INFRACTIONS EN RELATION AVEC LES NOUVELLES TECHNOLOGIES DE L'INFORMATION ET PROCÉDURE PÉNALE : L'INADAPTATION DES RÉPONSES NATIONALES FACE À UN PHÉNOMÈNE DE DIMENSION INTERNATIONALE.

PAR NDIAW DIOUF
PROFESSEUR AGRÉGÉ DE DROIT PRIVÉ
FACULTÉ DES SCIENCES JURIDIQUES ET POLITIQUES
UNIVERSITÉ CHEIKH ANTA DIOP DE DAKAR
DIRECTEUR DU CREDILA

I N T R O D U C T I O N

-*-*-

Souvent associé à la liberté d'opinion et d'expression, le droit à l'information[1], prolongement de la liberté de l'information, est proclamé et garanti dans pratiquement tous les Etats démocratiques par des normes juridiques supérieures[2]. A cette protection sur le plan interne s'ajoute une protection assurée au plan international par des textes de portée régionale

[1] La liberté de l'information se présente sous deux aspects : droit d'informer et droit d'être informé.
[2] Au Sénégal l'article 10 de la constitution actuelle prévoit que « chacun a le droit d'exprimer et de diffuser librement ses opinions par la parole, la plume, l'image la marche pacifique pourvu que l'exercice de ses droits ne porte atteinte ni à l'honneur et à la considération d'autrui, ni à l'ordre public ». ces principes étaient déjà consacrés par la constitution de 1963 V. Ndiaw DIOUF, La procédure pénale à l'épreuve des nouvelles technologies de l'information de la communication, RASTP n°s 5-6-7-8 1997-1998, p. 9.
Au Portugal, le texte constitutionnel consacre le droit pour tous d'informer, de s'informer et d'être informé sans entrave ni discrimination. Art. 37, n° 1. En France la liberté d'informer est reconnue depuis l'intégration de la Déclaration de 1789 dans le bloc de constitutionnalité. V. sur cette question, Favoreu, La protection constitutionnelle de la liberté de la presse in liberté de la presse et droit pénal Presses universitaires de Grenoble 1994 p. 221.

(art. 9-1 Charte africaine des droits de l'homme et des peuples : « toute personne a droit à l'information » ; art. 10 Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales : liberté de recevoir ou de communiquer des informations) ou universelle (art. 19-2 déclaration universelle des droits de l'homme de 1948 : « Droit de chercher de recevoir et de répandre… des informations ; art. 19-2 du Pacte des Nations- Unies relatif aux droits civils et politiques : « Liberté de chercher, de recevoir et de répandre des informations».

D'ailleurs, pour donner un contenu concret au droit à l'information certains Etats tentent de créer les conditions d'un accès facile à l'information en déclarant libres ses supports traditionnels que constituent la librairie et l'imprimerie[3].

Il faut dire que depuis quelques années, l'information sur support papier est en voie d'être supplantée par l'information sur support électronique avec le développement de nouvelles technologies de l'information.

C'est le lieu de rappeler que les technologies de l'information peuvent s'entendre, pour reprendre une définition donnée par le conseil des communautés européennes[4], de l'ensemble des « systèmes, équipement composants et logiciels qui sont nécessaires pour assurer la recherche, le traitement et le stockage de l'information dans tous les domaines de l'activité humaine et dont la mise en œuvre fait généralement appel à l'électronique et aux technologies similaires ».

[3] V. loi française du 29 juillet 1881
Loi sénégalaise du n° 96-04 du 22 février 1996 relative aux organes de communication sociale et aux professions de journaliste et de technicien.
[4] Décisions du 22 décembre 1986 relative à la normalisation dans le domaine des technologies de l'information et des télécommunications JO des Communautés Européennes.

Ces technologies de l'information ainsi définies ont connu, ces dernières années, un essor considérable. Aujourd'hui, compte tenu de leur diversité et de leur perfectionnement, ces technologies permettent d'avoir un espace informationnel de plus en plus vaste et de plus en plus riche. Ne parle-t-on pas actuellement des 'autoroutes de l'information ?

L'Internet[5] [6] est la meilleure illustration possible de l'importance quantitative des informations disponibles dans des domaines très divers allant du champ structuré du savoir à la vie quotidienne des individus en passant par la situation des entreprises.

Ce fabuleux outil de stockage et de transmission de l'information change progressivement la physionomie de la société traditionnelle qui se transforme en une société de l'information.

Cette brutale transformation qui engendre une modification totale de la manière dont les individus communiquent et se mettent en relation a suscité dans presque tous les pays, à tort ou a raison, des craintes des pouvoirs publics qui tentent de réagir. La diversité des réactions contestées un peu partout, surtout face à l'importance que prend l'Internet, traduit éloquemment le désarroi des Etats.

[5] Selon un auteur l'usage de l'article défini devant le mot « Internet » est du fait qu'il s'agit d'un nom commun et non d'une marque ; V. Sébastien Canevet, Fourniture d'accès à l'Internet et Responsabilité pénale, http://www.canvet.com/doctrine/resp-fai.htm

[6] L'Internet a été défini comme « le réseau mondial…auquel plusieurs centaines de millions d'usagers sont aujourd'hui connectés et qui permet de communiquer d'une machine à une autre à travers le monde pare des câbles intercontinentaux et des liassions par satellite au débit considérable » (E. Tois, Internet et libertés, Quelques repères, rapport de la Cour de Cassation 2001, http://www.cour de cassation.fr/_rapport/rapport01/etudes&dr/Tois.htm

On peut noter, à cet égard, que certains pays tentent de bloquer ou tout au moins de limiter l'accès à l'Internet[7] en contrôlant les points d'accès ou en faisant des pressions sur les fournisseurs d'accès[8].

Mais face aux difficultés techniques rencontrées pour arriver à couper l'accès à tous les sites ou pour interdire à des utilisateurs de se connecter à un site donné[9], d'autres solutions sont envisagées ; elles consistent à contrôler le contenu des informations[10] ou à interdire la circulation sur le Net de certaines informations[11].

Cette tentative de régulation des technologies de l'information était inévitable. Il ne faudrait pas en effet perdre de vue que si les nouvelles technologies assurent une liberté d'information et de communication sans entrave, elles peuvent aussi être l'occasion de diffuser des informations criminelles ou de se livrer à toute sorte de trafic. Les possibilités nouvelles

[7] V. Sur cette question Piette-Coudol et Bertrand « Internet et la loi », ed. Dalloz 1997, Coll. Dalloz.Service p. 47 note 1. Ces auteurs montrent que certains pays comme l'Arabie Saoudite, Singapour et le Vietnam essaient de limiter et/ ou filtrer l'accès et/ ou les passerelles Internet.

[8] Dans certains pays les gouvernements imposent aux fournisseurs d'accès un strict respect des cahiers des charges. V. Courrier International n° 312 du 24 au 30 oct. 1996 p.6.

[9] Même en Allemagne où l'Etat dispose des moyens énormes, Deutsche Telekom et Wissenschaftsnetz ont tenté sans succès, à en croire Mr. Chassaing, (l'Internet et le Droit pénal D. 1996-329) de filtrer l'accès à un site néo-nazi.

[10] Un ministre allemand a demandé en juillet 1996 à la tribune des Nations- Unies la création d'une commission chargée de définir des critères internationaux pour le contrôle du contenu des informations diffusées sur le Net.

[11] Aux Etats-Unis, la communication Decency act réprimait le fait d'envoyer ou rendre accessible à une personne âgée de moins de 18 ans tout commentaire, demande, suggestion, proposition, image ou autre communication qui dépeint ou décrit, en termes manifestement choquants des activités sexuelles ou excrétoires. Mais cette disposition a été déclarée non conforme à la constitution par le Tribunal de Philadelphie le 11 juin 1996. V. sur cette question Piette-Coudol et Bertrand précité pp 114 et 115. Quant à la commission de l'Union européenne, elle propose des mesures pour interdire la circulation sur le Net de matériel pornographique et d'autres informations jugées illégales. On peut relever que lors de la conférence ministérielle sur les droits de l'homme de Rome (3-4 novembre 2000), la résolution II insistera sur les dangers que peut engendrer l'Internet et invite les Etats membres à poursuivre leurs travaux visant à contrecarrer des activités qui menacent les droits de l'homme sur Internet, telles que, notamment des activités liées au racisme et aux mouvements extrémistes ; V. Alexis Guedj, Nature frontière du réseau Internet et Ordre public, droits fondamentaux, n° 1 juillet – décembre 2001, http://www.revue.df.org

offertes par les technologies de l'information modifient d'ailleurs fondamentalement les formes de la criminalité.

Il ne fait pas de doute que les problèmes soulevés par l'irruption des nouvelles technologies de l'information sont, pour la plupart, connus et traités. Comme on a pu l'écrire[12], à propos de la circulation dans l'espace électronique de données illicites qui portent atteinte à l'ordre public et aux bonnes mœurs ou d'informations à caractère haineux ou offensant, « ce qui était hier inadmissible sur papier demeure inacceptable, à l'heure d'Internet, sous forme de fichier électronique ». Seulement ce qu'il ne faudrait pas perdre de vue, c'est l'inadaptation des solutions traditionnelles – conçues pour un environnement matériel - à un environnement totalement dématérialisé. Outre les difficultés liées à l'impossibilité de transposer les solutions traditionnelles, il y a les problèmes nés de la modification des comportements consécutive au développement des nouvelles technologies. Aujourd'hui une nouvelle forme de criminalité est apparue, favorisée par l'environnement.

L'actualité récente fournit de nombreux exemples d'instructions illicites et de graves atteintes aux données contenues dans le matériel informatique. Il n'est pas possible à l'heure actuelle de faire l'impasse sur la multiplication des comportements répréhensibles jusque là ignorés et sur les problème nouveaux générés par ce phénomène.

On a certes soutenu jadis dans certains pays[13] que la législation qui existe permet de prendre en compte les problèmes posés par les réseaux.

[12] Daniel Padouin, Un point de vue nord – américain sur Internet et ses enjeux GP 11-12 sept. 1996 p.19.
[13] V. pour la France : Gauthier, Du droit applicable dans le « village planétaire au titre de l'usage immatériel des œuvres D.S 1996 p. 131. Cet auteur met en garde contre le risque d'implosion lié au fait que le droit français est déjà saturé de réglementation.

Mais cette opinion, pour judicieuse qu'elle soit, se heurte à deux objections majeures :

- d'une part, il n'y a pas de législation appropriée dans la plupart des pays, notamment ceux du Tiers-monde ; or en raison de la circulation internationale des données que permettent les nouvelles technologies de l'information, toute solution isolée se révèle à terme inefficace ;
- d'autre part, ces auteurs qui se contentent de l'existant en demandant aux juges d'adapter les textes n'ont raisonné que dans le cadre de la législation civile ; or ce qui est valable en matière civile ne l'est pas en matière pénale, la législation pénale s'accommodant mal d'une interprétation extensive, tout au moins dans les systèmes attachés au principe de la légalité.

Il y a donc des problèmes nouveaux en matière pénale et ces problèmes apparaissent aussi bien en droit pénal de fond qu'en procédure pénale. Pour ce qui concerne spécialement la procédure pénale, les problèmes se situent à deux niveaux : d'abord l'internationalisation des infractions et la diversité des législations rendent pratiquement toute poursuite impossible, par ailleurs les moyens classiques de recherche et de constatation des infractions ne sont plus adaptés face aux nouvelles formes de criminalité ; cela explique pourquoi les preuves susceptibles de servir de base à une condamnation pour des agissements liés aux nouvelles technologies sont pratiquement introuvables.

V. aussi Vivant, Cybermonde : Droit et droits des réseaux JCP 1996 I. n° 3969. Cet auteur relève qu'un droit de la télématique susceptible de venir appréhender la télématique s'est développé.

I – DES POURSUITES SOUVENT IMPOSSIBLES

Le recours aux nouvelles technologies de l'information pour commettre des infractions a mis en lumière les limites des règles classiques de procédure. En effet, autant la pluralité des intervenants complique la recherche de celui qui doit être tenu pour responsable, autant la dispersion des éléments de l'infraction rend aléatoire le rattachement de celle-ci à un territoire déterminé.

A –La détermination des responsables

Les difficultés d'une répression efficace des comportements antisociaux liés aux technologies de l'information ne sont pas nouvelles. Elles ont déjà été constatées à propos de ce que l'on appelle la criminalité informatique.

L'on admet maintenant, malgré les réserves de certains auteurs[14], qu'en plus des agissements dont l'outil informatique fait l'objet, par exemple le vol d'un ordinateur, il y a les agissements dont l'outil informatique n'est que l'instrument[15]. Si la répression du premier type d'agissements n'a suscité aucune difficulté, les textes réprimant les atteintes aux biens pouvant fort bien s'y appliquer, il n'en est pas de même du second type d'agissements. En effet, on ne peut, sans risquer de porter atteinte au principe de la légalité –en étendant considérablement la définition des éléments constitutifs de l'infraction- utiliser les qualifications

[14] Certains auteurs français ont tenté de tracer les contours d'une théorie générale de l'information en mettant l'accent sur l'information elle-même et pas nécessairement sur son support. L'information apparaît, à leurs yeux, malgré son caractère immatériel comme un bien susceptible d'appropriation : V. par exemple Catala, Esquisse d'une théorie juridique de l'information D. 1984. Chron. P.97 et s.

[15] V. Francillon, Les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique en France, Revue inter. Dr. Pen. 1993 p. 191.

pénales traditionnelles pour réprimer des actes tels que l'accès dans le système informatique d'autrui.

L'impossibilité d'opérer une transposition pure et simple s'explique aisément : la plupart des incriminations sont crées pour protéger la propriété des objets corporels et non des objets incorporels tels que l'information ; il s'y ajoute que, du fait de la liberté de circulation de l'information, il est difficile de concevoir la protection d'un droit privatif sur l'information[16].

Pour ne pas laisser impunies de graves atteintes au contenu de l'outil informatique, certains Etats n'ont pas hésité à adopter une législation spécifique permettant de réprimer efficacement des actes tels que l'accès ou le maintien frauduleux dans un système informatique[17].

Le problème de la protection des données s'est amplifié avec le développement du réseau Internet. Il est parfaitement possible aujourd'hui, avec les services qu'offre Internet, de « se promener » dans un système ou dans un réseau, de s'introduire illicitement sur des réseaux clients ou serveurs pour s'emparer des données qui y sont stockées, d'introduire dans les serveurs des virus[18], de transmettre à un système informatique des communications qui portent atteinte aux données du système ou en entravent le bon fonctionnement.

---

[16] V. sur cette question, U. Sieber, Les Crimes informatiques et d'autres crimes dans le domaine de la technologie informatique R I DP 1993 p. 53.
Cet auteur a montré que contrairement aux biens corporels qui normalement sont attribués exclusivement à une certaine personne déterminée, l'information est plutôt un bien public, qui par principe, doit être libre. Il en déduit qu'on ne doit pas la protéger par des droits d'exclusivité.

[17] V. par exemple la France où la loi n° 88-19 du 5 janvier, 1988 dite loi Godfrain dont les dispositions ont été remaniées et introduites dans le nouveau Code pénal. Il existe désormais en France un dispositif permettant de réprimer les intrusions dans un système ainsi que les altérations de données.

[18] Pour une étude détaillée des fraudes qui peuvent se rencontrer sur l'Internet. V. Bary, Internet et la fraude informatique – RFC 1996. p. 40.

A ce problème de protection du contenu des données, qu'elles soient nominatives ou créatives[19], s'ajoute celui de la protection contre le contenu des données. Il ne fait pas de doute qu'il y a actuellement circulation dans l'espace électronique d'informations portant atteinte à l'ordre public et aux bonnes mœurs[20], ayant un contenu antisémite ou révisionniste, en violation de la législation de certains Etats[21] ou comportant des propos diffamatoires ou injurieux[22]

---

[19] Sur la distinction données nominatives et données créatives V. Nicoleau, La protection des données sur les autoroutes de l'information. D.S. 1996 Chron. 111.

[20] V. par exemple l'affaire qui a donné lieu au jugement d'un tribunal du Tennessee aux Etats-Unis (United States V. Thoms, W. D. Tenn., july 28, 1994 The Int. Comp. Lawer oct. , 1994, p. 36 (cité par Piette-Coudol et Bertrand. Coll. Dalloz service 1996. p. 61). Dans cette affaire le tribunal a condamné pour atteinte aux bonnes mœurs un coupe qui avait stocké dans « Un babillard » des images osées. Voir aussi le jugement rendu par le tribunal correctionnel du Mans (France) le 16 février 1998 (inédit) qui a condamné, pour recel d'objet provenant de la diffusion d'image d'un mineur à caractère pornographique, un cadre qui utilisait l'ordinateur de son employeur (le conseil général) pour télécharger des images mettant en scène des viols de mineurs. V. aussi l'arrêt rendu par la deuxième chambre correctionnelle de la Cour d'Appel de Paris le 2 avril 2002 (E c/ Ministère Public accessible sur le site www.juriscom.net). Dans cet arrêt la Cour d'Appel de Paris a, en application de l'article 227-24 du Nouveau Code Pénal, condamné à une amende de 30 000 Euros le gérant d'une société ayant diffusé des messages pornographiques et des messages de nature à porter atteinte à la dignité humaine, messages susceptibles d'être vus ou perçus par des mineurs.

[21] V. en France Trib. Corr. Paris 26 février 2002 disponible sur http : // www. Foruminternet.org. Ce jugement a été rendu à la suite de poursuites (citation directe) déclenchées par l'association «Amicale des déportés d'Auchwitz et des camps de Haute Silésie ». Se fondant sur le maintien délibéré, sur le site Internet Yahoo.com propriété de la société Yahoo.Inc, d'un service de vente aux enchères d'objets nazis, cette Association a exercé des poursuites des chefs « de délits d'apologie de crime de guerre, contre l'humanité ou de crimes ou délits de collaboration avec l'ennemi » et « de contravention connexe d'exhibition en public d'insignes ou d'emblèmes qui ont été portés ou exhibés par les membres d'une organisation déclarée criminelle en application de l'article 9 du Statut du Tribunal Militaire annexé à l'accord de Londres du 8 août 1945 »

V. aussi en matière civileTGI de Paris, ord. De référé du 12 juin 1996, Les petites affiches du 10 juil. 1996 p. 22 Obs H. Maisl, l'Union des étudiants juifs de France (UEJF) avait demandé au juge des référés d' »enjoindre aux providers de ne plus reprendre les news groupes et sites Web américains qui diffusaient des informations antisémites et révisionnistes.

TGI Paris, ord. de référé, 22 mai 2000 Communication, Commerce électronique, sept. 2000, Commentaires, n° 92 p. 19, note J.- C. Galloux. Cette ordonnance fait suite à une demande de la Ligue contre le racisme et l'antisémitisme (LICRA) et l'Union des Etudiants Juifs de France (UEJF) tendant à obtenir du juge des référés du Tribunal de Grande Instance de Paris une mesure interdisant aux sociétés Yahoo Inc. et Yahoo France de permettre aux internautes français l'accès à des sites sur lesquels étaient proposés à la vente aux enchères des objets représentant des symboles de l'idéologie nazie.

[22] V ; par exemple l'affaire qui a donné lieu au jugement du tribunal correctionnel de Meaux en date du 19 novembre 2001.(accessible sur le site www.juriscom.net). Une personne avait créé un site Internet pour y faire apparaître les visages des collègues de travail dont certains sont représentés dans des scènes pornographiques et d'autres sous l'apparence de singes, ceci après manipulation de photos. V. aussi l'affaire qui a donné au jugement du tribunal d'instance de Plateaux en date du 28 septembre 1999 (AXA Conseil … et AXA Conseil Vie c/ Monsieur C.M. ; Monsieur D.S., PCA de la société informe, http://www.fiurnisseur.free.fr/JP-ti. Juste aux 280999 ex Lt.html). une personne avait rédigé un message intitulé comment AXA prend les gens pour des C. « et important à la société AXA et à sa filiale française

La législation existante dans la plupart des Etats permet de sanctionner de tels types d'agissements[23]. S'il existe une difficulté, c'est au niveau de l'exercice des poursuites, car il n'est pas toujours aisé de déterminer, compte tenu du nombre important d'intervenant, celui qui doit être tenu pour responsable.

Il ne fait pas de doute que la détermination de l'auteur de l'acte et l'exercice des poursuites peuvent s'effectuer facilement lorsqu'il s'agit d'actes consistant à accéder et à se maintenir dans un système. Mais la situation est tout à fait différente lorsqu'il y a utilisation de l'espace électronique pour véhiculer certaines informations.

Entre les auteurs des messages au contenu illicite dont l'identité n'est d'ailleurs pas toujours connue, les serveurs qui fournissent les informations, les fournisseurs d'accès[24], les fournisseurs d'hébergement[25] et le consommateur final il n'est pas facile de choisir. Le choix est d'autant plus compliqué que dans certains cas, « entre l'auteur et le consommateur final, les informations peuvent être relayées plusieurs fois »[26], les serveurs

---

AXA conseil des pratiques peu recommandables (mépris à l'égard des clients et des salariés, pratiques des gangsters, pratiques assimilables à de l'escroquerie, etc.). Ce message a été mis en ligne par cette personne a partir de sa page personnelle grâce aux moyens techniques mis à sa disposition par un fournisseur d'hébergement.

[23] En France la loi du 29 juillet 1881 sur la presse est applicable à l'utilisation des moyens de communication audiovisuelle pour diffuser de telles informations. Au Sénégal les articles 248 et suivants du Code pénal.

En Allemagne le législateur réprime la glorification de la violence et l'incitation à la haine raciale.

[24] On peut emprunter une définition à la loi française du 30 sept. 1986 dans sa rédaction issue de la loi 2000-719 du 1er août 2000 : personne dont l'activité consiste à offrir un accès à des services de communication en ligne autres que des correspondances privées ; d'après un auteur, cette définition correspond au fournisseur d'accès (V. E. Tois, Internet et Libertés, Quelques repères, in Rapport annuel de la Cour de Cassation, 2001, http : // www.cour de cassation.fr/_rapport01/etudes&doc/TOIS.htm).

[25] Pour reprendre la loi française de 1986, on peut dire qu'il s'agit de personne « assurant, à titre gratuit ou onéreux le stockage direct et permanent pour mise à disposition du public de signaux, d'écrits, d'images, de sons ou de messages de toute nature accessibles par ces services ».

[26] Piette-Coudol et Bertrand op. cit., p. 119.

faisant l'objet, lorsqu'il sont souvent sollicités, de duplications sur des sites miroirs.

Les prestataires de service soutiennent parfois que « dans la logique de l'Internet, celui qui met en ligne des données ne doit pas être inquiété [car] ce sont les internautes qui seuls ont un rôle actif et sont libres ou non de consulter lesdites données »[27].

Cette conception qui conduit à une « déresponsabilisation » totale des intermédiaires est inacceptable. Comme on l'a fait remarquer[28], « … sur ces nouveaux médiats, comme on sur les médiats traditionnels, la publicité donnée aux informations et la présence d'intermédiaire permettant aussi bien la réalisation de cette publication que l'accès des utilisateurs à l'information invitent à s'interroger sur une responsabilité d'ordre « éditorial » pour les intervenants que sont : fournisseurs d'accès, fournisseurs d'hébergement, fournisseur d'instrument, exploitant de moteurs de recherche… ».

On peut penser que cette responsabilité de type éditorial peut être envisagée dans des pays comme la France. L'on sait que dans ce pays, le régime de la responsabilité éditoriale résultant pour la presse de la loi du 29 juillet 1881 a été transposée au service de communication audiovisuelle par la loi du 29 juillet 1982. Or ce régime semble à priori transposable à l'ensemble des services disponibles sur les réseaux Internet, l'article 2 de la loi du 30 septembre 1986 définissant la communication audiovisuelle d'une manière suffisamment large pour englober ces services ; il est question en effet de « toute mise à disposition du public ou des catégories

[27] V. Vivant et le Stanc, Droit de l'information JCP 1997 – I Chron. N° 657.
[28] J. Huet, Quelle culture dans le « cyber – espace » et quels droits intellectuels pour cette « cyber - culture ? » D. S. 1998, Chron. P. 185.

de public par un procédé de télécommunication, de signes, de signaux, d'écrits, d'images de sons ou de messages de toute nature qui n'ont pas le caractère d'une correspondance privée »[29]. En cette matière le système de responsabilité en cascade désigne comme auteur principal le directeur de publication lorsque le message incriminé a fait l'objet d'une fixation préalable à sa communication au public[30] ; si cette condition n'est pas satisfaite, la responsabilité incombe à l'auteur principal et subsidiairement au complice.

Il ne faut cependant pas perdre de vue qu'avec la loi n° 2000-719 du 1er août 2000 modifiant la loi du 30 septembre 1986 relative à la liberté de la communication, la responsabilité pénale des intermédiaires ne peut être engagée de manière exceptionnelle. En effet lorsque le contenu d'un site est illicite, le fournisseur d'hébergement ne peut être déclaré pénalement (et civilement) responsable que si, ayant été saisi par une autorité judiciaire, il n'a pas agi promptement pour empêcher l'accès à ce contenu ; quant au fournisseur d'accès, il ne peut être pénalement responsable.[31]

Toutes les fois que la responsabilité pénale des intermédiaires est écartée, comme c'est souvent le cas, il ne restera que celle de l'auteur du message au contenu illicite. Hélas, l'identification de cet auteur se révèle

[29] Des réserves sont cependant émises quant à une possibilité de transposition. Il ressort en effet du rapport d'information fait, au nom de la mission commune sur l'entrée dans la société de l'information (sénat français) par Alain Joyaudet, Pierre Herisson et Alex Truk (http://www.senat.fr./rap/r96-43621.html) qu'il n'est pas évident que les dispositions de la loi de 1982 qui définissent le système de responsabilité en cascade dans le domaine de la communication audiovisuelle puissent s'appliquer sur Internet. Selon les auteurs du rapport, ces dispositions visent les intervenants d'une production audiovisuelle dans son acception classique où les rôles sont clairement distribués, alors que sur l'Internet la chaîne des intervenants peut être plus élaborée et que la confusion des rôles y est fréquente.

[30] Dans ce cas l'auteur est complice.

[31] La situation des intermédiaires est clairement décrite par Mme Le Professeur Marie Anne Frison-Roche (Nouvelles obligations pour les acteurs de l'Internet, Le Monde du 4 septembre 2000) en ces termes : « lorsque le contenu d'un site est contraire au droit, la responsabilité du fournisseur du site est automatique s'il ne réagit pas à l'ordre du juge et peut être non seulement civile mais encore pénale, alors que la responsabilité du fournisseur d'accès suppose l'établissement d'une faute et ne peut être que civile ».

souvent délicate même si la législation française a, pour faciliter la tâche des autorités judiciaires, mis à la charge des fournisseurs d'accès et des fournisseurs d'hébergement l'obligation de déterminer et de conserver les données de nature à permettre l'identification de toute personne ayant contribué à la création d'un contenu des services dont [ils] sont prestataires[32].

En dehors des textes permettant la mise en œuvre de la responsabilité de type éditorial, il existe, dans certains pays, des textes permettant incontestablement de retenir la responsabilité pénale de ceux qui rendent techniquement possible l'accès à certaines informations, même s'ils n'étaient pas destinés à titre principal à fixer les principes de détermination des personnes responsables. Il suffit pour s'en convaincre, de lire les articles 383 bis et 383 quinquies du Code pénal belge consacrés respectivement à la répression de la traite des être humains et de la pornographie enfantine et à la répression de la publicité et / ou la distribution de produits pornographiques impliquant ou non des mineurs.

L'article 383 bis, réprime les personnes qui auront « exposé, vendu, loué, distribué ou remis des emblèmes, objets… ou autres supports visuels qui représentent des positions ou des actes sexuels à caractère pornographique impliquant ou représentant des mineurs… ou les aura, en vue de la distribution ou du commerce, fabriqué ou détenu, importé ou fait importer, remis à un agent de distribution ».

Quant à l'art. 383 quinquies, il prévoit une peine d'emprisonnement pour toute personne qui « quel qu'en soit le moyen, fait ou fait faire, publie, distribue ou diffuse de la publicité, de façon directe ou indirecte, même en

[32] Art. 43-9 nouveau de la loi n° 86-1067 du 30 septembre 1986

dissimulant la nature sous des artifices de langages, pour une offre de services à caractère sexuel ayant un but lucratif direct ou indirect, lorsque ces services sont fournis par un moyen de télécommunication ».

Ces textes sont conçus en termes tellement généraux qu'ils permettent d'atteindre les émetteurs de message contenant des données illicites telles qu'elles y sont définies ainsi que ceux qui donnent accès à de tels messages. Ils permettent aussi, dans une certaine mesure, de retenir la responsabilité de celui qui consulte le message puisque la possession, en connaissance de cause ,d'emblèmes, objets, films, photos, diapositives ou autre support visuel représentant des actes sexuels impliquant des mineurs rentre dans les prévisions de la loi. On peut parfaitement, dans ces conditions, envisager la poursuite d'une personne détenant des photos représentant de tels actes après les avoir téléchargés sur Internet.

L'efficacité des solutions qui consistent à déterminer la responsabilité en s'appuyant sur des textes de cette nature est cependant doublement limitée.

La première limite tient au fait que de tels textes ont un champ d'application très restreint. Le domaine de ces textes est limité aux seuls messages liés à la pornographie ou à la pédophilie de telle sorte qu'il est impossible de les mettre en œuvre lorsqu'il s'agit de réprimer l'auteur d'un message illicite mais sans rapport avec les pratiques visées. Il faut donc nécessairement adopter un texte de portée générale permettant de définir de manière claire la responsabilité des différents acteurs.

L'autre limite résulte de la diversité des législations. Si en Belgique il est possible de poursuivre un intermédiaire qui a permis la mise en ligne

ou l'accès à des images de caractère pornographique, il ne semble pas en être de même dans d'autres pays. Il a été jugé, par exemple aux Pays-Bas que les prestataires d'accès à Internet ne peuvent être considérés comme responsables des actes illicites commis par les utilisateurs[33].

On perçoit immédiatement la limite d'une solution conçue seulement au plan interne. Il suffit que celui qui a mis en ligne le message se trouve aux Pays-Bas pour que toute poursuite en Belgique soit impossible.

B – La localisation de l'infraction

En l'absence de règle de Droit International Public fixant la compétence internationale des juridictions, il appartient à chaque Etat de dire quelles sont les infractions présentant un élément d'extranéité qui peuvent être jugées par les juridictions relevant de sa souveraineté. Presque tous les Etats sont attachés au principe de la territorialité[34] [35] qui veut que la « loi pénale s'applique à tous les individus quelle que soit leur

[33] Pour un résumé de la décision du tribunal du district de la Haye du 12 mars 1996 V. GP 1996. 2 – p.9.

[34] En Italie, l'article 6 du Code Pénal énonce le principe de l'application territoriale ; en effet toute personne qui a commis un délit sur le territoire italien. est punissable selon la loi italienne (V. Instrument juridiques pour lutter contre le racisme sur Internet, rapport établi par l'Institut suisse de droit comparé, http://www.coe.int../…3. mesures -juridiques-nationales/2Racisme sur_internet). En France le principe de territorialité est consacré dans les articles 113 -2 et suivants NCP. Il résulte de ces dispositions que les juridictions françaises sont compétentes pour juger les infractions commises sur le territoire français (l'infraction est réputée commise en France si l'un de ses faits constitutifs a eu lieu sur ce territoire) et les actes de complicité accomplis en France d'un crime ou d'un délit commis à l'étranger si ce fait principal est puni à la fois par la loi française et par loi étrangère et s'il a été constaté par une décision définitive de la juridiction étrangère.

[35] Malgré leur attachement au principe de territorialité, les Etats prévoient aussi des compétences extraterritoriales fondées sur la nationalité des protagonistes (compétence personnelle active par laquelle un Etat confie à es tribunaux le jugement d'une infraction commise à l'étranger et compétence personnelle passive par laquelle un Etat donne à ses tribunaux le pouvoir de juger une infraction commise à l'étranger au préjudice de son ressortissant) ou l'impératif de protection de leur intérêt supérieur (compétence réelle par laquelle un Etat confie à ses tribunaux le jugement des atteintes à sa monnaie, son sceau ou sa sûreté ; V. par exemple art. 667 du CPP Sénégalais).

nationalité ou celle de leurs victimes, qui ont commis une infraction sur le territoire de l'Etat où cette loi est en vigueur[36].

La mise en œuvre de ce principe pose cependant des problèmes dans certains cas ; il n'est pas en effet toujours aisé de déterminer le lieu de commission de l'infraction. Comme on l'a fait observer[37], « de même qu'une activité délictueuse peut se prolonger dans le temps et s'y exprimer par des actes ou des états successifs, il lui arrive d'éclater dans l'espace et de se situer à la foi en deux lieux différents… ». Si les divers éléments d'une même activité criminelle sont situés sur des territoires différents, il sera difficile de localiser l'infraction.

On comprend aisément pourquoi les infractions commises au moyen des nouvelles technologies de l'information posent autant de problème de compétence. L'utilisation des réseaux entraîne inévitablement des flux transfrontaliers de données et généralise l'internationalisation des infractions. Il arrive souvent par exemple que celui qui met en ligne l'information illicite reçue dans un pays donné se trouve dans un autre pays. L'infraction est-elle commise dans le pays ou l'information est mise en ligne ou doit-on considérer qu'elle est commise dans le pays où elle est reçue ?

En France à la question de savoir si le fait qu'une information illicite puisse être reçue sur le territoire français par l'intermédiaire du réseau Internet constitue cet élément de rattachement indispensable à l'application de la loi française et donc à la compétence des juridictions

[36] V. Merle et Vitu, Traité de Droit criminel T. 1 – Problèmes généraux de la science criminelle – Droit Pénal Général – Paris Cujas 6ème édit. 1988 n° 277 p. 372.
[37] Merle et Vitu op. Cit.

françaises, un auteur[38] a répondu par l'affirmative ; selon lui, « la jurisprudence a une conception particulièrement extensive de la notion de critère de rattachement, n'hésitant pas parfois à « disséquer » certaines infractions afin de les rendre françaises ». Une juridiction [39] a adopté ce raisonnement dans le jugement rendu à propos des poursuites dirigées contre le PDG de la société Yahoo par une association d'anciens déportés d'Auchwitz. Dans ce jugement le tribunal, a commencé par constater que la mise à disposition du public d'un site de vente aux enchères d'objets nazis, qui peut être vu et reçu sur le territoire national et auquel l'internaute peut accéder, du fait de la simple existence d'un lien informatique « search » qui l'y invite, caractérise l'élément de publicité nécessaire à la constitution du délit d'apologie de crime de guerre, et ce, sans qu'il soit besoin que l'internaute soit spécialement démarché par le propriétaire du site » ; il en a déduit ensuite que cet élément de publicité suffit « à emporter la compétence des tribunaux français et l'application de la loi pénale française ».

Cette tendance des juridictions à « atomiser » les infractions pour trouver un élément de rattachement justifiant leur compétence n'est pas une spécialité française. En Australie la Cour Suprême a jugé que les responsables de la publication d'informations jugées diffamatoires relèvent de la compétence des tribunaux où ces informations sont lues[40]. Cette décision a été rendue dans une affaire où une personne vivant en Autriche se plaignait de la parution dans la version électronique du Barron's magazine, par l'intermédiaire de l'agence de presse américaine Dow Jones, d'un article dont le contenu était, à son avis, diffamatoire.

[38] Sébastien Canevet, Fourniture d'accès à l'Internet et Responsabilité pénale, http : //www.canvet.com/doctrine/resp-fai.htm
[39] Trib corr. Paris 26 février 2002, précit.
[40] V. N. Rolland, Quel tribunal pour apprécier la liberté d'expression dans le cyberespace ? L'audace (payante ?) de la jurisprudence autrichienne, http : //www.droit-technologie.org/1_2.asp ?actu_id :708

Face à la diversité des réponses apportées, par les différentes législations, aux problèmes de localisation de l'acte[41], les risques de conflit de compétence sont importants, ce qui est nature à gêner la répression.

Il ne suffit plus d'ailleurs pas de régler les questions de compétence pour éviter les problèmes rencontrés pour la répression. La diversité des règles pénales de fond est, elle aussi, source de vide. Un seul exemple suffit pour illustrer cette possible impunité des délinquants. Un nostalgique du nazisme installé dans un pays où la liberté d'expression ne connaît pas de limite met en ligne, de façon tout à fait légale[42] à partir de ce pays, des propos racistes qui sont reçus en France où la législation[43] incrimine les provocations à la haine raciale par tous supports écrits ou moyens de communication audiovisuelle.

Les juridictions françaises sont certainement compétentes pour juger l'auteur de tels propos compte tenu des dispositions de l'article 113-2 du nouveau Code pénal ainsi conçu : « La loi pénale française est applicable aux infractions commises sur le territoire de la République ».[44]

---

[41] Trois solutions sont concevables en matière de localisation des infractions :
celle qui consiste à localiser l'infraction au lieu où l'agent a agi (théorie de l'action) ;
celle qui consiste à localiser l'infraction au lieu où le comportement de l'agent a produit le dommage (théorie du résultat) ;
celle qui consiste à localiser l'infraction indifféremment aux lieux de manifestation de l'action et de la survenance du résultat (théorie de l'ubiquité).
Pour un exposé des différentes théories V. Huet et Koering-Joulin Droit Pénal international. Paris PUF 1993 n° 135 p. 218.
En Allemagne le lieu de commission de l'infraction est défini soit comme le lieu où le malfaiteur a agi, soit comme le lieu où les conséquences de son acte se sont matérialisées ou étaient censées se matérialiser. V. rapport de l'Institut suisse de droit comparé (Instruments juridiques pour lutter contre le racisme sur Internet) précit.
En Italie une infraction doit être considérée comme commise sur le territoire lorsque l'acte ou l'omission y a lieu en tout ou en partie ou lorsque l'événement qui en est la conséquence s'y est produit (Art. 6 al. 2 ; V. Rapport de l'Institut suisse de droit comparé précit.

[42] Aux Etats-Unis la liberté d'expression et de communication est solidement garantie et toutes les tentatives de répression de la transmission de certains messages sont nouées à l'échec.

[43] Loi du 29 juillet 1881.

[44] V. Trib. corr. Paris 26 février 2002 précit.

Pourtant même si leur compétence est retenue, les autorités judiciaires françaises pourront difficilement exercer les poursuites. L'auteur de l'infraction étant par définition à l'étranger, sa comparution est subordonnée à une décision d'extradition prise par les autorités du pays sur le territoire duquel l'acte a eu lieu. Or cette décision se heurte à plusieurs obstacles.

Il y a un premier obstacle lié à la nationalité de l'auteur des propos. Il existe un principe fondamental que l'on trouve dans la plupart des conventions d'extradition et dans de nombreuses lois nationales ; ce principe veut que l'Etat requis ne puisse pas donner suite à une demande d'extradition qui vise un de ses nationaux[45]. Il en résulte que si l'auteur est ressortissant du pays où l'acte a été commis, il ne pourra jamais être jugé en France. Certes certaines conventions énoncent, pour éviter l'impunité du délinquant, que si l'intéressé est un national de l'Etat requis, cet Etat, à la demande de l'Etat requérant, soumet l'affaire aux autorités compétentes afin que des poursuites soient exercées s'il y a lieu[46]. Mais il ne faut pas perdre de vue que de telles conventions n'imposent pas toujours les poursuites à l'Etat requis.

Un autre obstacle à l'extradition résulte de l'exigence d'une double incrimination des faits. Il ne suffit pas que les faits soient pénalement qualifiés par l'Etat requérant ; il faut aussi qu'ils supportent une qualification pénale au regard de la législation de l'Etat requis. Les faits

[45] Il semble cependant que les systèmes anglo-saxons ignorent ce principe ; V. Huet et Koering-Joulin op ; cit ; n° 240 p. 357.

[46] V. Huet et Koering-Joulin op. Cit. N° 206, p. 317 qui donnent l'exemple de l'article 6 de la Convention européenne d'extradition.
En vertu du principe « aut dedere aut judicare (extrader ou poursuivre) consacré par plusieurs conventions, si l'extradition demandée par un Etat partie est rejetée, l'Etat requis doit, à la demande du représentant, soumettre à ses autorités judiciaires aux fais de poursuites

n'étant pas par définition punis par l'Etat requis, cette règle protège même l'auteur des faits qui n'a pas la nationalité de cet Etat.

Il convient de signaler enfin un obstacle tenant à la mise en œuvre des règles de compétence internationale. L'on sait que certaines conventions d'extradition et certaines légalisations internes prévoient la faculté pour l'Etat requis de refuser l'extradition lorsque la réciprocité de compétence fait défaut. Il suffit donc que la compétence des juridictions de l'Etat requérant soit fondée sur une règle qui n'est pas consacrée par l'Etat requérant pour que la demande d'extradition ne soit pas suivie d'effet.

L'exercice des poursuites apparaît ainsi comme un véritable parcours du combattant lorsque l'infraction est localisée à l'étranger ; or très souvent en cas d'utilisation des nouvelles technologies à des fins criminelles, l'infraction est localisée à l'étranger. Face aux graves menaces que font peser sur la communauté internationale les agissements de cette nature, la collaboration des Etats nous paraît indispensable. Elle pourrait prendre la forme d'une convention universelle répressive comportant des stipulations relatives au droit matériel (détermination des agissements à incriminer et de la catégorie de personnes auxquelles ils peuvent être imputés) et aux questions de compétence que les Etats signataires seraient tenus de prendre en compte dans leur législation interne.

Pour l'heure il y a la convention sur la cybercriminalité[47] adoptée par le comité des Ministres du Conseil de l'Europe à l'occasion de sa 109ème session et ouverte à la signature à Budapest le 23 novembre 2001 à l'occasion de la Conférence internationale sur la cybercriminalité. Mais cette convention est loin d'avoir un caractère universel puisqu'elle concerne pour l'instant les pays membres du Conseil de l'Europe ainsi que

[47] (STE n° 185)

le Canada, le Japon, l'Afrique du Sud et les Etats-Unis qui bien qu'ils n'étaient pas membres du Conseil de l'Europe l'ont signée. Cette convention vise pour l'essentiel trois objectifs :

- d'abord l'amélioration des moyens de prévention et de répression de la criminalité informatique par l'adoption des normes minimales destinées à être intégrées dans les législations internes ;

- ensuite l'accroissement de l'efficacité des procédures par l'élaboration de mesures à prendre au niveau national aux fins d'enquête et de poursuites des infractions liées aux nouvelles technologies ;

- enfin la mise en place d'un régime rapide et efficace de coopération internationale[48].

L'harmonisation des règles de droit matériel et des règles de compétence indispensable dans le contexte actuel devrait s'accompagner d'un engagement des Etats de mettre en œuvre tous moyens propres afin de créer les conditions d'une entraide répressive internationale efficace. Cet effort est d'autant plus nécessaire que, contrairement à l'opinion de certains auteurs[49] qui croient avoir décelé à travers l'évolution des idées depuis un demi-siècle, des signes de déclin du principe d'inefficacité des décisions rendues à l'étranger, on est obligé de constater que le rayonnement des sentences pénales dépasse rarement le cadre des frontières de l'Etat où elles sont intervenues[50]. En effet les Etats refusent, se plaçant dans une optique purement nationaliste, de faire produire au plan interne les sentences rendues à l'étranger.

[48] V. Convention sur la cybercriminalité, Rapport explicatif, http://www.conventions.coe.int/treaty/fr./Reports/html/185.htm.
[49] Merle et Vitu, op. cit. n° 333, p. 445.
[50] Le phénomène n'est pas propre aux décisions portant condamnation des auteurs d'agissements liés aux nouvelles technologies, mais il revêt une signification particulière dans ce domaine compte tenu des enjeux.

C'est ce qui explique le refus des Etats de reconnaître une autorité positive aux sentences rendues à l'étranger. Ainsi la condamnation prononcée contre une personne dans un pays donné ne peut être considérée comme le premier terme de la récidive dans un autre pays.

Cette réticence constatée dans l'attitude des Etats à l'égard de l'autorité positive de la chose jugée se retrouve aussi en matière d'exécution. En effet les Etats refusent de prêter leur concours pour l'exécution des sentences rendues à l'étranger.

L'impunité de ceux qui utilisent les nouvelles technologies à des fins criminelles est, dans ces conditions, quasiment assurée. Il leur suffit, pour être définitivement à l'abri, de ne pas se rendre dans le pays où leur activité criminelle a produit ses effets et où une condamnation a été prononcée contre eux.

Une convention répressive universelle prenant en compte les spécificités de cette forme de criminalité serait là aussi indispensable ; elle pourrait prévoir des règles ayant pour objet, non seulement de mettre à la charge des Etats signataires l'obligation de prendre en considération les effets des décisions rendues à l'étranger, mais aussi de fixer les règles de recherche des preuves qui se trouvent à l'étranger. A défaut, les preuves permettant d'asseoir la culpabilité des adeptes de la criminalité sur Internet seraient toujours introuvables. Ce qui constitue, il faut le reconnaître, un autre facteur de l'impunité.

II - DES PREUVES INTROUVABLES

On a toujours souligné les difficultés concrètes de détection des délits et d'identification de leurs auteurs lorsque ceux-ci ont eu recours aux nouvelles technologies, mais il ne semble pas qu'on ait à ce jour trouvé des solutions adéquates. En effet devant l'insuffisance des procédés classiques de recherche des preuves, les autorités policières et judiciaires tentent d'utiliser elles-mêmes les nouvelles technologies pour leurs investigations, mais l'efficacité de telles méthodes est très limitée.

A – L'insuffisance des méthodes d'investigations classiques face aux infractions commises au moyen des nouvelles technologies

Même en cas de commission d'une infraction au moyen des nouvelles technologies, les autorités chargées de la recherche des preuves mènent l'enquête dans le cadre d'actes classiques de la procédure pénale[51] : constatations matérielles, perquisitions, saisies etc. Le recours à ces procédés de recherche se révèle souvent inapproprié en raison de l'immatérialité de l'objet de l'activité et de la localisation des éléments de preuve.

1° - L'immatérialité de l'objet

L'accomplissement des actes classiques peut, sans doute, se révéler efficace dans le cadre d'une procédure menée pour rechercher les preuves d'une infraction ayant pour objet le support de l'information. Après

[51] Padouin, Lutter contre la criminalité sur les systèmes d'information : La police judiciaire RFC 1996, p. 66.

tout, il n'y a aucune différence entre le vol d'une disquette ou d'un C. D – Rom et le vol d'un objet mobilier quelconque.

En revanche, lorsqu'il s'agit de réunir des preuves contre une personne poursuivie pour avoir manipulé le système informatisé d'autrui ou pour avoir stocké et transmis des informations illicites, les méthodes classiques peuvent se révéler tout à fait inappropriées.

En réglementant les perquisitions, on a généralement en vue la découverte d'objets provenant de l'infraction ou ayant servi à la commettre. Manifestement, une telle mesure ne peut être prise lorsqu'il s'agit de se rendre dans un « lieu virtuel », où tout est immatériel.

La même observation peut être faite à propos des saisies. L'on sait que lorsque la perquisition effectuée révèle l'existence d'objets susceptibles de servir à la manifestation de la vérité, il peut être procédé à leur saisie, en observant un certain nombre de formalités telles que la mise sous scellé. Une telle mesure conçue pour des objets corporels peut difficilement être mise en œuvre pour les besoins d'une procédure initiée par exemple contre l'auteur du stockage et de la transmission d'informations illicites. On peut, il est vrai envisager la saisie des supports des informations ; mais une telle saisie englobe t-elle celle des informations qu'ils sont supposés contenir ? La question reste posée, même si une réponse positive semble devoir être donnée dans certains pays[52]. En tout état de cause, une mesure de cette nature est tout à fait inconcevable lorsqu'il s'agit de données non fixées sur un support. C'est d'ailleurs parce qu'il a pris conscience de ce phénomène que le comité des

[52] V. pour le Luxembourg – M. Jaeger, Les Crimes informatiques et d'autres crimes dans le domaine de la technologie informatique au Luxembourg. RTDP 1993. p. 451.

ministres du conseil de l'Europe a rappelé, dans la Recommandation n° R (95) 13[53], la nécessité d'adapter les règles de procédure pénale afin « de permettre aux autorités chargées de l'enquête de perquisitionner dans les systèmes informatiques et d'y saisir des données, dans des conditions similaires à celles utilisées dans le cadre des pouvoirs traditionnels de perquisition de perquisition et de saisie ».

On peut noter à ce sujet que cette nécessaire adaptation des règles de procédure n'est pas absente des préoccupations des signataires de la convention sur la cybercriminalité[54]. En effet, partant de l'idée qu'il est extrêmement difficile d'identifier l'auteur de l'infraction et d'évaluer l'impact ou la portée de celle-ci ou de trouver des données électroniques intactes en raison de leur caractère volatile[55], ils ont opté non seulement pour l'adaptation des procédures classiques telles que les perquisitions et saisies au contexte technologique actuel, mais aussi et surtout pour de nouvelles mesures telles que celles qui tendent à la conservation des données[56], à la collecte des données relatives au trafic[57], à l'interception des données relatives au contenu[58] et l'injonction de produire[59].

---

[53] Il s'agit du principe du chapitre I de la Recommandation n° R (95) 13 relative aux problèmes de procédure pénale liés à la technologie de l'information.

[54] Conseil de l'Europe (STE n° 185) précit.

[55] Cette volatilité s'explique par les possibilités de modification, de déplacement ou de destruction.

[56] Conserver les données signifie garder les données qui existent déjà sous une forme stockée en les protégeant contre tout ce qui pourrait en altérer ou en dégrader la qualité ou l'état actuel (Convention sur la cybercriminalité, rapport explicatif précit).

[57] Cela désigne toutes les données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication avec une indication relative à l'origine, à la destination, à l'itinéraire, à l'heure, à la date, à la durée de la communication ou au type de service. Cette mesure permet de déterminer la source ou la destination, ceci afin d'identifier les personnes auteurs des faits poursuivis.

[58] Ces données désignent le contenu informatif de la communication c'est à dire le message ou l'information transmis par la communication. Cela permet de constater certaines infractions comme la diffusion de pornographie infantile ou d'établir la preuve d'autres infractions telles que l'association de malfaiteurs, la contrebande, etc.

[59] C'est une mesure souple qu'il est possible de mettre en œuvre lorsque certaines mesures plus contraignantes se révèlent disproportionnées ou lorsque les tiers gardiens des données, tels que les fournisseurs d'accès ou d'hébergement sont disposés à collaborer sur une base volontaire mais souhaitent se prémunir contre les conséquences de leur collaboration (en disposant par exemple d'un moyen propre à leur permettre de s'exonérer d'une éventuelle responsabilité contractuelle).

L'adaptation des règles de procédure pénale est d'autant plus nécessaire que les délinquants ont recours à des méthodes de plus en plus sophistiquées pour rendre impossible la découverte de leurs agissements. C'est pourquoi la cryptologie constitue un enjeu considérable dans un environnement dématérialisé où la quasi-totalité des relations s'établit à travers des systèmes électroniques d'informations. La cryptologie qui « permet de chiffrer les messages et de maintenir leur confidentialité »[60] est assurément, à l'heure actuelle, l'un des moyens les plus sûrs pour assurer la sécurité des transactions qui se nouent dans l'espace électronique. Aussi, les utilisateurs réclament-ils sa libéralisation. Seulement elle peut aussi être utilisée à des fins criminelles. C'est ce qui explique que les pouvoirs publics se montrent souvent réservés face à une libéralisation totale de ce procédé.

En France, avec l'entrée en vigueur de la loi n° 96-659 du 26 juillet 1996[61], le régime applicable à la cryptologie a été assoupli[62] même si on ne peut pas encore parler de liberté totale. Comme on l'a souligné, en effet, « le dispositif oscille entre l'autorisation administrative et la pleine liberté en passant par la déclaration administrative selon le type de prestations, mais également selon les garanties de sécurité recherchées »[63].

[60] H. Maisl, De la télématique à Internet : Rupture ou continuité GP. 11 – 12 sept. 1996 p.57.
[61] J.O 27 juillet 1996.
[62] A l'origine avec le Décret-loi du 18 avril 1939 complété par le décret du 12 mars 1973, l'Etat français exerçait un contrôle sévère sur les précédés de cryptologie pour des raisons liées à la Défense nationale et la sûreté de intérieure.
[63] Piette-Coudol et Bertrand op. cit. pp 76-77.

Aux Etats-Unis, la législation sur le trafic international des armes (International Trafic in Arms Regulation) classe comme « munitions », dont l'exportation est soumise à autorisation, les logiciels de cryptage[64].

Malgré cette tentative d'encadrement du recours à la cryptologie, certains fabricants mettent au pont des logiciels du chiffrement qui assurent une protection même contre « les écoutes » légales[65]. En ce qui concerne certains malfaiteurs, ils n'ont pas attendu la vente de logiciels de chiffrement pour stocker dans leurs ordinateurs des données codées[66] auxquelles les autorités peuvent difficilement accéder en mettant en œuvre les moyens classiques[67].

Ces quelques difficultés recensées révèlent à quel point les autorités chargées de mener les enquêtes peuvent être démunies face jà la nouvelle forme de délinquance.

La situation est d'autant plus complexe que les éléments de preuve se trouvent le plus souvent à l'étranger.

2° - La localisation des éléments de preuve

Lorsqu'un nostalgique de nazisme décide, à partir d'un pays ou la liberté d'expression n'a pas de limite, d'inonder le monde entier de

[64] V. Nouel et Cousi, Au fil du Net GP 22-23 janv. 1997 p. 57.
[65] Maisl, Da la télématique à Internet art. précit. Selon cet auteur Philip Zimmerman a mis au point le logiciel de chiffrement Pretty Good Privaty qui offre des garanties même contre les écoutes légales. Ce logiciel est commercialisé sur Internet.
[66] U. Dieber, Les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique. RIDP 1993 p. 53.
[67] Dans la Recommandation 95 (13) du comité des ministres du conseil de l'Europe on peut lire ce passage qui est assez révélateur de la crainte suscitée par le chiffrement : « Des mesures devraient être examinées afin de minimiser les effets négatifs de l'utilisation du chiffrement sur les enquêtes des infractions pénales, sans toutefois avoir des conséquences plus que strictement nécessaires sur son utilisation légale »

message de caractère raciste, il peut, en utilisant les possibilités qu'offrent les nouvelles technologies de l'information, se faire entendre sur tous les points du globe. Les messages seront donc nécessairement reçus dans un pays ou on considère que la liberté d'expression ne peut autoriser certains excès notamment la provocation à la haine raciale. Si les autorités de ce pays décident d'engager des poursuites, il leur faudra au préalable résoudre un problème de taille : localiser l'auteur des messages et le territoire à partir duquel il les a mis en ligne. Il ne s'agit certes pas d'un problème insurmontable, mais il faut tout de même reconnaître que la tâche des autorités chargées de l'enquête ne sera pas aisée, compte tenu de la relative fiabilité des moyens techniques de repérage qui sont actuellement disponibles.

A supposer ce problème résolu, il faudra faire face à d'autres difficultés lorsque l'auteur présumé des messages et le site émetteur sont localisés à l'étranger. Dans une telle hypothèse il y a de fortes chances que les éléments de preuve se trouvent aussi à l'étranger ;, or le principe de la souveraineté des Etats s'oppose à ce que l'activité des autorités judiciaires ou policières relevant d'un Etat puisse s'exercer en dehors des frontières de cet Etat. Une « perquisition » des systèmes automatisés de traitement de l'information situés à l'étranger serait impensable. Il ne reste qu'une solution ; solliciter de l'Etat sur le territoire duquel est situé le site. (Commission rogatoire internationale, communication transfrontalière de pièces etc.). Mais on mesure immédiatement la faiblesse d'une telle solution ; on voit mal un Etat s'engager dans une entreprise d'entraide judiciaire ou policière qui conduit à la répression d'un agissement qu'il juge parfaitement licite.

La diversité des règles apparaît, là aussi, comme un facteur d'impunité de ceux qui se livrent à des activités illicites en utilisant les nouvelles technologies.

En attendant une harmonisation des législations, les autorités chargées des enquêtes n'ont d'autres ressources que d'utiliser elles aussi les mêmes méthodes que les délinquants, mais à des fins tout à fait différentes. C'est ce qui explique le recours de plus en plus fréquent aux nouvelles technologies pour les besoins des investigations ; mais cette solution est, compte tenu de l'environnement, d'une efficacité très limitée.

B – Les limites d'une recherche des preuves au moyen des nouvelles technologies de l'information

Le recours aux nouvelles technologies de l'information pour mener des investigations va certainement, en raison des possibilités qu'offrent ces outils, se généraliser et s'étendre même aux cas de poursuites dirigées contre les auteurs d'infractions classiques : trafic d'armes, trafic de drogues etc. Ce recours suscite deux interrogations majeures tenant l'une à la conformité à la loi des procédés utiles, et l'autre à la valeur des preuves obtenues au moyen de tels procédés.

1° - La légalité des procédés utilisés

Droit de compromis, la procédure pénale est caractérisée, dans tous les pays démocratiques, par la recherche d'un équilibre entre les exigences de la répression et la nécessité de protéger les libertés individuelles.

Il ne faut donc pas que dans le souci d'assurer une efficacité dans la recherche des preuves, les autorités chargées de conduire les investigations aient recours à des procédés de nature à porter atteinte aux droits fondamentaux de la personne humaine. C'est pourtant à un tel résultat que risque de conduire une utilisation systématique des moyens que procure les nouvelles technologies.

Il est relativement facile aujourd'hui d'intercepter des données lors de leur circulation dans les réseaux informatiques. Mais le recours à un tel procédé peut constituer une atteinte à un droit fondamental de l'homme reconnu et protégé par tous les instruments internationaux, le droit au respect de la vie privée et de la correspondance[68].

La règle contenue dans ces textes et garantissant aussi fondamental du domicile ne cède que sous certaines conditions, notamment l'existence d'une loi indiquant clairement en quelles circonstances et sous quelles conditions la puissance publique peut porter atteinte à la valeur protégée.

En l'absence de loi l'autorisant expressément, l'interception, pour les besoins d'une enquête, de messages mis en ligne soulève donc une question qui se pose dans les mêmes que celle qu'avait suscitée dans certains pays[69] (et que continue à susciter dans d'autres pays) l'interception des correspondances téléphoniques encore appelée écoutes

[68] V. par exemple 17-1 du pacte international relatif aux droits civils et politiques.
Art. 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.

[69] Pour prendre l'exemple de la France, la question de la légalité des écoutes téléphoniques avait été posée avant l'intervention de la loi du 10 juillet 1991 (JORF 13 juillet 1991 p. 91-67) qui a complété le code de procédure pénale. Avant l'entrée en vigueur de cette loi, la jurisprudence française avait admis la possibilité de recourir aux écoutes sous certaines conditions (Cass. Ass. Plen. 24 nov. 1989. D. S 1990-34 ; JCP 1990 II. 21418) ; mais la Cour européenne des droits de l'homme avait estimé dans un arrêt du 24 avril 1990 (DS 1990-353 Note Pradel) que le droit tel qu'il existait en France ne fournissait pas une sécurité juridique adéquate contre d'éventuels abus, faute de règles détaillées et claires en la matière ;ce qui a valu à la France une condamnation par cette juridiction.

téléphoniques. Il s'agit de la question de savoir si le recours à un tel procédé est licite. La réponse ne fait aucun doute. Elle doit être la même que pour les écoutes téléphoniques : à défaut d'un texte l'autorisant expressément, elle ne saurait être utilisée.

C'est pourquoi à notre avis, une interception effectuée dans un pays où aucune disposition légale ne la réglemente constitue une atteinte au droit au respect de la vie privée et du secret de la correspondance et doit, en tant que telle être considérée comme illégale. Il nous semble d'ailleurs que même l'existence d'une loi réglementant les écoutes téléphoniques ne saurait légitimer une interception des messages mis en ligne, car le principe de légalité régit aussi les lois de procédure. C'est ce qui explique, selon nous, l'un des principes formulés dans la Recommandation n° (95) 13[70] du Conseil de l'Europe : « Etant donné la convergence de la technologie de l'information et des télécommunications, les législations concernant la surveillance technique employée à des fins d'enquêtes pénales, comme l'interception des communications devraient être, là où cela s'avère nécessaire, révisées ou amendées pour assurer leur applicabilité.

La légalité de ce que l'on appelle [à tort] la perquisition dans les systèmes informatiques est tout aussi douteuse. Les autorités chargées de la constatation des infractions sont amenées parfois à accomplir des opérations non prévues par la loi en s'inspirant de règles applicables à des actes qui peuvent être légalement accomplis dans le cadre d'une enquête. Tel est le cas par exemple, de l'intrusion dans un système pour y effectuer

[70] Principe n° 5 chapitre II.

un « constat »[71]. Un tel acte s'apparentant à une perquisition, l'autorité chargée de l'enquête a tendance à s'inspirer des règles de la perquisition, mais elle ne peut pas les respecter toutes. C'est ce qui se passe dans les pays où la législation prévoit que la perquisition doit s'effectuer en présence de la personne chez laquelle elle a lieu[72]. Dans ces pays l'accès à un système afin de constituer une preuve ne se prête guère à ce type de formalisme : le délinquant qui a stocké des données compromettantes s'empressera certainement de les faire disparaître sitôt informé du projet.

Le débat sur la question de la régularité de l'accès à un système peut aussi être placé sur le terrain de l'inviolabilité du domicile. C'est ce qu'avait tenté de faire un jeune étudiant français qui, dans une affaire l'opposant aux titulaires de droits d'auteurs dont les œuvres étaient mises en ligne, soutenait que ses pages privées abritées par le serveur de son école constituaient son domicile virtuel[73], et que tout constat effectué à la suite d'un accès non autorisé devait être considéré comme irrégulier. Hélas, le juge des référés qui avait été saisi, ne s'est pas prononcé sur la valeur de cet argument au demeurant fort astucieux ; en effet, après en avoir souligné l'originalité, il a retenu qu'il devait faire l'objet d'un débat de fond[74] qui ne peut être mené que devant la juridiction saisie du fond de l'affaire.

Certes cette argumentation avait été développée dans le cadre d'une procédure devant le juge civil, mais rien ne s'oppose à ce qu'elle le soit dans le cadre d'une enquête pénale. En tout état de cause, la question

[71] Sur la manière de dresser un « constat » sur Internet. V. Gauthier – Note ss T GI paris Ord. De référé du 14 août 1996 DS 1996 – 491.
[72] V. par exemple 95 et suivants du code français de procédure pénale.
Art 86 et87 du code sénégalais de procédure pénale.
[73] V. l'affaire qui a donné lien à l'ordonnance de référé rendue par le premier vice-président du tribunal de Grande Instance de Paris du 14 août 1996 (D.S.) 1996. p. 491).
[74] Ce débat ne peur être mené devant le juge des référés qui avait été saisi de cette affaire.

de savoir si les pages privées d'un serveur constituent un domicile virtuel reste posée, tout au moins dans les pays où il n'y a pas de législations spécifiques.

L'autorité qui est amenée à s'introduire dans un système de traitement automatisé de données peut y découvrir des données nominatives dont on sait qu'elles font l'objet de mesures de protection dans certains pays. C'est par exemple le cas de la France où la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés[75] a mis en place un dispositif destiné à préserver les intérêts des personnes fichées : prohibition des mentions sensibles telles que l'origine raciale, les opinions politiques ou la religion ; reconnaissance de droits d'information, d'opposition et d'accès[76]. Il n'est pas facile de concilier l'ensemble de ces dispositions protectrices avec l'impératif d'efficacité qui implique le droit pour la police de recourir à la collecte, au stockage et à la coordination des renseignements nécessaires à la lutte contre le crime.

En dehors des obstacles juridiques qui peuvent se dresser devant l'exercice de l'activité des organes chargés de conduire les investigations, il existe des obstacles de fait tenant par exemple à ce que l'accès au système est subordonné à l'utilisation d'un code ou d'un mot de passe détenu par une personne qui refuse de le révéler. Pour lever cet obstacle, il est possible de recourir à des mesures coercitives pour contraindre l'intéressé à faire la révélation. Si le recours à de telles mesures peut se concevoir à l'égard d'un témoin, il n'en est pas de même lorsqu'il s'agit de la personne poursuivie. En effet la règle universellement admise selon

[75] Cette loi est en intégrée en partie (dispositions répressives) dans le nouveau code pénal (art. 226-16 et s.)
[76] Sur cette question V. Francillon, Les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique en France - RIDP 1993 p. 291.

laquelle nul ne peut être contraint de s'accuser lui-même s'oppose à ce que la personne poursuivie puisse faire l'objet d'une telle contrainte.

Il convient d'observer que dans certains pays les autorités ont pris des mesures appropriées pour adapter les règles de procédures au nouveau contexte. En Belgique par exemple le législateur est intervenu par une loi du 28 novembre 2000[77] pour mettre en place de nouvelles mesures permettant de faire face à des situations que le code d'Instruction Criminelle n'avait pas jusque là prises en compte. Avec cette loi[78] apparaissent des mesures nouvelles consistant à copier, rendre inaccessibles et retirer des données découvertes dans le système informatique. Ainsi lorsque les données découvertes dans le système informatique sont utiles et lorsque la saisie du support se révèle inappropriée, il pourra être procédé à leur copie ; celle-ci pourrait d'ailleurs être étendue[79] aux données nécessaires pour les comprendre (clé de déchiffrage ou outil de décodage des données qui seraient copiées dans un format intelligible ou encore logiciels ayant servi à la création des fichiers copiés)[80].

De même, il est possible d'utiliser des moyens techniques appropriés pour empêcher l'accès à certaines données ainsi qu'aux copies de ces données qui sont à la disposition des personnes autorisées à utiliser le système informatique ; dans le même ordre d'idée, il est possible de rendre inaccessible par l'utilisation de techniques appropriées, des

[77] Moniteur Belge 3 fév.2001, p.2909. cette loi relative à la criminalité informatique n'est pas seulement destinée à adapter la procédure pénale belge aux difficultés de la poursuite des infractions commises sur les réseaux informatiques ; elle a aussi pour objet de prévoir dans le code pénal des infractions spécifiques à l'informatique.

[78] V. pour une analyse de cette loi, Florence de Villefagne et Séverine Dussolier, La Belgique sort enfin ses armes contre la cybercriminalité : à propos de la loi du 28 novembre 2000 sur la criminalité informatique, http://www.droit-techologie.org.

[79] V. art. 39 bis § 2.

[80] F. de Villefagne et S. Dussolier, précit.

données qui forment l'objet d e l'infraction ou le produit de celle-ci et qui sont contraires à l'ordre public ou aux bonnes mœurs ou constituent un danger pour l'intégrité des systèmes informatiques[81].

Ces mesures pouvant porter atteinte aux droits des tiers, des dispositions prises pour assurer leur protection. Ainsi il est prévu[82] que le responsable du système informatique est informé de la recherche effectuée dans ledit système ; un résumé des données qui ont été copiées, rendues inaccessibles ou retirées lui est alors communiqué.

La loi nouvelle a également, en ajoutant un article 88 ter au Code d'Instruction criminelle, prévu la possibilité pour le juge d'instruction qui ordonne une recherche[83] dans un réseau ou dans une partie de celui-ci, d'étendre cette recherche vers un autre système ou une autre partie de celui-ci qui se trouve dans un autre lieu. Cette extension n'est cependant possible qu'à la double condition qu'elle soit nécessaire pour la manifestation de la vérité à l'égard de l'infraction qui fait l'objet de la recherche et que d'autres mesures soient disproportionnées ou qu'il existe un risque que, sans cette extension, des éléments de preuve soient perdus.

Cette mesure peut poser cependant problème lorsque les données sont hébergées dans un système informatique situé à l'étranger. Cette difficulté ne semble pas pourtant avoir impressionné le législateur belge qui autorise l'extension même dans ce cas ; mais les données pourront seulement être copiées. Compte tenu des risques d'atteinte à la souveraineté des Etats étrangers sur le territoire desquels sont hébergés les serveurs, le juge d'instruction doit, dans ce cas, par l'intermédiaire du Ministère Public communiquer l'information au Ministre de la justice qui saisit les autorités

[81] Art. 39 bis § 3.
[82] Art. 39 bis § 5.
[83] Que l'on assimile à une perquisition (V. F. de Villfagne et S. Dussolier précit.)

compétentes de l'Etat concerné si celui-ci peut raisonnablement être déterminé.

Il ne suffit pas d'accéder dans les systèmes informatiques pour y trouver des données. Il faut aussi pouvoir les lire et les déchiffrer, entreprise difficile puisque « les sites et systèmes informatiques se barricadent derrière des mots de passe, des identifications biométriques et d'autres outils d'accès… »[84]. C'est pourquoi la loi nouvelle belge a prévu l'obligation de collaboration des personnes qui sont présumées avoir une connaissance particulière du système informatique concerné[85]. Cette obligation pèse aussi, dans le cadre des écoutes, sur les personnes qui ont connaissance particulière des services de télécommunication[86]. Désormais le Procureur de la République, la juridiction d'instruction, ou la juridiction de jugement peut, lorsqu'il apparaît que des données saisies ou obtenues au cours de l'enquête ou de l'instruction ont fait l'objet d'opérations de transformation empêchant d'accéder aux informations en clair qu'elles contiennent, désigner toute personne qualifiée pour effectuer les opérations techniques permettant d'obtenir la version en clair de ces informations[87]. Dans le même ordre d'idées, les agents autorisés peuvent demander aux personnes physiques ou morales[88] qui fournissent des prestations de cryptologie visant a assurer une fonction de confidentialité, les conventions permettant le déchiffrement des données transformées au moyen des prestations qu'elles ont fournies[89].

L'obligation de collaboration est prévue également par le législateur français qui a apporté, avec la loi n° 2001-1062 du 15 novembre 2001

[84] V. F. de Villefagne et S. Dussolier, précit.
[85] Art.88 .quater
[86] Art. 90 quater.
[87] Nouvel art. 230-1 du code de procédure pénale
[88] Le fait de ne pas déférer est pénalement sanctionné.
[89] Nouvel art. 11-1 de la loi n° 91-646 du 10 juillet 1991.

relative à la sécurité quotidienne[90], certaines modifications dans le Code de procédure pénale[91] et dans la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications[92].

Au-delà des problèmes que l'utilisation des nouvelles technologies pour les besoins d'une enquête peut soulever sur un plan interne, il y a ceux qui sont liés à la localisation de l'infraction. Lorsque l'infraction est localisée à l'étranger, on l'a déjà souligné, il y a de fortes chances que les éléments de preuve se trouvent aussi à l'étranger ; il sera alors nécessaire d'accomplir des actes d'instruction en dehors des limites territoriales de l'Etat où les poursuites s'exercent. Si, par exemple, des systèmes informatiques situés dans des territoires différents sont interconnectés, il peut être nécessaire d'étendre une perquisition que l'on a commencée dans un pays à un système situé dans un autre. Cette extension ne sera pas possible lorsque la législation du pays qui accueille ce système n'admet pas l'interception des communications. Face à cette situation, même l'existence d'un accord d'entraide judiciaire ne pourrait permettre de surmonter la difficulté. En effet la mesure d'instruction qui est demandée dans le cadre d'une commission rogatoire peut ne pas être compatible avec la législation nationale de l'Etat requis ; or dans un tel cas aucune suite ne sera donnée à la demande.

L'existence de règles fixant le cadre dans lequel doit s'exercer l'activité des autorités chargées de conduire les investigations conduit à remettre en cause la régularité de « la recherche électronique des preuves » ; il reste à s'interroger sur la valeur des preuves électroniques obtenues au moyen de tels procédés.

[90] JORF n° 266 du 16 novembre 2001, p. 18215.
[91] V. Les nouveaux articles 230-1 à 230-4
[92] Art. 11-1.

2° - La valeur des preuves obtenues

La théorie des preuves en matière pénale est généralement dominée par deux principes : la liberté de la preuve et l'intime conviction[93].

Le principe de la liberté de la preuve s'explique aisément. Les délinquants se gardent bien d'agir en plein jour ; ils s'empressent plutôt, une fois leur forfait accompli, de faire disparaître toute trace de l'infraction. Dans ces conditions, il serait hasardeux de vouloir limiter artificiellement les modes de preuve.

On est obligé cependant d'admettre que le juge ne peut utiliser comme fondement de sa décision que les preuves régulièrement obtenues, car « si la preuve est libre, son administration ne l'est pas »[94]. C'est ce qui explique que parfois, les juges ont tendance à rejeter les preuves obtenues au moyen de procédés qui portent atteinte aux droits fondamentaux de la personne humaine[95].

Compte tenu de l'exigence de régularité dans la recherche des preuves, nous pensons que les preuves obtenues au moyen de procédés électroniques mis en œuvre en violation des prescriptions légales, doivent être écartées des débats. En effet, même si le recours aux procédés

[93] Au Sénégal l'article 414 du C.P.P. prévoit qu'en dehors des cas où la loi en dispose autrement, les infractions peuvent être établies par tout mode de preuve et le juge décide d'après son intime conviction.
Ce principe est emprunté au code français de procédure pénale (art. 427). On le trouve aussi dans d'autres pays. V. par exemple pour le Luxembourg – Jager – précit.

[94] V. Blondet, ruses et Artifices, dans l'enquête de police – JCP 1958. I - n° 14719.
Dans le même sens Brigitte Pesquée RSC 1990. 429.

[95] V. par exemple en France l'arrêt rendu par la Chambre criminelle de la Cour de cassation le 28 octobre 1991 (JCP 1992 II n° 21952. Note paumier). Cependant dans des arrêts rendus postérieurement, la Chambre criminelle s'est montrée moins exigeante. C'est ainsi que dans un arrêt rendu le 15 juin 1993 (DS 1994. 613 Note Mascalaà, elle a estimé, s'appuyant sur la liberté de la preuve, que les juges répressifs ne peuvent écarter les moyens produits par les parties au seul motif qu'ils auraient été obtenus de manière illicite ou déloyale.

électronique est admis, c'est sous réserve que les preuves soient légalement obtenues. Dans ces conditions une preuve obtenue au moyen d'une intrusion dans un système informatique situé à l'étranger en violation des règles qui y sont en vigueur doit être purement et simplement rejetées des débats.

A cet égard il n'y a pas à distinguer selon qu'il s'agit de preuves produites par la victime ou de preuves produites par la partie publique. C'est le lieu de rappeler que pour certaines infractions liées aux nouvelles technologies, ce sont les victimes elles-mêmes qui organisent la preuve des agissements[96] et elles peuvent être tentées de mettre en œuvre, dans un but probatoire, des procédés illicites de repérages et de fichage de ceux qui accèdent à leur système[97].

Il arrive cependant que la collecte des preuves soit régulière or dans la plupart des législations, il est prévu que lorsque les éléments de preuve sont régulièrement produits aux débats, il appartient aux juges d'apprécier souverainement leur valeur probante. C'est ce que l'on appelle le système de l'intime conviction qui dispense le juge « de rendre compte du cheminement par lequel il est parvenu à la certitude »[98].

Dans un tel système, il est donc permis au juge de s'appuyer, pour forger sa conviction, sur les preuves obtenues au moyen des nouvelles technologies dès lorsqu'elles sont régulièrement collectées. Il faut cependant savoir raison garder. Il existe en effet des risques inhérents au recours à des preuves électroniques.

---

[96] Francillon, précit.
[97] On a démontré que l'encryptage, en plus de son aspect préventif peut permettre un repérage des intrus.
[98] Lombois, la présomption d'innocence. Pouvoirs 1990 p. 81

Il y a d'abord le fait qu'on n'est jamais tout à fait sûr de l'exactitude des données collectées. On s'est demandé à juste titre si les images et les voix numérisées sont toujours fiables[99]. Indépendamment des manipulations toujours possibles, la technologie, si perfectionnée soit-elle laisse toujours «subsister un risque d'erreur dû à un mauvais fonctionnement de l'appareil »[100].

Il y a aussi et surtout le risque de voir le juge abdiquer, et donc abandonner ce qui fait sa raison d'être, (l'exercice de la mission de juger) au profit de la machine qui se substituerait à lui dans le processus d'application de la règle de droit.

En effet, comme on l'a souligné[101] « si l'informatique est pour la justice, un indispensable outil de gestion, en tant qu'instrument d'aide à la prise de décision, elle risque de porter atteinte à des principes aussi essentiels que la présomption d'innocence, l'intime conviction du juge, l'oralité, le contradictoire ou les droits de la défense.

[99] V. sur cette question Maisl art. précit.
[100] D. Amar, La preuve électronique. RTD Civ 1993. 499.
[101] Francillon, art. précit.

C O N C L U S I O N

-*-*-

Dans les sociétés modernes, nul ne songe à contester l'intérêt que représentent, pour les individus, les entreprises et les institutions, les nouvelles technologies de l'information. On ne peut que se réjouir des possibilités qu'offrent les moyens électroniques pour la collecte, le stockage, la conservation et la transmission des informations.

Hélas ! Les nouvelles technologies de l'information constituent aussi, on est obligé de l'admettre un « potentiel de risque spécifique »[102]. Les délinquants tirent aussi profit des possibilités qu'offrent ces nouvelles technologies c'est pourquoi le développement de ces nouvelles technologies engendre de nouveaux problèmes auxquels il faut faire face. A cet égard, chaque Etat tente, au niveau interne, de trouver des solutions appropriées. C'est nécessaire, car il faut adapter la législation interne pour assurer une répression efficace de la nouvelle forme de criminalité. Mais c'est insuffisant car les solutions isolées se révèlent le plus souvent inappropriées face à la criminalité transfrontalière que favorise le développement des moyens électroniques. En effet compte tenu de la circulation internationale des données, il peut être nécessaire de mener des investigations dans un pays autre que celui où l'infraction a été commise. Il nous paraît dès lors indispensable de coordonner les efforts. Cette action commune pourra aller dans deux directions.

Il s'agira d'abord de fixer des normes minimales communes ayant pour objet d ériger certains actes en infraction pénale et destinées à être

[102] Pour reprendre l'expression de Mr. Ulrich Sieber.

intégrées dans les législations internes. Ainsi sera faciliter la lutte contre la criminalité puisque « la concordance entre les législations internes peut s'opposer au développement des actes illicites dans les pays dont la législation est la moins rigoureuse et la coopération internationale en sera facilitée.

Il s'agira ensuite de mettre en place les mécanismes de coopération entre Etats[103]. C'est par ce seul moyen qu'il sera possible de conduire des investigations et de rechercher des éléments de preuve dans les lieux qui se trouvent en dehors de la compétence territoriale de l'Etat où les poursuites sont déclenchées.

A défaut d'une informatisation, à priori impossible à réaliser entre de systèmes trop différents, il est possible de réaliser une harmonisation des législations.

Cette harmonisation serait cependant vaine si elle ne s'accompagnait pas d'un soutien aux Etats qui ne peuvent avoir, faute de moyens, recours aux nouvelles technologies sans un tel soutien, il y aurait simplement transfert du problème par la création de nouveau « paradis de fraudes » dans le domaine des technologies.

[103] Convention sur la cybercriminalité, Rapport explicatif, précit.