et la poursuite des infractions pénales, pour une durée maximale d'un an ; elles ne pourront en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit.

— la conservation des données de connexion pour des questions de sécurité informatique.

Les données techniques concernées au titre de ces deux lois doivent faire l'objet d'une définition par décret en Conseil d'Etat pris après avis de la commission nationale de l'informatique et des libertés. les fournisseurs d'accès et hébergeurs sont par ailleurs tenus de vérifier, de détenir et de conserver les données de nature à permettre l'identification de quiconque ayant contribué à la création d'un contenu. L'autorité judiciaire peut requérir la communication de ces informations.

La convention sur la cybercriminalité prévoit la conservation des données de trafic *a posteriori* et non *a priori*. Une telle mesure semble insuffisante dans la mesure où très souvent ce sont les investigations qui vont conduire l'enquêteur à solliciter un fournisseur d'accès pour obtenir de lui des informations utiles à l'enquête. Dès lors, ne pas conserver par anticipation les données de trafic revient à faciliter l'action des organisations criminelles et terroristes. De plus, comme la cybercriminalité ignore les frontières, la durée de conservation des données de trafic entre les Etats doit être suffisante et harmonisée. On constatera que dans certaines affaires d'intrusion dans un système informatique, les plaignants ont déposé plainte plusieurs mois après les faits. En matière d'escroqueries à la carte bancaire, les victimes se rendent le plus souvent compte de l'infraction, lorsqu'elles reçoivent leur relevé bancaire, soit parfois un mois après les faits.

Lors des négociations du texte, la France avait tenté d'intégrer cette mesure dans la convention, mais seule la Belgique qui avait déjà légiféré pour une conservation des données de trafic par les fournisseurs d'accès pour une durée d'un an minimum a soutenu l'initiative française. Cette proposition n'a donc pas été retenue. Aujourd'hui, l'Union européenne travaille sur un projet de décision-cadre destiné à harmoniser la durée de conservation de ces données.

Quant aux prestataires de services, ils ne sont pas des producteurs. Aussi, la responsabilité en cascade ne saurait être invoquée. Sauf intervention de leur part, les hébergeurs, les fournisseurs d'accès et les opérateurs n'ont respectivement aucune obligation générale de surveillance des contenus qu'ils

hébergent, transportent ou stockent automatiquement ou temporairement pour améliorer la performance des réseaux**.** Toutefois, les hébergeurs doivent concourir à la lutte contre la diffusion d'informations faisant l'apologie des crimes de guerre ou des crimes contre l'humanité, incitant à la haine raciale ou ayant un caractère pédophile en offrant aux internautes un dispositif pour dénoncer les faits qui seront ensuite portés à la connaissance des autorités publiques. Le non respect de ces obligations est sanctionné d'un an d'emprisonnement et de 7 500 euros d'amende. Les personnes morales sont passibles de 375 000 euros d'amende.

Faisant écho aux dispositions prévues par les articles 808 et 809 du code de procédure pénale, la loi rappelle que le juge peut prescrire aux hébergeurs, ou à défaut aux fournisseurs d'accès, en référé ou sur requête, toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par un contenu en ligne. Ils doivent par ailleurs retirer tout contenu dont ils connaîtraient effectivement le caractère illicite. Leur responsabilité pénale et civile ainsi que celles des opérateurs peut être engagée, s'ils n'agissent pas pour retirer un contenu illicite dont ils ont effectivement connaissance.

3) La procédure pénale

La loi d'orientation et de programmation pour la sécurité intérieure, la loi pour la confiance dans l'économie numérique et la loi portant adaptation de la justice aux évolutions de la criminalité ont créé de nouvelles procédures destinées à renforcer l'efficacité des investigations policières.

- Les perquisitions à distance

En application des articles 57-1, 76-3, 97-1 du code de procédure pénale, les officiers de police judiciaire peuvent désormais accéder directement à des fichiers informatiques et les saisir à distance par la voie informatique, afin de recueillir les renseignements qui paraîtraient nécessaires à la manifestation de la vérité. Toutefois s'il s'avérait préalablement que les données étaient stockées dans un système informatique situé en dehors du territoire national, il ne pourrait être accédé à celles–ci qu'en vertu des engagements internationaux en vigueur.

- Les réquisitions télématiques

Pour éviter la paralysie des enquêtes judiciaires résultant souvent de l'incapacité des personnes morales sollicitées de répondre avec célérité aux réquisitions, les articles 60-2, 77-1-1 et 151-1-1 du code de procédure pénale permettent dorénavant aux officiers de police judiciaire d'agir par voie télématique ou informatique dans le cadre des enquêtes préliminaires, de flagrant délit et sur commission rogatoire.

A la demande de l'officier de police judiciaire, les organismes publics ou les personnes morales de droit privé, à l'exception des Eglises ou des groupements à caractère religieux, philosophique, politique ou syndical, ainsi que

les organismes de la presse audiovisuelle, doivent mettre à sa disposition les informations utiles à la manifestation de la vérité, à l'exception de celles protégées par un secret prévu par la loi.

- La préservation du contenu des informations consultées

Suivant les dispositions de la convention sur la cybercriminalité, il est devenu possible de requérir des opérateurs de télécommunications et des fournisseurs d'accès toutes mesures destinées à préserver pour une durée maximum d'un an le contenu des informations consultées. En l'espèce, l'officier de police judiciaire ne pourra intervenir que sur réquisition du procureur de la République, préalablement autorisé par ordonnance du juge des libertés et de la détention.

- La collecte des éléments de preuve

Il est possible de collecter des éléments de preuve par copie des informations contenues sur le disque dur d'un système informatique. Il n'est donc plus nécessaire de saisir systématiquement le matériel. Ces mesures sont insérées aux articles 56 et 97 du code de procédure pénale.

- Remise de clés de déchiffrement et mise au clair de données chiffrées

L'article 434-15-2 du code de procédure pénale prévoit l'obligation de remettre les clés de déchiffrement aux agents habilités, agissant dans le cadre d'interceptions administratives, ou à l'autorité judiciaire, lorsqu'un moyen de cryptologie est susceptible d'avoir été utilisé pour préparer, faciliter, ou commettre un crime ou un délit. Les articles 230-1 à 230-5 du code prévoient pour leur part la possibilité de mise au clair des données chiffrées nécessaires à la manifestation de la vérité dans le cadre d'une poursuite judiciaire. Il peut ainsi être fait appel aux moyens de déchiffrement de l'Etat couverts par le secret de la défense nationale lorsque la peine encourue est supérieure à deux ans d'emprisonnement. La saisine par l'autorité judiciaire devra être adressée à l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication, qui transmettra le dossier à un centre technique d'assistance placé sous l'autorité du ministère de l'intérieur, de la sécurité intérieure et des libertés locales.

B - L'application de la loi française dans l'espace

La loi pénale française est applicable aux infractions commises sur le territoire de la République, d'un bâtiment battant pavillon français ou d'un aéronef immatriculé en France. L'infraction est réputée commise sur le territoire de la République dès lors qu'un de ses faits constitutifs a eu lieu sur le territoire. En outre, la loi pénale française est applicable aux infractions commises hors du

territoire de la République pour les crimes et délits punis d'une peine d'emprisonnement commis par un français ou un étranger ainsi que pour les crimes et délits commis par un français.

En matière de cybercriminalité, la jurisprudence indique que le juge français s'estime compétent « *dans la mesure où les messages ou le contenu du site sont rendus accessibles par Internet sur le territoire français* » (Tribunal de grande instance de Paris du 26 février 2002). Les juridictions étrangères ont souvent tendance, tout comme les tribunaux français, à appliquer leur droit national. Ainsi par exemple, la Cour constitutionnelle allemande a jugé que la loi allemande était applicable à des publications néonazies sur internet alors que les contenus en cause étaient publiés depuis l'étranger.

Il existe sur ce point une divergence entre la France et les Etats-Unis. Ainsi, dans l'affaire *Yahoo*, des associations françaises de lutte contre le racisme et l'antisémitisme se fondant sur le code pénal qui prohibe le port ou l'exhibition en public d'emblèmes nazis, ont demandé au tribunal de faire cesser la mise à disposition sur le territoire français, par la société *Yahoo Inc.* d'objets nazis par l'intermédiaire d'un site de vente aux enchères. Il y a eu au total trois référés (22 mai, 11 août, 20 novembre 2000). Dans les trois cas, la société américaine a soulevé l'incompétence territoriale du juge français, au motif que le fait avait été commis sur le territoire américain. Cette affaire a clairement posé le problème de la territorialité du droit pénal et de la portée du premier amendement de la constitution américaine garantissant la liberté d'expression.

Par ailleurs, ans le domaine de la pédopornographie, certains Etats répondent difficilement aux sollicitations des enquêteurs. Dans le cas des Etats-Unis, l'entraide directe avec le FBI est souvent plus efficace que l'entraide par les canaux traditionnels.

A l'heure actuelle, compte tenu du coût et de la complexité des procédures, la plupart des magistrats renoncent à la saisine d'un service étranger. Selon l'importance des valeurs détournées, ou encore des images pédopornographiques mises en ligne, les représentants du parquet français ont dès lors tendance à classer les dossiers pour des raisons d'opportunité. La convention sur la cybercriminalité et le protocole additionnel qui s'y rapportent devraient permettre d'améliorer l'harmonisation des règles et des procédures et réduire ainsi les inconvénients que présente les règles de territorialité en matière de lutte contre la cybercriminalité.

CONCLUSION

La convention sur la cybercriminalité constitue un outil indispensable pour permettre aux magistrats et aux services enquêteurs d'agir efficacement dans un domaine où la technologie a aboli les frontières. On peut toutefois regretter que nombre d'Etats se refusent à toute régulation et adoptent le comportement de « paradis cybercriminels ». Il conviendra, à l'avenir, d'étendre le champ d'application de cette convention. Alors même que la France a modifié sa législation pour l'adapter à la convention, votre Rapporteur propose à la Commission d'autoriser l'approbation de la convention qui constitue un gage d'efficacité pour la Justice et les services enquêteurs.

Quant au protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe, il constitue également un outil indispensable, compte tenu de l'utilisation d'internet à des fins de propagande raciste et négationniste. Votre Rapporteur vous propose d'en autoriser l'approbation en complétant par voie d'amendement le projet de loi dont l'Assemblée est saisie. Une telle démarche permettra ainsi de gagner du temps dans la procédure d'approbation, alors même que le protocole n'est toujours pas en vigueur.

DISCUSSION GENERALE

Au cours de sa réunion du 8 décembre 2004, la Commission a examiné le projet de loi autorisant l'approbation de la convention sur la cybercriminalité.

Après l'exposé du Rapporteur, plusieurs commissaires sont intervenus dans la discussion générale.

M. Didier Julia a rappelé qu'une grande entreprise française avait récemment été victime du vol d'un important programme informatique, mais s'était abstenue de porter plainte afin de ne pas reconnaître publiquement les faits. Elle a préféré créer sa propre cellule pour rechercher l'origine de cette attaque, et n'a bénéficié d'aucune aide des pouvoirs publics. Par ailleurs, il faut garder à l'esprit la dimension internationale de certains actes de cybercriminalité. Pour certains, par exemple, les pannes intervenues ces dernières semaines dans les systèmes informatiques de Bouygues et de la SNCF auraient été le résultat de l'intervention de services étrangers qui voulaient ainsi tester la vulnérabilité de la France dans ces domaines. L'Etat n'apporte pas de soutien particulier aux entreprises pour contrer ces attaques.

Le Président Edouard Balladur a demandé au rapporteur pourquoi il était nécessaire de définir les actes racistes et xénophobes dans le protocole additionnel à la convention sur la cybercriminalité, au risque que cette définition ne couvre pas la totalité des situations susceptibles d'être rencontrées. N'aurait-il pas été plus prudent de viser l'ensemble des propos contraires à la législation pénale ?

M. Guy Lengagne s'est interrogé sur les raisons pour lesquelles la plupart des signataires de la convention était des pays de petite taille, souvent récemment entrés dans l'Union européenne. Il a ensuite observé que la principale difficulté à laquelle se heurtait la police en matière de répression des sites racistes et xénophobes provenait du fait que c'était l'émission du message qui était condamnable et non sa réception.

Le Président Edouard Balladur a fait remarquer que la consultation de sites pédophiles constituait un délit.

En réponse aux différents intervenants, **M. Jean-Marc Nesme** a apporté les précisions suivantes :

- les cas cités par M. Didier Julia, qui ne sont pas des phénomènes nouveaux, relèvent plus de l'espionnage industriel que de la cybercriminalité ; pour ce qui concerne la panne du système informatique de la SNCF ou de

Bouygues Telecom, leur origine n'est pas nécessairement due à une malveillance, mais peut provenir de défaillances techniques ;

- conscients des limites de leurs interventions dans la lutte contre la cybercriminalité, les services de gendarmerie et de police réclament des moyens plus importants pour faire face à la montée en puissance de ce phénomène ;

- de nombreux problèmes concrets restent à résoudre pour améliorer la lutte contre la cybercriminalité ; on constate, par exemple, que la durée légale de conservation des données informatiques varie considérablement d'un pays à l'autre ; elle est d'une année en France alors que, dans certains Etats, elle est nulle ou limitée à vingt-quatre heures ; c'est pourquoi l'ONU devra, à terme, se saisir de cette question tant la nécessité d'une coordination internationale est nécessaire ;

- une convention internationale incriminant les actes de nature raciste et xénophobe par la voie des systèmes informatiques est nécessaire pour permettre les poursuites dans le cadre de l'entraide judiciaire ; en effet, dans certains pays hébergeant les sites en cause, la législation nationale ne prévoit pas l'interdiction de tels actes racistes ou xénophobes ; on ne peut, dès lors, se contenter de renvoyer à la législation française qui n'est pas applicable dans ces pays ; on doit également observer qu'en droit français les personnes qui consultent des sites contrevenant à la loi réprimant, par exemple, la pédophilie peuvent aussi être poursuivies ;

- si la convention sur la cybercriminalité a été ratifiée très rapidement par certains nouveaux membres de l'Union européenne, c'est sans doute en raison de la volonté de ces pays de montrer leur engagement européen.

*

* *

La Commission est ensuite passée à l'examen des articles du projet de loi.

EXAMEN DES ARTICLES

Article unique

Autorisation de l'approbation de la convention sur la cybercriminalité

La Commission a *adopté* cet article sans modification.

Article additionnel après l'article unique

Autorisation de l'approbation du protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques

La Commission a *adopté* un amendement du Rapporteur autorisant l'approbation du protocole additionnel à la convention sur la cybercriminalité relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques (**amendement n° 1**).

Titre du projet de loi

La Commission a *adopté* un amendement de coordination du Rapporteur modifiant le titre du projet de loi (**amendement n° 2**).

*

* *

La Commission a adopté l'ensemble du projet de loi ainsi modifié.

*

* *

En conséquence, la Commission des Affaires étrangères vous demande d'adopter le projet de loi (n° 905) modifié par les amendements figurant au tableau comparatif ci-après.

NB : Le texte de la convention figure en annexe au projet de loi n° 905
Le texte du protocole additionnel figure en annexe au projet de loi déposé au Sénat sous le n° 182 (2003-2004)

TABLEAU COMPARATIF

___

Texte du projet de loi	Propositions de la Commission
___	___
Projet de loi autorisant l'approbation de la convention sur la cybercriminalité	**Projet de loi autorisant l'approbation de la convention sur la cybercriminalité *et du protocole additionnel à cette convention, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques*** **(amendement n° 2)**
Article unique	Article unique
Est autorisée l'approbation de la convention sur la cybercriminalité, signée à Budapest le 23 novembre 2001, et dont le texte est annexé à la présente loi.	*(Sans modification).*
	Article additionnel
	Est autorisée l'approbation du protocole additionnel à la convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, fait à Strasbourg le 28 janvier 2003. **(amendement n° 1)**

PERSONNES ENTENDUES PAR LE RAPPORTEUR

• Ministère de l'Intérieur

Général Marc Watin-Augouard
Conseiller du Ministre pour la sécurité

• Office central contre la criminalité liée aux technologies de l'information et de la communication

Mme Catherine Chambon
Directeur Général

• Ministère de la Justice

Mme Myriam Quemener
Chef de Bureau des politiques pénales générales
Direction des affaires criminelles et des grâces
