Le Projet de convention européenne sur la criminalité dans le cyberespace L'organisation des poursuites internes

Elhadj Mame GNING(*)

***Lex Electronica*, vol. 6, n°2, Hiver/Winter 2001**

Synopsis

On the 27th of April 2000, the Council of Europe published the *Draft Convention on Cyber-Crime*. The text is expected to be finalized by a group of experts in December 2000 and ready to be signed by the Council in autumn 2001.

The *Draft Convention on Cyber-Crime* was designed with two goals in mind. First, considering the exponential increase of the use of computers, the internet and open data bases, the convention seeks to maintain the protection of privacy rights. Second, the convention promotes a tougher set of sanctions on cyber-violators who encroach on privacy rights. The legislation drafted in this convention is viable if it facilitates the detection, research and pursuit of internet crimes from a national to an international perspective. Therefore, in order to attain such objectives, global co-operation is a necessity.

The purpose of this article is to closely examine the *Draft Convention on Cyber-Crime,* in order to see the benefits and the effects to our rights and freedom.

Résumé

Le Conseil de l'Europe a publié le 27 avril 2000 un *Projet de convention sur la cybercriminalité* dans le cadre d'un appel public à contribution de ses pays membres. Le texte doit être finalisé par un groupe d'experts avant décembre 2000 pour être adopté et ouvert à la signature par le comité des ministres du Conseil de l'Europe à l'automne 2001. Ce projet constitue le futur traité international contre la criminalité dans le cyberespace dans l'espace européen.

Le *Projet de convention sur la cybercriminalité* poursuit deux objectifs. Premièrement, il vise la prévention des actes portant atteinte à la confidentialité, à l'intégrité et à la disponibilité des systèmes informatiques, des réseaux et des données. En second lieu, il prône l'adoption de pouvoirs suffisants pour permettre une lutte efficace contre les infractions pénales de haute technologie. Le cadre de mise en œuvre est possible, d'une part, en facilitant la détection, la recherche et la poursuite, tant au plan du droit de la procédure interne, qu'au niveau international. D'autre part, en prévoyant la création de dispositions matérielles appropriées en vue d'une coopération internationale alliant rapidité

et efficacité. Finalement, en garantissant un équilibre adéquat entre les nécessités d'une répression démocratique et le respect des droits fondamentaux.

L'objet de cet article est d'examiner le *Projet de convention* en ses dispositions organisant l'exercice des poursuites à un niveau interne, afin de pouvoir en percevoir autant les avantages que les faiblesses éventuelles au plan de la protection des droits et libertés de la personne.

Table des matières

Introduction

1. La société de l'information a fait naître une demande pressante de régulation des réseaux informatiques, dont le plus performant en ce début de millénaire, à savoir l'Internet. L'interconnexion des réseaux réalisée à travers cet outil riche de promesses, en termes de prospective, crée un espace de relations et d'échanges où se développent des situations juridiques dont certaines, il faut bien le reconnaître, revêtent un caractère inédit qui échappent aux catégories nommées auxquelles les usagers du droit sont si familiers.

2. Le cyberespace, qui en est à la fois le lieu et le socle, se refuse à une définition précise. Celui-ci ne pouvant être déterminé dans l'espace, il rend singulièrement impertinentes les notions de territorialité, de nationalité, voire de temps qui ont été jusqu'ici les éléments fondamentaux de la création de la règle de droit ou de son application[1]. Le débat sur la caractérisation du cyberespace ne manque pas d'intérêt pour le juriste, même si ce dernier semble l'avoir abandonné pour le moment à l'investigation philosophique.

3. D'autres enjeux décisifs préoccupent beaucoup plus la communauté juridique et celle des affaires qui, sous les pressions du développement des réseaux numériques et de l'insécurité qui en est la conséquence directe, se trouvent interpellées sur la nécessite de sa régulation.

4. L'attaque informatique dont l'Internet a été récemment l'objet par le vecteur du virus "*I love you"* devrait suffire pour convaincre la communauté internationale de l'urgence d'une régulation du Réseau qui ne saurait être considérée comme une zone de non-droit et où se développe aujourd'hui une criminalité de haute technologie aussi bien attentatoire aux biens qu'aux droits et libertés de la personne.

5. Les enjeux de la régulation se posent à un niveau mondial, compte tenu notamment du caractère transnational du Réseau même si, pour l'essentiel, les débats font ressortir des différences d'approches et de méthodologies sur les techniques d'organisation de cette régulation[2].

6. Certains États s'ouvrent, néanmoins, de plus en plus à des négociations internationales pour parvenir à des accords sur la régulation des réseaux informatiques, dans le cadre d'instances comme l'OMC, l'OMPI ou l'OCDE dont les activités ont permis d'améliorer sensiblement la protection de la vie privée et du consommateur, celle des droits de propriété intellectuelle afférents à la diffusion d'œuvres sur les réseaux ou la normalisation des procédures et pratiques en matière d'enregistrement des noms de domaine, en instaurant un mécanisme d'exclusion en faveur des marques renommées et notoires[3].

7. Le Conseil de l'Europe a créé en 1997 un comité chargé d'élaborer une convention sur la cybercriminalité dans le cyberespace visant à renforcer la coopération en matière pénale. Le *Projet de convention sur la cybercriminalité*, rendu public le 27 avril 2000, vise à

prévenir les actes portant atteinte à la confidentialité, l'intégrité et la disponibilité des systèmes informatiques, des réseaux et des données ainsi que leur usage frauduleux et à faciliter la détection, l'investigation et la poursuite de ces infractions pénales. Ce texte doit être finalisé par un groupe d'experts avant décembre 2000, pour être adopté et ouvert à la signature par le comité du Conseil des ministres de l'Europe à l'automne 2001[4].

8. Il faut cependant constater que la régulation des réseaux fait l'objet de demandes complexes, voire contradictoires[5], des équilibres doivent être trouvés entre libertés et contrôles, conciliant les nécessités de l'ordre, l'exercice des libertés et la pleine jouissance des droits. C'est la soumission à cet exercice périlleux que les experts du Conseil de l'Europe ont du s'astreindre tout au long de leurs travaux à bien lire l'exposé des motifs dudit *Projet de convention*, objet de la présente étude cantonnée aux seules dispositions afférentes à l'organisation des poursuites internes en matière d'infraction cybercriminelle. Il convient d'examiner les règles de compétence en matière de poursuites, avant d'envisager les procédures internes prévues par le *Projet de convention* du Conseil européen.

I. La compétence juridictionnelle en matière d'infraction cybercriminelle

9. La commission de l'infraction est toujours concomitante à des situations de temps, de lieux, ou à d'autres circonstances légalement définies qui déterminent les modalités de sa poursuite régulière.

A. Détermination de la compétence juridictionnelle

10. Il faut bien se rendre compte que le Conseil européen s'est contenté, dans son *Projet de convention sur la cybercriminalité*, de donner de simples recommandations aux États membres devant permettre à ces derniers d'édicter des règles législatives nécessaires pour établir leur compétence juridictionnelle, de la même manière qu'il a procédé par ailleurs pour le contenu matériel du *Projet de convention* en ses dispositions afférentes aux délits informatiques. La raison à cela est bien simple : les autorités communautaires ne peuvent pas édicter elles-mêmes des incriminations ou des sanctions proprement pénales[6].

11. Il convient de préciser ces recommandations de procédure pour parvenir à l'établissement de la compétence juridictionnelle en matière d'infraction cybercriminelle. Aux termes de l'article 19 du *Projet de convention*, "*chaque partie devra adopter les mesures législatives et autres nécessaires, pour établir sa compétence relativement à une infraction pénale établie conformément aux articles 2 à 11 dudit projet, lorsque l'infraction est commise :*

a. *[en tout ou en partie] sur son territoire, à bord d'un navire, d'un aéronef ou d'un satellite battant son pavillon ou étant immatriculé dans cette partie ;*

b. *par un de ses ressortissants, si l'infraction est punissable pénalement là ou elle a été commise ou si l'infraction ne relève de la compétence territoriale d'aucun État*".

12. Il ressort de ces indications au moins deux critères de détermination de la compétence juridictionnelle au sens du *Projet de convention* : la règle de compétence territoriale qui dépend du seul lien avec le territoire et la règle de compétence personnelle active qui résulte du lien de nationalité.

1. Le critère du territoire

13. Par l'élection de ce critère, le projet instaure une compétence qui est déterminée par le lieu où l'infraction a été commise. Les juridictions nationales de l'État sur le territoire duquel l'infraction a été commise en tout ou en partie sont compétentes pour enclencher des poursuites, procéder à des enquêtes ou connaître du fond de l'affaire en jugement en application des seules dispositions de leurs lois nationales.

14. Par territoire, il faut entendre le cadre de délimitation géographique de l'État où celui-ci a vocation à exercer une souveraineté exclusive et permanente, selon les règles du droit international[7]. Il englobe le territoire terrestre proprement dit (le sol et le sous sol, mais également les eaux comprises à l'intérieur des frontières), le territoire maritime, le territoire aérien qui comporte l'espace atmosphérique et, par extension ou fiction, les navires battant pavillon ou aéronefs immatriculés dans cet État.

15. L'infraction doit avoir été commise au moins en partie dans le territoire de l'État considéré, ce qui vise à notre sens son début d'exécution, à savoir les actes préparatoires tendant à la commission directe de l'infraction.

16. La question est cependant discutée de savoir si un État comme cela est souvent le cas qui partage la responsabilité d'un satellite avec d'autres États, devrait, en vertu de l'article 19 précité du *Projet de convention*, établir sa compétence concernant une infraction dont le seul lien avec cet État est que les données impliquées par l'infraction ont transité par le satellite. Le Conseil de l'Europe, qui n'a pas encore définitivement tranché le débat en l'état du projet, semble plutôt s'orienter vers d'autres instruments internationaux déjà élaborés, en prenant en considération la manière dont la compétence des États est régie en matière de satellites[8].

17. La question n'en perd pas moins de son importance, si l'on sait que le développement des réseaux numériques, particulièrement de l'Internet, se fera avec l'apport des technologies du futur, dont notamment les innovations enregistrées ces dernières années en matière de satellites qui sont appelés à relayer les réseaux de communication classiques (les réseaux téléphoniques traditionnels, comme les réseaux câblés à fibre optique), pour le transfert des données. Cela aura pour conséquence prévisible une progression sans précédent de la toile, laquelle devrait alors s'étendre aux zones les plus reculées de la planète.

18. C'est dire que, concomitamment, la criminalité dans le cyberespace gagnera en complexité et en croissance, d'autant que le couplage du réseau numérique au réseau satellitaire renforcera les capacités en matière de communication, en particulier une circulation sans entraves du texte, du son et de l'image, par la généralisation des hauts

débits qui devra consacrer l'Internet de la troisième génération, ouvrant de larges horizons dans le domaine des applications[9].

19. Apparemment, le Conseil européen ne se contentera pas d'une adoption pure et simple des dispositions d'autres instruments internationaux, élaborés selon des logiques qui leur sont propres, pour la détermination de la compétence des États en matière de satellites[10]. Il devrait sans doute apporter des innovations en la matière en anticipant sur le développement technologique futur, prenant cette question en considération dans toutes les composantes de sa complexité.

2. Le critère de la nationalité

20. La nationalité est le deuxième critère retenu pour la détermination de la compétence de l'État. La nationalité reste un critère classique, comme du reste le territoire, en matière de détermination de la compétence juridictionnelle ou d'applicabilité de la loi et, bien souvent, de jouissance des droits en droit international. L'article 19 du *Projet de convention* arrête la compétence de l'État chaque fois que l'auteur présumé de l'infraction est national ou ressortissant de cet État.

21. La nationalité pourrait être définie comme le lien politique qui rattache un individu à un État[11]. Il importe peu que l'infraction ait été commise dans un État autre que celui dont l'auteur présumé de l'infraction est national ou ressortissant, pourvu que l'infraction soit elle même punissable dans cet État. Ainsi, le *Projet de convention* retient le principe de la double incrimination pour établir la compétence de l'État au sujet des infractions commises par ses nationaux ou ressortissants à l'étranger. Il convient de préciser que ce principe de la double incrimination est exigé dans certains pays européens, à l'instar de la France pour ce qui concerne uniquement les délits commis à l'étranger et à l'exclusion des crimes commis par ses nationaux, à l'égard desquels ce principe n'est pas exigé la compétence de l'État Français étant retenue d'office[12].

22. Le *Projet de convention* est venu, il nous semble, harmoniser les différentes législations nationales des pays européens en ne faisant aucune distinction quant à la nature de l'infraction commise, la double incrimination étant retenue pour établir la compétence de l'État national, peu importe qu'il s'agisse d'un délit ou d'un crime commis à l'étranger, pourvu que l'infraction soit pénalement répréhensible dans l'État ou elle a été commise ou lorsque la compétence d'aucun État n'est retenue pour sa poursuite.

23. La réciprocité d'incrimination n'implique ni une identité absolue entre les incriminations des deux pays, ni l'identité des peines encourues. Il suffit que le fait réputé délictueux soit considéré pénalement répréhensible par l'État étranger[13]. Aucune poursuite ne peut avoir lieu lorsque l'intéressé justifie qu'il a été jugé définitivement à l'étranger et, en cas de condamnation, qu'il a subi sa peine ou obtenu une mesure de grâce. Cependant, la prescription ou l'amnistie intervenue à l'étranger ne peut, en principe, faire obstacle à la compétence des juridictions nationales[14].

24. La nationalité s'apprécie du jour de la commission de l'infraction. En cas de contestation sérieuse, l'exception de nationalité est préjudicielle. Elle ressort de la compétence des juridictions civiles. Sans aucun doute, les pays membres du Conseil de l'Europe ont pris les options décisives dans le *Projet de convention* sur la criminalité dans le cyberespace d'observer les valeurs et principes démocratiques garants d'une bonne justice pénale, notamment les principes de la stricte territorialité des lois pénales et de la légalité des peines, ce qui nous semble conforme aux principes universellement reconnus et consignés dans les instruments internationaux de protection des droits humains[15].

B. Limites apportées par le Projet de convention

1. Les réserves pouvant être faites par les États

25. Le *Projet de convention* sur la criminalité dans le cyberespace ne constitue pas un projet d'acte uniforme, il renvoie sur bien des points, aux législations nationales des États aussi bien pour l'incrimination des actes et des contenus informationnels dans les réseaux numériques, que pour la détermination des règles de compétence afférentes à la poursuite des infractions, laissant toutefois aux États le soin d'émettre des réserves.

26. Ainsi, l'alinéa 2 de l'article 19 précité prévoit expressément : "*Chaque État peut, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou de d'adhésion, dans une déclaration adressée au Secrétaire Général du Conseil de l'Europe, préciser qu'il se réserve le droit de ne pas appliquer, ou de n'appliquer que dans des cas ou conditions spécifiques, les règles de compétence définies au paragraphe 1b du présent article ou une partie quelconque de ces paragraphes…*".

27. Cet article porte en lui-même ses propres limites en édictant de telles possibilités conférées aux États en matière de réserves, puisque l'État n'est point tenu, dans ces conditions, de se cantonner aux strictes règles de compétence définies à l'article 19, alinéa 1. Il pourrait alors, par le jeu des réserves, invalider à son égard, de manière partielle ou totale, les dispositions pertinentes de la convention auxquelles il substitue ses propres règles nationales de compétence ou toute autre règle qu'il aura lui même définie. Il est simplement fait obligation, à l'alinéa 3 de l'article19, à l'État désireux d'émettre des réserves, d'adopter les mesures nécessaires, aux termes du *Projet de convention*, pour établir sa compétence au sujet d'un certain nombre d'infractions limitativement énumérées à l'article 21 dudit projet lorsque, après une demande d'extradition, l'auteur présumé de l'infraction présent sur son territoire ne peut être extradé au seul titre de sa nationalité.

28. Les infractions retenues à titre simplement indicatif, comme pouvant donner lieu à extradition, sans doute pour leur caractère attentatoire à la vie privée dans les réseaux ou pour la gravite des dommages qu'elles sont susceptibles d'occasionner aux systèmes informatiques, voire du degré du trouble qu'elles apportent à l'ordre public, sont celles dont l'incrimination est recommandées aux articles 3, 5, 7, 11 du *Projet de convention*, à savoir :

- l'interception illégale définie selon les propres termes du *Projet de convention* comme "*l'interception intentionnelle et sans droit de données informatiques, effectuées par des moyens techniques, lors de transmissions non-publiques, à destination, en provenance ou à l'intérieur d'un système informatique ainsi que des émissions électromagnétiques en provenance d'un système informatique transportant de telles données*" ;

- l'atteinte à l'intégrité du système appréhendée, selon les dispositions propres du projet, comme "*l'entrave grave, intentionnelle et sans droit au fonctionnement d'un système informatique, par l'introduction, le transfert, l'endommagement, l'effacement, la détérioration, l'altération et la suppression de données informatiques*" ;

- la falsification informatique ou encore,aux termes dudit, "*l'introduction, l'altération, l'effacement ou la suppression intentionnels et sans droit de données informatiques, engendrant des données non authentiques, dans l'intention qu'elles puissent être prises en compte ou utilisées à des fins légales comme si elles étaient authentiques, indépendamment du fait qu'elles sont ou non directement lisibles et intelligibles (possibilité étant laissée à une partie à la convention d'exiger en droit interne, une intention frauduleuse ou une intention pernicieuse pour la constitution de l'infraction)*" ;

- la complicité d'accès illégal à un système informatique qui doit être, aux termes du projet, "*un accès intentionnel et sans droit à tout ou partie d'un système informatique (les parties pouvant requérir que l'infraction soit commise soit en violation de mesure de sécurité soit dans une intention d'obtenir des données informatiques ou une autre intention délictueuse)*" ;

- la complicité de violation des droits d'auteur ou des droits voisins, à savoir : "*la reproduction et la diffusion intentionnelle et sans droit, à l'échelle commerciale, par le moyen d'un système informatique, d'œuvres protégées au titre du droit d'auteur, d'œuvres, (d'articles) ou de créations équivalentes protégées au titre des droits voisins, conformément à la Convention de Berne, l'accord ADPIC, les traites de l'OMPI sur les droits d'auteur et sur interprétations, exécutions et phonogrammes (l'intention doit être établie aussi bien pour l'infraction principale, que pour les actes de complicité, devant être interprétés au sens large comme visant les instigateurs et les auxiliaires).*"

29. En l'état du *Projet de convention*, la question est discutée de savoir si la tentative d'accès illégal à un système informatique devrait être incluse dans la liste des infractions pouvant donner lieu à extradition et à l'égard desquelles l'État qui a émis des réserves prévues plus haut pourrait appliquer ses propres règles de compétence. La disposition sur la tentative devra être rediscutée par le plénier afin de décider à quelles infractions elle devra s'appliquer[16].

2. Portée des réserves

30. Il ressort de l'examen de cet article 19, alinéa 2, que par le jeu des réserves qu'il instaure, l'on ne doit pas exclure le risque de voir les États vider le projet de son contenu quant à ses dispositions objectives sur la détermination de la compétence, en élaborant leurs

propres critères qui ne seront pas tout à fait étrangers, nous le savons par expérience, aux préoccupations de défense des intérêts nationaux, au détriment certain de la protection globale des réseaux numériques. En effet, la règle de compétence réelle qui fait dépendre la compétence juridictionnelle des seuls intérêts de l'État effectivement "victime" devra être décisive dans l'application de la future convention, avec ses difficultés d'appréciation liées à son imprécision et l'entrée en jeu d'autres critères de compétence concurrents qui devraient finir par causer des dysfonctionnements, voire des risques d'inefficacité dans la lutte contre la cybercriminalité qui, est-il encore besoin de le rappeler, doit être menée dans le strict respect des droits et libertés individuels[17]. C'est sans doute en prévision de telles difficultés qu'il faudrait lire l'alinéa 3 de l'article 19 du *Projet de convention* qui assortit de conditions précises l'option prise par l'État désireux d'émettre des réserves sur les règles de compétence définies à l'alinéa 1 de l'article19 précité.

31. Ainsi, les dispositions législatives prises par l'État en question, sur ses propres règles de compétence devront présenter, il nous semble, l'allure de véritables "lois de police" qui astreindraient toute personne présente sur le territoire de cet État, exclusivement de toute autre législation étrangère[18]; néanmoins la nature des infractions qu'il serait compétent à juger auront été déjà prédéterminées, dans le cadre de la convention. Les experts ont sans nul doute anticipé, par ces dispositions, sur de nombreuses difficultés d'application de la convention future sur la cybercriminalité en apportant des solutions qui nous semblent heureuses, à bien des égards, aux conflits de compétence prévisibles[19].

II. Les procédures internes envisagées en matière de poursuites d'infraction cybercriminelle

32. Le *Projet de convention* européenne sur la criminalité dans le cyberespace prévoit un certain nombre de procédures en matière de poursuites d'infractions informatiques. Ces procédures sont utilisées en vue de la recherche et de la conservation d'éléments matérialisant l'existence des faits incriminés ou leur prévention. Dans le cas des infractions visées par le *Projet de convention*, il s'agira surtout, lors de l'enquête préliminaire de police ou de la phase d'instruction qui lui succède menée par le juge ou sous sa supervision par commission rogatoire, de poser un certain nombre d'actes reconnus par la plupart des législations des États, en vue de perquisitionner et de saisir, s'il y a lieu, des systèmes informatiques ou des données stockées dans de tels systèmes. Le *Projet de convention* a déterminé le principe, l'étendue ainsi que les limites de ces mesures.

A. Les mesures clairement envisagées

1. Perquisitions et saisies de données informatiques stockées

a. Principe

33. Le principe de la perquisition et de la saisie de données informatiques stockées est prévu par l'article 14 du *Projet de convention* qui dispose : "*Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder d'une façon similaire à :*

a) un système informatique ou à une partie de celui-ci ou aux données informatiques qui y sont stockées ou ;

b) *à un support permettant de stocker des données informatiques, sur [son territoire ou en un autre lieu relevant de sa souverainet] pour les besoins d'enquêtes ou de procédures pénales…".*

b. Étendue de la perquisition ou de la saisie

34. Les perquisitions et saisies peuvent s'étendre aux termes de l'article 14 susvisé, soit au système informatique ou à une partie de celui-ci, soit aux seules données qui y sont stockées ou alors à tout support pouvant permettre de stocker des données informatiques. Le chapitre premier du *Projet de convention* consacré à la terminologie utilisée dans le texte définit le système informatique comme-"*désignant tout dispositif isolé ou ensemble de dispositifs interconnectés qui assure, en exécution d'un programme, un traitement automatisé de données (ou d'autres fonctions*)". Ainsi défini, un système informatique peut englober à l'heure de la numérisation un nombre important de dispositifs, allant d'un ordinateur ou de ses composantes (unité centrale, disque dur) à tous les réseaux d'ordinateurs interconnectés, comme l'Internet par exemple, ou simplement designer une carte de paiement ou de crédit.

35. Les données informatiques s'entendent, selon la terminologie précitée, comme "*toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, ou un ensemble d'instructions de nature à faire en sorte qu'un système informatique exécute une fonction*". Ces données informatiques désignent en pratique toute donnée relative au texte, au son à l'image et à la vidéo susceptible d'être traitée ou conservée, par des systèmes et moyens informatiques. Il est fait obligation à l'État-Partie de prendre des mesures spécifiques pour permettre la perquisition lorsque les autorités compétentes dans la pratique les officiers police judiciaire, le Procureur de la République ou le juge d'instruction estiment nécessaire de procéder en accédant à un système informatique précis et de pouvoir étendre rapidement ladite perquisition à un autre système informatique lorsqu'elles ont des raisons de penser que les données recherchées sont stockées dans ce système ou dans une partie de celui-ci, sis sur le territoire de l'État ou en un autre lieu relevant de sa souveraineté, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système

36. Les données informatiques auxquelles l'accès a été autorisé par la perquisition peuvent être saisies en vue de leur utilisation éventuelle dans des enquêtes et procédures pénales. Les mesures spécifiques que les États doivent envisager permettront en particulier les prérogatives suivantes aux autorités habilitées à procéder à des perquisitions et saisies :

- saisir ou acquérir d'une façon similaire un système informatique ou une partie de celui-ci ou un support permettant de stocker des données informatiques ;

- réaliser et conserver une copie de ces données informatiques ;

- préserver l'intégrité des données informatiques stockées pertinentes ;

- rendre inaccessibles ou enlever ces données du système informatique consulté.

37. L'État-Partie devra prendre en outre toute disposition appropriée pour habiliter, pour des besoins d'enquêtes ou de procédures pénales, les autorités compétentes à faire injonction à toute personne connaissant le fonctionnement du système informatique ou les applications, pour protéger les données informatiques qu'il contient, de fournir les informations raisonnablement nécessaires pouvant faciliter l'exécution des opérations de perquisitions et de saisies.

c. Limites en matière de perquisitions et saisies

38. Le *Projet de convention* s'assigne des limites en matière de perquisitions et de saisies qu'il subordonne aux conditions et garanties prévues par le droit interne de chaque État-Partie[20]. Le droit de l'État-Partie aura vocation à s'appliquer, au surplus pour ce qui concerne les autres conditions de forme, de temps ou de lieux requises pour la validité d'une opération de perquisition ou de saisie[21].

39. Le *Projet de convention* envisage d'imposer toutefois à l'État-Partie, en matière de perquisition ou de saisie, une obligation d'informer la personne responsable du système informatique saisi ou simplement perquisitionné, dès que cela est raisonnablement possible, sur les mesures effectivement exécutées[22]. Il est souhaitable, en considération du seul fait que, en matière de perquisitions et de saisies, les législations des pays européens ne sont pas harmonisées sur bien des points, que le Conseil puisse poser un certain nombre de règles de forme constitutives de garanties supplémentaires, au moins applicables en la matière et qui devront être intégrées au droit interne des États-Parties, pour une meilleure protection des droits et libertés individuels, particulièrement de la vie privée. En effet, les perquisitions et saisies constituent un domaine sensible en ce qu'elles sont toujours effectuées dans un contexte d'invasion de la vie privée. Et les garanties qui en sanctionnent ou préviennent les abus sont un domaine vital pour le citoyen et un instrument efficace de mesure de l'évolution des tendances d'une société[23].

40. Il nous sera sans doute répondu que ces garanties existent d'ores et déjà et résultent d'une simple lecture de l'article 8 de la *Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales[24]*. Certes, il faudrait reconnaître cependant que les dispositions de cet article 8 sur le droit à la vie privée sont générales. Leur réception par le droit des pays européens ne s'est pas faite sans difficultés et aura nécessité, pour bon nombre d'entre eux et même les plus réputés dans la protection des droits individuels, une intervention de la Cour européenne des Droits de l'Homme[25].

41. Ces règles de forme pourraient être envisagées dans le but d'assurer, aussi complètement que possible, la protection des droits individuels et la contradiction lors des opérations de perquisitions et de saisies d'un système informatique ou de simples données informatiques, à savoir :

- la présence nécessaire de la personne suspectée ou inculpée ou d'un représentant de son choix, à défaut, des témoins présentant des garanties de neutralité choisis par le juge d'instruction, le procureur de la République ou l'officier de police judiciaire chargé des opérations ;

- recueillir sur procès verbal l'assentiment exprès et préalable de la personne chez qui la perquisition est opérée ;

- l'établissement d'un procès verbal des opérations portant la signature de toutes les personnes qui ont assisté aux opérations ;

- promouvoir des formalités spéciales pour garantir l'authenticité et la conservation des objets saisis et protéger les droits individuels en cause, notamment contre l'indiscrétion et la malignité publique, en assurant l'interdiction, sous peine de sanction, de toute communication ou divulgation à une personne non qualifiée par la loi pour en prendre connaissance de documents provenant d'une perquisition ou d'une saisie d'un système ou de données informatiques.

Le *Projet de convention* européenne prévoit d'autres procédures permettant à l'occasion d'enquêtes ou de procédures pénales, de prendre des mesures conservatoires sur des données informatiques détenues par des tiers.

2. L'injonction de produire au détenteur ou conservateur de données informatiques

42. Le pouvoir d'injonction est prévu à l'article 15 du *Projet de convention* qui envisage d'obliger l'État-Partie à "*prendre des dispositions nécessaires pour habiliter les autorités compétentes à enjoindre à une personne présente sur son territoire, de fournir des données informatiques spécifiées qui sont sous son contrôle ou stockées dans un système informatique ou un support permettant de stocker de telles données, sous la forme requise par ces autorités, pour les besoins d'enquêtes ou de procédures pénales*".

43. L'injonction de produire est sans doute différente de la perquisition en tant que telle, qui est une mesure pouvant aboutir à une saisie ou à une acquisition forcée par l'autorité compétente de l'objet recherché comme indice ou preuve d'une infraction informatique. Par l'exercice du droit d'injonction, la personne sommée n'est pas préalablement suspectée ni même directement impliquée dans la commission d'une infraction. Il lui est simplement demandé de fournir des données informatiques qui se trouvent sous son contrôle et qui doivent être utilisées dans le cadre d'une procédure pénale. Il n'est pas excessif de penser que les dispositions de cet article 15 sont spécialement édictées pour amener les tiers à concourir aux opérations de poursuites pénales, dans des conditions de rapidité et de souplesse que n'aurait pas permis la lourdeur attachée à une perquisition ou saisie régulière. Son utilisation devrait être exceptionnelle cependant et cantonnée aux seules situations d'urgence pour assurer l'acquisition rapide de données informatiques suspectes, puisque l'article 14 du *Projet de convention* devrait permettre raisonnablement une perquisition ou une saisie effectuée chez un tiers à l'occasion de la recherche de faits ou d'indices afférents

à une infraction, dans des conditions de sécurité plus favorables aux tiers ainsi qu'à l'autorité publique.

Enfin, les résultats issus de cette procédure d'injonction ne sont pas à l'abri de contestations complexes et restent soumis à beaucoup d'aléas, contrairement à la perquisition[26].

3. Autres mesures conservatoires prévues

a. Mesures tendant à la conservation rapide de données stockées dans un système informatique

44. Alors que l'injonction examinée plus haut permet d'obtenir d'un tiers la production directe de données informatiques spécifiées qui se trouvent sous son contrôle, la deuxième règle que les parties devront s'obliger à adopter par des mesures législatives appropriées aux termes de l'article 16 tend à "*permettre aux autorités compétentes, à l'occasion d'une enquête ou d'une procédure pénale, à ordonner ou obtenir, la conservation rapide de données stockées dans un système informatique, lorsqu'il y a des raisons de penser que celles-ci sont soumises à une période de conservation limitée ou sont particulièrement sensibles aux risques de perte ou de modification*". Cette mesure constitue, à proprement parler, une injonction faite à un tiers d'avoir à conserver des données et se différencie de l'injonction de produire pour cette autre raison décisive que les États-Parties devront adopter des dispositions de droit interne pour en assurer l'exécution directe par la personne concernée qui sera tenue de conserver et de protéger l'intégrité des données pour une durée déterminée et à garder le secret sur l'existence et la mise en œuvre desdites procédures par l'autorité publique.

b. Mesures tendant à la conservation et la divulgation rapides de données relatives au trafic

45. Elles sont définies avec précision à l'article 17 du *Projet de convention*. Ces mesures sont complémentaires à celles relatives à la conservation rapide de données, quoique légèrement différentes. En effet, de telles mesures visent à la conservation et à la divulgation de données relatives au trafic concernant une communication spécifique. Le *Projet de convention* envisage d'obliger l'État-Partie à "*adopter en droit interne des dispositions législatives, permettant non seulement une conservation rapide de données brutes relatives au trafic, mais également une divulgation d'une quantité suffisante de ces données à qui de droit, aux fins d'identification des fournisseurs de service et de la voie par laquelle la communication a été transmise*".

c. Limites apportées par le Projet de convention à la conservation et à la divulgation de données stockées dans un système informatique ou relatives au trafic

46. Toutes ces mesures afférentes à la conservation et à la divulgation de données ainsi que les prérogatives reconnues aux autorités publiques quant à leur mise en œuvre sont subordonnées aux conditions et garanties prévues par le droit interne. Elles doivent être prises à l'occasion d'une enquête ou de procédures pénales. De telles mesures, bien que

revêtant un caractère conservatoire, devraient satisfaire aux dispositions de l'article 13 de la Convention de sauvegarde des droits de l'homme en donnant la possibilité au tiers d'user d'un recours effectif contre une mesure d'injonction devant une juridiction nationale de l'État-Partie[27].

B. Étude d'une mesure en cours de discussion : l'interception

47. Parmi les mesures en cours de discussion, l'interception aura le plus attiré notre attention. Ceci s'explique aisément aussi bien par le caractère particulièrement grave d'une telle mesure, analysée sous l'angle strict de la protection de la vie privée, mais aussi par les difficultés techniques de nature législative qui résultent de sa mise en œuvre. L'article 18 du *Projet de convention* sur la criminalité dans le cyberespace se contente d'énoncer son titre "l'interception" qu'il consacre sans le définir pour autant ni lui donner un contenu matériel encore sujet à de sérieux questionnements.

1. Définition

48. L'interception peut être définie comme "*le fait d'écouter ou d'enregistrer des communications privées, fonctions ou données d'un ordinateur dans le but d'en prendre connaissance pour en appréhender le sens ; l'objet ou la substance*"[28]. Ainsi, l'interception peut s'appliquer à des communications de nature privée comme cela est bien souvent le cas par exemple pour les écoutes téléphoniques ou les interceptions de correspondance postales effectuées par les autorités policières ou, encore, le fait par ces mêmes autorités de prendre connaissance des fonctions d'un ordinateur, par exemple du courrier électronique qu'il dessert, afin d'en appréhender le contenu[29].

49. Dans le cas des environnements électroniques, il n'est en rien prophétique d'affirmer que cette technique policière, trop redoutable pour être laissée entre les mains périssables de la police scientifique et des services de renseignement de certaines puissances étatiques, a son âge d'or devant elle. Et son utilisation devra déterminer en effet, pour beaucoup, l'issue de la question cruciale de la sécurité sur les inforoutes et du type de société dans laquelle nous serons appelés à vivre, peu ou prou[30]. D'ou l'impérieuse nécessité de sa réglementation stricte reconnaissant de larges garanties au citoyen.

2. Le problème législatif de l'interception

50. Analysée sous l'angle de la protection de la vie privée dans les inforoutes, l'interception pose des problèmes de technique législative. En effet, l'article 8 alinéa1 de la *Convention de sauvegarde* dispose expressément : "*Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance…* ".

51. L'interception policière d'une communication privée ou alors des fonctions d'un ordinateur et de ses données constitue sans doute une ingérence grave de l'autorité publique dans la vie privée du citoyen qui fait l'objet d'une protection particulière aussi bien par la plupart des constitutions des pays d'Europe mais aussi et surtout par l'article 8 paragraphe 2 de la *Convention de sauvegarde* susvisée, lequel prescrit des règles strictes en matière

d'ingérence : "*Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence soit prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique est nécessaire à la sécurité nationale, à la sûreté publique, au bien être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé et de la morale, ou à la protection des droits et libertés d'autrui*".

52. La Cour européenne des Droits de l'Homme s'est prononcée sur l'application des dispositions de l'article 8-2 susvisée, au moins par deux arrêts qui ont eu pour effet d'annuler des mesures prises par les autorités étatiques en matière d'interception de conversations téléphoniques privées. La Cour souligne notamment dans son arrêt du 21 août 1984, que "*la loi elle-même, par opposition à la pratique administrative dont elle s'accompagne doit définir l'étendue et les modalités d'exercice du pouvoir d'appréciation de l'exécutif en matière d'interception. Et cela avec une netteté suffisante pour fournir à l'individu une garantie contre l'arbitraire*"[31].

53. Ces décisions de la Cour européenne, qui ont entraîné la correction de dispositions légales de certains pays d'Europe en matière de droit d'ingérence dans la vie privée du citoyen, renseignent sur les difficultés de réception par le droit interne de ces pays des dispositions de l'article 8 de la *Convention de sauvegarde* des droits de l'homme et des libertés fondamentales. Le *Projet de convention* européenne sur la criminalité dans le cyberespace prendra en considération, dans la rédaction future de l'article 18 consacré à l'interception, l'expérience tirée des décisions rendues par la Haute Cour, lesquelles font encore autorité dans le domaine précieux de la protection du droit à la vie privée du citoyen[32].

Conclusion

54. Le Conseil de l'Europe aura entrepris, par le *Projet de convention* dont nous venons d'examiner, un certain nombre de dispositions et par d'autres directives en matière de commerce électronique ou de protection des données personnelles, le pari d'accompagner la transition des pays européens vers la société de l'information dans le respect des droits individuels. Il faut convenir que les enjeux sont importants et la nouvelle économie ne s'embarrassant pas de frontières, la mondialisation devra poursuivre son chemin à une vitesse encore sans précédent. Nous remarquons par ailleurs, avec une grande satisfaction, que les pays européens ont bien compris les nécessités présentes dans leur large majorité, non seulement en s'engageant dans des chantiers juridiques majeurs, comme celui objet de la présente étude sur la cybercriminalité, mais en cherchant également à promouvoir dans l'espace européen des programmes pratiques pour faciliter la transition de la société industrielle vers la société de l'information.

55. Tel était l'objectif de la conférence réunissant les Experts de la police et les milieux industriels à Paris pour l'examen de solutions de nature à sécuriser les réseaux électroniques, tenue en mai 2000 à la suite d'une résolution du sommet du G8 à Birmingham en 1998, et de nombreuses initiatives communautaires (plan communautaire pluriannuel du Conseil de l'Europe, en cours jusqu'en 2002 pour assurer la sécurité sur

l'Internet, l'initiative Europe de l'Union européenne sur la société de l'information pour tous etc…).

56. Il faut relever qu'il existe, au niveau communautaire, une coordination des politiques en matière de lutte contre la criminalité dans les réseaux entre l'Union européenne et le Conseil de l'Europe, ainsi qu'il ressort de la position commune 99/364/JAI du 27 mai 1999 prise dans le but d'éviter des incompatibilités entre les différents instruments de lutte contre la criminalité organisée utilisant les technologies avancées élaborés au niveau de l'Union européenne et le *Projet de convention* sur la criminalité dans le cyberespace négocié au sein du Conseil de l'Europe.

57. Il résulte de cet acte susvisé que les États membres ont adopté des principes à respecter au cours des négociations et ont indiqué les domaines dans lesquels ils souhaitaient l'intervention de la future convention, notamment l'extension du droit pénal aux infractions informatiques et à celles liées au contenu (pornographie infantile), les juridictions compétentes pour juger ces infractions devant être clairement désignées. En outre, les États membres envisagent l'extension de l'entraide judiciaire internationale et la création de "points de contacts des services répressifs" accessibles à toute heure afin de compléter les structures existantes ; de même qu'ils recommandent l'adoption de dispositions en matière de stockage des données dans les États signataires, l'accès à ces données par les autres États et la recherche de données transfrontalières.

58. Nous relevons, après examen du *Projet de convention* publié le 27 avril 2000, que le Conseil de l'Europe a satisfait, sur bien des points, aux prescriptions contenues dans le document précité exprimant la position des États membres. Il faut néanmoins souhaiter que des actions soient entreprises au niveau des instances internationales afin que puissent être engagées des négociations en vue de permettre les Pays en développement, en particulier les pays Africains, à élaborer des instruments juridiques dans le domaine de la lutte contre la cybercriminalité applicables selon leur zone d'appartenance géographique. Il est évident que la protection des réseaux ne pourra être assurée avec efficacité aussi longtemps qu'il existera un coin de l'univers qui ne sera pas couvert par ces instruments et qui constituera, de fait, un paradis numérique ou une zone de non-droit pour la criminalité de haute technologie.

Note d'actualisation (5 janvier 2001)

Nous avons été informé, alors que le présent article a été transmis à la rédaction de *Lex Electronica* et que s'ouvrait à Berlin le 23 octobre 2000 la toute dernière conférence du G8 consacrée à la cybercriminalité après celle de Paris tenue en mai de la même année, que les experts du Conseil de l'Europe ont élaboré de nouvelles dispositions, dans un document additif, dont, entres autres, celles afférentes à l'article 18 du *Projet de convention sur la cybercriminalite dans le cyberespace*.

Le document approuvé par le Conseil de l'Europe le 2 octobre 2000 à Strasbourg a suscité de vives controverses lors du dernier sommet de Berlin ouvert dans l'hostilité générale de

nombreuses associations Internet regroupées sous la bannière du GILC (*Global Internet Liberty Campaign*).

Le premier point d'achoppement avait été l'article 18 dudit projet consacré à l'interception qui devrait contraindre les fournisseurs d'accès à collecter ou à enregistrer les contenus de communications spécifiques circulant sur son territoire, seuls ou avec l'aide des autorités publiques.

Le GILC a estimé à juste titre que le terme de « *service provider* » repris dans les dispositions de l'article 18 susvisé revient à instaurer une surveillance généralisée du Réseau, mêlant acteurs publics et acteurs privés de tout acabit, confirmant hélas nos craintes légitimes exprimées dans notre article au sujet de l'interception.

Le projet encourage parallèlement les États à déployer leurs propres systèmes de surveillance, type *RIPAct* au Royaume-Uni, le logiciel *Carnivore* aux États-Unis ou les boites noires du FSB, ex- KGB , en Russie.

Il convient de relever toutefois que la conférence de Berlin n'a pas enregistré un franc succès et les trois jours de discussion qui se sont achevés le 26 octobre 2000 ont surtout mis en évidence autant les différences d'approche que les nombreuses difficultés rencontrées par les pays européens pour établir des normes communes en matière de régulation du cyberespace.

Note d'actualisation (15 avril 2002)

Le comité des ministres du Conseil de l'Europe a invité l'assemblée parlementaire à donner son avis sur le projet de convention sur la cybercriminalité qu'elle a définitivement adoptée avec amendements lors de sa session du mois d'avril 2001. Nous rappelons que ladite assemblée avait précédemment organisé en mars 2001 une audition d'experts internationaux sur ce projet de convention alors à l'étude. Le projet approuvé par les délégués des ministres le l9 septembre 2001 a été adopté par les ministres des affaires étrangères du Conseil de l'Europe le 8 novembre 2001 et ouvert à la signature des États le 23 novembre 2001 à Budapest à l'occasion de la Conférence Internationale sur la Cybercriminalité.

Les représentants des vingt six États membres ont signé le traité dont notamment, la France, le Royaume-Uni, la Suisse, l'Allemagne, l'Italie, l'Espagne, la Grèce et Chypre.

Le Canada, le Japon, l'Afrique du Sud et les États-Unis, pays non-membres du Conseil de l'Europe ayant participé à l'élaboration de ladite convention l'ont également signée. Aux termes de l'article 37, paragraphe 1 dudit traité, le comité des ministres du Conseil de l'Europe pourra ultérieurement inviter d'autres États non membres à la signature de la convention sur la cybercriminalité dont l'entrée en vigueur est prévue dès qu'elle sera ratifiée par cinq États, dont au moins trois États membres du Conseil de l'Europe.

Un protocole additionnel est en préparation au sein du Conseil de l'Europe pour la criminalisation des actes de propagande haineuse, raciste et xénophobe sur les info-routes.

Note d'actualisation(29 mars 2004)

Entrée en vigueur de la convention internationale sur la criminalité dans le cyberespace

Le 18 mars 2004, la Lituanie a ratifié la convention internationale sur la cybercriminalité.Ce traité, contraignant, devait entrer en vigueur dès que cinq Etats, dont au moins trois membres du Conseil de l'Europe, l'auront ratifié. Or, avec la Lituanie, le seuil des 5 ratifications a été atteint et le texte est pleinement entré en vigueur.

Nous rappelons que la convention a été ouverte à signature le 23 novembre 2001, à Budapest lors d'un sommet du Conseil de l'Europe consacré à la cybercriminalité.

Notes

(*) Avocat au Barreau de Dakar, Chargé de cours à l'Université Gaston Berger de Saint-Louis (Sénégal). Email : finishthejob@hotmail.com.

[1] Le débat engagé autour de la régulation du Cyberespace est, avant toute chose, un débat sur une définition des rationalités qui sous-tendent le droit des réseaux, voir à ce propos Pierre Trudel, *Droit du cyberespace*, Montréal, Les Éditions Thémis, 1997, chapitre 1er, 1-4 à 1-52.

[2] Voir "La corégulation, contribution française pour une régulation mondiale de l'Internet", rapport remis au Premier Ministre Lionel Jospin par Christian Paul, Député de la Nièvre, le 29 juin 2000, *Internet.gouv.fr*, <http://www.internet.gouv.fr/francais/textesref/pagsi2/lsi/rapportcpaul/sommaire.htm>.

[3] *Idem*.

[4] *Projet de convention sur la cybercriminalité* (projet N° 19) établi par le secrétariat Direction Générale I (Affaires Juridiques) du Conseil de l'Europe ; <http://www.coe.int> et <http://conventions.coe.int>

[5] *Op. cit.*, note 2.

[6] Voir V. Bigay, "Droit communautaire et droit pénal", *Revue trimestrielle de droit européen*, 1971 et "L'application des règlements communautaires en droit pénal français", *RTD*, 1971.

[7] Pierre Marie Dupuy, *Droit international public*, Dalloz-Sirey, 1992, pp. 23-24.

[8] Voir note n°26 dans les notes explicatives annexées au *Projet de convention sur la cybercriminalité, op. cit.*, note 4.

[9] *op. cit.*, note 2.

[10] Voir Charles Debbasch, *Droit de l'audiovisuel*, Dalloz, 1991, pp. 608-611. Selon cet auteur, les instruments juridiques en matière de satellites dans l'espace européen se cantonnent à deux catégories juridiques : les droits d'auteur et la question épineuse de la liberté d'expression dans ses rapports avec la souveraineté des États en matière de diffusion par la télévision satellite ; sur toutes ces questions, voir Cohen Jehorane H., "Problèmes juridiques soulevés par la télévision par satellites en Europe", *RIDA*, n° 122, oct.1984, pp.147 et suivantes.

[11] Marc Puech, *Droit pénal*, Litec, 1988, pp.147-148 ; Yvon Loussouarn et Pierre Bourel, *Droit international privé*, 3ème Édition, Dalloz, 1988, n° 521.

[12] *Idem*, p. 153 et suivantes.

[13] *Idem.*

[14] *Idem.*

[15] À titre indicatif, voir de manière générale *: Déclaration des droits de l'homme et du citoyen du 26 Août 1789*, art. 7 ; *Déclaration universelle des droits de l'homme du 10 Décembre 1948*, art. 11. Nous examinons plus loin les aspects spécifiques de la*Convention de sauvegarde* des droits de l'homme et des libertés fondamentales de 1950 uniquement applicable dans l'espace européen.

[16] Voir note n° 19 annexée au *Projet de convention sur la cybercriminalité, op. cit.*, note 4.

[17] C'est sans doute en prévision des conflits de juridictions que les experts des pays européens envisagent d'instituer un principe de concertation préalable lorsque plusieurs parties ont compétence à l'égard d'une infraction présumée ; voir particulièrement le paragraphe 5 de l'article 19 du *Projet de convention sur la cybercriminalité*. Les règles de compétence étant précisées, il convient à présent d'examiner les procédures internes envisagées, dans le cadre du projet, pour les poursuites exercées contre l'auteur présumé d'une infraction cybercriminelle.

[18] *op.cit.*, note 11, p. 168.

[19] Autrement les États seraient libres d'invoquer la règle de compétence réelle, avec toutes ses incertitudes. Cette règle rend compétente la juridiction de l'État qui se prévaut d'une atteinte à ses intérêts vitaux, voir Marc Puech, *op. cit.*, note 11, p. 159 ; Pierre

Trudel, *op.cit*., note 1, p. 4-22. Cet auteur ne semble pas avoir une affection particulière pour le principe de la protection "*qui peut facilement donner ouverture à des abus, les États l'employant à toutes les sauces*" selon le professeur Pierre Trudel. Par ailleurs, l'auteur relève l'inexistence d'un consensus entre les pays européens quant aux intérêts à définir comme essentiels. Il renvoie au document ci-après *: Conseil de l'Europe, compétence extra- territoriale en matière pénale, comité européen pour les problèmes criminels*, Strasbourg, 1990, p. 14.

[20] Voir art. 14-7 du *Projet de convention* qui renvoie expressément aux garanties prévues par le droit interne auxquelles les perquisitions et saisies restent subordonnées ; voir également les dispositions de l'article 8, de la *Convention de sauvegarde des droits de l'homme et des libertés fondamentales* de 1950.

[21] Notons les immunités diplomatiques et consulaires reconnues aux membres du corps diplomatique accrédité prévues par la *Convention de Vienne* du 18 avril 1961 et du 24 avril 1963. Il est reconnu en particulier certaines garanties spéciales en matière de perquisitions et de saisies aux avocats pour la sauvegarde du secret professionnel et aux médecins et établissements hospitaliers pour la préservation du secret médical.

[22] Voir art. 14-6 du *Projet de convention* et la note n° 24 annexée audit projet, sur ce que couvre la notion de responsable, laquelle viserait tout aussi bien le propriétaire que l'utilisateur et de manière générale toute personne qui exerce un contrôle physique sur l'ordinateur ou le système informatique.

[23] Yves de Montigny, "La protection contre les fouilles, les perquisitions et saisies abusives: un premier bilan", *La revue du Barreau*, Barreau du Québec, Les Éditions Yvon Blais Inc., 1989, p. 79, voir note 67. Nous sommes dans les mêmes dispositions que l'auteur qui partage entièrement le point de vue du Doyen Griswold dans le contexte de l'article 8 de la charte canadienne, objet de son étude susvisée. Le doyen Griswold, a déjà émis l'opinion suivante : "*The protections of the fourth amendment largelydetermine the kind of society in which we live*". E. Griswold, "*Search and Seizure: A dilemna of the Supreme Court*", 1975, p. 39, cité par W. R. Lafave, "The Fourth Amendment Today: A Bicentennial Appraisal", (1987) 32, *Villanova Law Review*, p. 1061 et p. 1064. Nous précisons que le quatrième amendement consacre le droit à la vie privée entre autres dispositions de la constitution américaine et dispose expressément *:* "*Le droit des citoyens d'être garantis dans leurs personne, domicile, papiers et effets, contre les perquisitions et saisies non motivées ne sera pas violée, et aucun mandat ne sera délivré, si ce n'est sur présomption sérieuse, corroborée par serment ou affirmation, ni sans qu'il décrive particulièrement le lieu à fouiller et les personnes ou les choses à saisir* ". Voir, J.W Peltason, *La constitution des Etats Unis d'Amérique*, suivie de notes explicatives, p.46-usia-1987. Selon cet auteur, le 4^{e} amendement exige surtout que, dans la majorité des cas de perquisitions ou de saisies, les autorités, après avoir exposé les motifs de leur demande, puissent solliciter d'un juge un mandat d'arrêt ou de perquisition.

[24] Voir *Convention de sauvegarde des droits de l'homme et des libertés fondamentales* de 1950. L'article 8 consacre les garanties attachées à la protection du droit à la vie privée.

[25] Voir note 31 pour les références. Par deux arrêts intervenus le 21 août 1984 et le 24 avril 1990, la Cour européenne des Droits de l'Homme a annulé des mesures d'interception de conversations téléphoniques privées prises par l'autorité publique, notamment le Royaume-Uni et la France. Curieusement, ces derniers pays ont une bonne réputation en matière de protection des droits individuels. Les arrêts susvisés de la Cour européenne des Droits de l'Homme renseignent sur les difficultés de réception par le droit national de ces mêmes pays des dispositions de l'article 8 de la *Convention de sauvegarde*. Les difficultés de réception des dispositions de la convention précitée vont très probablement augmenter en considération du profil des pays qui frappent à divers titres à la porte de l'Union européenne, particulièrement les anciens pays de l'Est et la Turquie.

[26] Voir *New York Times*, 17 octobre 2000, article relaté par le quotidien *sénégalais* « *Le soleil* » du 21 octobre 2000, <http://www.lesoleil.sn>, la question est discutée aux États-Unis d'Amérique de savoir si *Yahoo ! Inc.* est tenu de dévoiler l'identité d'un internaute suspecté par son employeur d'avoir posté sous le pseudo de Jane Doe des propos diffamatoires à son encontre sur un forum de *Yahoo!*. Nous précisons que ce débat est engagé autour d'une injonction d'un tribunal fédéral de l'Ohio adressée à*Yahoo! Inc.* et AOL, le fournisseur d'accès du "suspect", afin que puisse être levé l'anonymat. Cette démarche a fait réagir les groupes de protection des libertés civiles, tels que *Electronic Frontier Foundation* et *Public Citizen* qui veulent empêcher l'exécution de l'injonction. Ces groupes font référence à une déclaration de la Cour Suprême des États-Unis qui aurait rappelé que "*le premier amendement protège le droit de parler anonymement afin de garantir la liberté d'expression*". La première audience est prévue le 9 novembre 2000. Pour de nombreuses raisons, ce débat ne nous semble pas transposable à l'échelle européenne ; cependant le pouvoir d'injonction reconnu à l'autorité publique est subordonné à l'article 8 de la *Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales*.

[27] Voir l'article 13 de la *Convention de sauvegarde* de 1950 qui institue le droit à un recours effectif devant une instance nationale contre les actes violant les droits fondamentaux.

[28] Pour une définition de l'interception, voir Pierre Trudel, *Droit du cyberespace*, op. cit., note 1, p. 10-8.

[29] Sur l'interception de communications privées, voir Pierre Trudel, *op. cit*., note 1, p.10-8 / 10-9 / 10-10.

[30] Sur les aspects constitutionnels et sociologiques des fouilles, perquisitions et saisies abusives, voir Yves de Montigny, *op.cit.*, note 23. Pour un aperçu plus large de la question Échelon, voir Philippe Rivière, « Premiers débats sur Échelon », 18 avril 2000, *Le Monde Diplomatique*, <http://www.monde-diplomatique.fr/dossiers/echelon/>. Le nombre d'articles qui lui est consacré renseigne amplement sur la gravité de la problématique Échelon. Nous rappelons que le système Échelon est le produit du Pacte Ukusa signé au tout début de la guerre froide par les États-Unis et le Royaume-Uni. Il constitue un dispositif de surveillance générale et d'interception très sophistiqué des communications privées (conversations téléphoniques, fax et courriers électroniques) et permet de collecter quantité d'informations, secrètes ou non, concernant l'ensemble des domaines d'intérêt stratégique : données économiques, stratégies des décideurs, milieux concernés par tel ou tel enjeu. Le

Canada, l'Australie et la Nouvelle -Zélande devaient rejoindre rapidement ce partenariat. Il serait souhaitable que le système Échelon puisse évoluer précisément vers une sorte de cyberinterpol pour la prévention du crime dans le cyberespace, au bénéfice de tous les pays membres des Nations-Unies. Autrement, sa légalité nous semblerait douteuse, sous l'angle du 4ème amendement de la Constitution des États-Unis et de l'article 8 de la *Convention de sauvegarde*.

[31] Voir Vincent Berger, *Jurisprudence de la Cour européenne des Droits de l'Homme*, Sirey, 1991, p. 24 ; particulièrement l'arrêt du 21 août 1984, *James Malone c. Royaume Uni* et l'arrêt du 24 avril 1990, l'affaire *Kruslin et Huvig c. Gouvernement Français*. Ces deux arrêts se prononcent sur la légalité de l'interception de communications téléphoniques opérées par l'autorité publique dans le cadre d'une perquisition. Ces mesures ont été annulées au motif que les lois de ces Etats n'avaient pas défini avec une netteté suffisante l'étendue et les modalités d'exercice du pouvoir exécutif en matière d'interception.

[32] Nous constatons qu'aucun contenu n'a été proposé dans le cadre de l'article 18 du *Projet de convention* sur l'interception, mesure qui serait en cours de discussion. L'inexistence d'un contenu même provisoire témoigne apparemment d'un désaccord des délégations des différents pays européens sur la question.

ISSN 1480-1787