Un net pas très net
Réflexions sur la criminalité virtuelle

Wanda CAPELLER
Université des Sciences sociales de Toulouse

> …« Au niveau des technologies avancées, il semble que nous assistons à un renversement de perspective qui affecte les capacités humaines de contrôle, voire même de simple appréhension des phénomènes. »
> Paul Virilio, *Un paysage d'événements*

RÉSUMÉ. — Confiance, risque, anonymat et responsabilité s'enchevêtrent au sein de la communauté virtuelle suivant un jeu d'interactions complexe qui engendre l'émergence d'un *champ criminel abstrait et systémique*. Les acteurs virtuels sont des co-constituants de ces systèmes. Ils produisent et reproduisent en permanence des *contextes matériels réels* où se concrétisent aussi des relations illicites. Ils engendrent une véritable communauté d'action virtuelle interactive illégale. La criminalité virtuelle se révèle ainsi comme une *question sensible* pour la société globalisée. En matière de cybercontrôle étatique, une « démarche purement nationale est illusoire ». Par son caractère transnational et décentralisé, par la fugacité et la volatilité de ses contenus, le cyberespace ne peut s'organiser et définir des règles communes de fonctionnement qu'à partir d'une coopération internationale sans faille. Les activités criminelles virtuelles, étant « désincarnées » n'ont pas besoin du face-à-face. L'adoption d'un nouveau paradigme s'impose si l'on veut rendre compte de ce glissement vers l'immatériel et encadrer une réflexion criminologique novatrice. L'auteur suggère qu'on se réfère à un *paradigme systémique abstrait*.

Voilà plusieurs années que l'on annonçait l'irruption d'une révolution cachée. Cette révolution sournoise, qui allait peu à peu renverser les notions de temps et d'espace, préparait le terrain pour un changement radical de la perception du monde. À cette époque, les mouvements qui engendraient ces transformations étaient souvent méconnus, peu visibles à l'œil de l'homme de la rue. Les métamorphoses de notre vision du monde ne s'effectuent alors que de façon obscure, malgré l'effort accompli par certains

auteurs pour déchiffrer les tendances et les signes de cet immense bouleversement [1]. Paul Virilio montre, ainsi, comment l'histoire vient d'emboutir le mur du temps, d'un temps réel qui correspond à une constante cosmologique, celle de la vitesse dans le vide [2]. Ce brusque embrouillage du temps mêle le présent au plus récent passé, un passé vieux de peu d'années où « tout a basculé dans une rupture de continuité qui ruine l'ancienne concordance des temps » [3].

L'intense développement des technologies de la communication et l'avènement d'une réalité virtuelle incitent alors l'ensemble de la communauté scientifique à revoir ses prémisses philosophiques, historiques et sociologiques. L'espace et le temps sont désormais au cœur de réflexions sur le monde et le moi, rappelant que ce ne sont pas là des cadres immuables, mais les moyens grâce auxquels nous percevons les choses et agissons sur elles, et les principes de toute communication concrète [4].

Cette révolution silencieuse, obscure, a fini par poser la technoculture comme destin de l'humanité. Présente, au début, dans les lieux de travail les plus hautement techniques, la réalité virtuelle devint rapidement une culture populaire concernant encore, il est vrai, des populations privilégiées, désormais envahies dans leurs vies quotidiennes par ces technologies avancées. On constate, alors, que d'autres formes de symbolisation s'imposent, et que de nouvelles questions sociales et psychologiques apparaissent, qui touchent non seulement les individus isolés, mais la société tout entière.

Ces nouvelles réalités technosociales se présentent comme des « contextes matériels », c'est-à-dire des lieux de rencontre électroniques où se concrétise le dépassement des limites corporelles de la communication [5]. L'espace cybernétique, lieu par excellence de ces grandes mutations technologiques et culturelles où se construisent de plus en plus de mondes abstraits fondés sur la simulation du monde naturel, reflète avant tout la société des individus. Par suite des changements dans les modes de communication et d'information, les pratiques de reconnaissance et d'intégration sociales se modifient. Et, par conséquent, le cyberespace présente l'occasion de repenser les dilemmes politiques et éthiques les plus tangibles de la société contemporaine[6].

Un certain nombre d'auteurs se sont mis en devoir de dénoncer cette technoculture qui échappe aux lois et au droit coutumier [7] puisque « l'ultime frontière » n'est plus notre corps, notre peau, notre conscience, « les nouvelles limites se trouv(a)nt désormais *au-delà*, dans des régions autrement transcendantes » [8]. En effet, le cyberespace, s'il peut être perçu comme un monde où de nouvelles formes de culture sont en train d'être créées, qui atteignent la vie des gens d'une manière immédiate et active, est utilisé

[1] Cf. notamment Raymond Ledrut, *La révolution cachée*, Casterman, 1979 ; Paul Virilio, *Un paysage d'événements,* Paris, Éd. Galilée, 1996 ; A. Giddens, *The Constitution of Society*, Polity Press, 1984.

[2] Cf. Paul Virilio, *Un paysage d'événements*, *op. cit.*, p. 12.

[3] *Ibid.,* p. 11.

[4] Raymond Ledrut, *op. cit.*, p. 101.

[5] Cf. Fred Grass, « The "New Bad Future" Robocop and the 1980's Sci-Fi Films », dans *Science as Culture*, 1989 : 5, pp. 5-70.

[6] Cf. David Holmes (ed.), *Virtual Politics. Identity and Community in Cyberspace*, Sage Publications, London, Thousand Oaks, New Delhi, 1997, p. 1.

[7] Cf. Paul Virilio, *op. cit.*, p. 22.

[8] *Ibid.,* p. 27.

aussi de façon instrumentale pour acquérir des choses et satisfaire des besoins [9]. Dans ce sens, David Holmes affirme que, plus qu'un outil au service de communautés pré-établies, les technologies virtuelles et les instances qui y sont représentées constituent des contextes où surgissent de nouvelles réalités corporelles et de nouvelles politiques correspondant à des « mondes-espaces » et à des « mondes-temps » qui n'ont jamais existé auparavant [10]. En fait, la notion *d'utilité* liée à cet espace s'estompe pour laisser apparaître des contextes matériels. Un glissement se produit de *l'espace virtuel considéré comme service* à *l'espace virtuel considéré comme contexte de formes diverses d'interaction*. De ce point de vue, l'outil virtuel ne saurait être perçu comme un simple *support* d'une nature nouvelle.

En réalité, les interactions techno-humaines fondent leurs références dans les relations pré-virtuelles, même si, dans ce type de rapport, il y a un effacement du corps [11]. De véritables communautés virtuelles surgissent de l'ombre et du vide apparent. C'est pour cela que l'utopie virtuelle selon laquelle on pourrait y célébrer les possibilités de revalorisation des cultures et d'identités, de communication directe et libre de contrainte avec les autres a, paradoxalement, posé des doutes et des questionnements. Ces interrogations concernent non seulement les questions liées à l'identité et aux subjectivités comme le montre Nicola Green [12], les nouvelles formes de citoyenneté [13], mais aussi des contextes matériels où se déroulent les relations commerciales dans ce qu'on nomme le *cybermarché* [14].

Le cybermarché est un espace ouvert, d'échange sans contrainte, où les possibilités d'une régulation étatique et juridique sont encore polémiques. Là, s'insinue et se développe une partie de l'économie illégale, celle même qui avait envahi, au-delà des limites consenties par les États, les marchés légaux pré-virtuels au début des années 1980 [15]. Ainsi, le cybermarché se présente-t-il également comme un lieu d'interactions criminelles ou déviantes – fait inconnu jusqu'alors –, constituant des contextes matériels où se manifestent de nouvelles formes de criminalité, une *criminalité virtuelle*.

On s'interroge, en conséquence, sur la neutralité de l'espace virtuel et sur les *contenus* qu'on peut y trouver. À ce propos, certains ont soutenu l'idée selon laquelle le déclin du politique, du social, du civique devait être lu d'une manière constructive, car il est le signe de la dominance du cyber [16], et qu'en aucun cas le cyberespace ne devait devenir « le jouet des États » [17]. D'autres affirment que l'ère digitale ne peut pas être perçue comme un « réseau universel sans responsable » [18].

[9] *Ibid.*, p. 3.
[10] *Ibid., eod. loc.*
[11] Cf. Nicola Green, « Beyond Being Digital: Representation and Virtual Corporeality », dans *Virtual Politics*, *op. cit.*, p. 59-78.
[12] *Ibid.*, *eod. loc.*
[13] Le « citizennet » est un terme largement utilisé par la littérature américaine sur ce sujet.
[14] Ce terme traduit le mot de l'anglais « cybermarket ».
[15] Sur un thème voisin, voire notre étude sur « La transnationalisation du champ pénal : réflexions sur les mutations du crime et du contrôle », dans *Droit et société*, 35/1997, p. 61-78.
[16] Cf. Paul Virilio, *op. cit.*, p. 24.
[17] *Ibid.*, p. 25.
[18] *Ibid., eod. loc.*

Ce que l'on note, en tout cas, c'est une rupture des modèles de comportements. Dans l'espace virtuel, en effet, apparaissent des comportements déviants ou délictueux. Des *discontinuités* surgissent dans le champ criminel, sans que cela signifie, pour autant, l'abandon de formes plus traditionnelles d'activités criminelles. Ces dernières continuent d'exister, témoignant de *continuités* dans ce domaine. Ces *continuités* apparaissent aussi lorsqu'une forme traditionnelle de criminalité s'insère dans l'espace virtuel comme, par exemple, le crime organisé. Les possibilités de pénétration du crime organisé transnational dans des contextes virtuels sont incontestables, renforçant par ailleurs de nouveaux espaces d'interaction criminelle.

Quant au contrôle, dans l'espace virtuel, on trouve encore, sous certains aspects, des traces de pratiques à fondement positiviste, notamment lorsqu'il s'agit de l'informatique identificatoire [19]. Les technologies d'identification, en effet, se développent, reconstruisant des « sujets virtuels » sur la base de « systèmes biométriques qui reconnaissent un individu à partir de ses caractéristiques physiques, morphologiques et même génétiques » [20].

Cela montre bien les aspects de *continuité des modèles de contrôle*. C'est le retour de Lombroso dans la sphère virtuelle ! Les traces d'une conception positiviste du crime et du contrôle sont encore présentes. Il semble alors qu'une révision des matrices criminologiques soit nécessaire, l'édifice criminologique étant désormais insuffisant pour rendre compte de ces nouvelles formes de criminalité et déviance qui constituent le cybercrime. Peut-être s'imposeront-elles comme dominantes au XXI^{e} siècle. Même si la culture cybernétique, promise à un avenir de plus en plus populaire, n'atteint pas encore l'ensemble des populations, la criminalité virtuelle s'étend, en effet, aujourd'hui de manière impressionnante.

Je voudrais, dans ces quelques lignes, mettre l'accent sur quelques propositions. Je tiens que, avec cette *criminalité virtuelle*, nous assistons à l'émergence de ce qu'on nomme une *question sensible*, la criminalité adoptant la virtualité moins comme un support que comme l'opportunité d'user de cadres et de contours créés, d'une manière générale, pour le fonctionnement de véritables communautés virtuelles. Méritent d'être analysés, en conséquence, premièrement l'émergence même de cette criminalité virtuelle comme celle d'une question sensible (I) ; deuxièmement, le mode de fonctionnement dans le cyberespace de ces *trafiquants du vide*, qui se comportent comme des membres d'un « club », d'une communauté, au sens traditionnel, alors qu'il s'agit d'une communauté virtuelle (II) ; troisièmement, les causes de la précarité et de l'inefficacité structurelle d'un contrôle qui traite à tort de ces problèmes de l'espace virtuel comme s'il ne s'agissait que d'un support, et les réponses possibles à ces agissements de la part d'un cybercontrôle en voie de construction (III). Ces réflexions mènent inévitablement à imaginer, ce pour quoi nous plaiderons en conclusion, un nouveau paradigme criminologique susceptible de rendre compte de ces nouvelles formes de criminalité immatérielle.

[19] Voir Danièle Bourcier, « Données sensibles et risque informatique. De l'intimité menacée à l'identité virtuelle », dans *Questions sensibles*, Paris, PUF, 1998, p. 39-58.

[20] *Ibid.*, p. 44.

I. — LA CRIMINALITÉ VIRTUELLE UNE QUESTION SENSIBLE ÉMERGENTE

L'idée même de « sensible » est révélatrice d'incertitudes, d'instabilités qui affectent l'ordre et engendrent les désordres. Tout ce qui est « sensible » dans le champ des sciences politiques, des sciences sociales ou des sciences juridiques contraint à une « connaissance recommencée du sens ». Les questions sensibles, en effet, se révèlent à l'occasion de conflits sociaux, de compétitions politiques, d'une controverse juridique, et leur résolution devient « un des enjeux politiques majeurs, une des préoccupations sociales essentielles, un des soucis individuels élémentaires » [21]. La criminalité immatérielle que l'on rencontre, aujourd'hui, sur Internet, constitue, en ce sens, une *question sensible* dans la mesure où il est difficile non seulement de concevoir ce thème de façon consensuelle, mais aussi de présenter « communément » ce phénomène. Ici, l'on est invité à « décider l'indécidable », à « résoudre l'insoluble ». Il reste néanmoins « l'impératif du dire », la « nécessité d'agir », le besoin d'appréhender ce phénomène [22].

Et il est bien vrai que la criminalité virtuelle est une question « conjoncturellement sensible ». Elle émerge brusquement en tant que question sensible en ce sens qu'elle suscite une sensibilité nouvelle [23]. Ce qui caractérise ce type de questions, c'est l'importance des processus de construction, le fait qu'elles appellent à une intervention publique et le particularisme des modes de traitement politique [24]. Quelques concepts qui se trouvent au centre d'une réflexion sur la société de modernité avancée [25], où les rapports humains traditionnels de co-présence sont parfois remplacés par de relations désincarnées [26], présentent, à cet égard, une importance considérable pour comprendre l'émergence de cette *question sensible* que constitue la criminalité virtuelle. Ils peuvent être présentés, d'une manière heuristique pour la présente réflexion, en couples d'opposition. Au nombre de ces paires de concepts, on trouve celles de *confiance* et de *risque*, et encore d'*anonymat* et de *responsabilité*.

La confiance et le risque : notions changeantes dans la modernité avancée…

À l'époque moderne, la notion de confiance est liée à celle de risque, car elle présuppose, avant tout, une conscience de ce dernier. Néanmoins, selon Luhmann, la confiance n'est pas identique au sentiment de sécurité dans la mesure où celui-ci porte en connotation la certitude, la stabilité des choses familières [27]. La confiance renvoie plutôt l'indi-

21 Cf. Geneviève Koubi, Présentation de l'ouvrage *Questions sensibles*, *op. cit.*, p. 5-7.
22 *Ibid.*, *eod. loc.*
23 Cf. Jacques Chevallier, « Qu'est-ce qu'une question sensible ? », dans *Questions sensibles, op. cit.,* p. 11-16.
24 *Ibid.*, p. 12.
25 Cf. Anthony Giddens, *Les conséquences de la modernité*, Paris, L'Harmattan, 1994.
26 Cf. David Holmes (sous la dir. de), *Virtual Politics. Identity and Community in Cyberspace, op. cit.*
27 Cf. Anthony Giddens, *Les conséquences de la modernité*, *op. cit.*, p. 38.

vidu aux choix possibles, et celui qui ne maîtrise pas les implications inhérentes à ces choix reste dans une situation de *sécurité passive* [28], exposé aux situations de danger [29].

À partir de ces réflexions sur la modernité avancée, Anthony Giddens revoit ces distinctions conceptuelles affirmant que la confiance est désormais « liée à l'absence dans le temps et l'espace » [30]. Selon lui, point ne serait besoin de faire confiance à quelqu'un dont les activités seraient visibles et les modes de raisonnement transparents, ni à un système dont les rouages seraient parfaitement connus et compris. Ainsi, plus encore qu'au risque, la confiance paraît fondamentalement liée à la contingence, les individus s'en remettant non au danger mais au hasard » [31].

Giddens, de son côté, affirme que « la confiance n'est pas la foi dans la fiabilité d'une personne ou d'un système », mais dérive de cette foi [32]. Selon ses propres mots, « on peut parler de confiance envers des gages symboliques ou des systèmes experts, mais cela repose sur la foi en la validité de principes que l'on ignore, et non la foi en la "droiture morale" (les bonnes intentions) d'autrui ». La confiance concerne plutôt le *bon* fonctionnement du système que son fonctionnement en tant que tel [33]. Or si le champ virtuel où s'installe la cybercriminalité peut être contextuellement caractérisé, c'est bien par la présence de la contingence, du hasard et du risque. Si l'on parlait déjà de la *société mondiale du risque,* on peut désormais faire allusion à la *société virtuelle du risque*.

On a vu, en effet, comment le progrès est potentiellement générateur de risques importants où l'action de l'homme échappe à la main de l'homme [34]. Parler de risques, et non pas seulement de maux ou de dangers, c'est parler d'événements qui atteignent une activité partagée avec d'autres dans un espace social. En effet, la prévision et le calcul des risques supposent d'abord la constitution d'un « espace social d'activités partagées » [35]. À ce propos, on a signalé opportunément certaines caractéristiques du risque [36], notamment son empreinte collective portant sur des groupes ou des « populations », sa capacité à atteindre un « capital », ce qui permet l'objectivation économique indispensable pour la prévention et la réparation [37]. On a également affirmé, par ailleurs, que le risque présuppose des relations sociales ; il est toujours risque social [38].

De l'État de prévoyance à la « société du risque », le pas est franchi depuis un certain temps, cette dernière naissant au moment où les bases de calcul de la société industrielle sont éliminées au cours d'une modernisation qui a développé une dynamique particulière niant les fondements de sa propre rationalité. La société contemporaine, parce qu'elle maintient son équilibre au-delà des limites assurables, aggrave les consé-

28 *Ibid., eod. loc.*
29 *Ibid.,* p. 39.
30 *Ibid.,* p. 40.
31 *Ibid., eod. loc.*
32 *Ibid., eod. loc.*
33 *Ibid.,* p. 41.
34 Cf. Jacques Lautman, « Risque et rationalité », dans *L'Année sociologique*, n° consacré à l'*Étude sur le risque et la rationalité*, Vol. 46/1996/2, p. 273-285.
35 Cf. Frédéric Worms, « Risques communs, protection publique et sentiment de justice », dans *L'Année sociologique,* n° consacré à l'*Étude sur le risque et la rationalité*, Vol. 46/1996/2, p. 287-307.
36 Cf. François Ewald, *L'État-providence*, Paris, Grasset, 1985, notamment p. 173-181.
37 Voir encore Frédéric Worms, *op. cit.*, p. 291 sq.
38 *Ibid., eod. loc.*

quences et les dangers en en faisant abstraction, et refuse du même coup de prendre conscience des risques et de sa responsabilité [39].

Le terme « société du risque » marque, en effet, une phase de la société moderne dans laquelle les risques sociaux, politiques, écologiques (individuels ou collectifs) engendrés par la dynamique de renouvellement se soustraient de plus en plus aux instances de contrôle et de sécurité de la société. Cependant, face à la dynamique de la société du risque, les sociétés contemporaines décident et agissent encore en fonction du modèle de l'ancienne société industrialisée, avec des systèmes politiques et juridiques incapables de sortir des débats et conflits [40].

Par ailleurs, la transition de l'époque industrialisée vers celle du risque des temps contemporains s'opérerait de manière involontaire, méconnue et inévitable, selon une dynamique de modernisation qui s'est développée de façon autonome ignorant totalement les conséquences et les dangers [41]. Ces derniers dépassent les limites de la notion de sécurité telle que la société industrialisée occidentale l'avait conçue, et, par conséquent, bouleversent les principes fondamentaux de l'ordre social actuel. Les difficultés pour endiguer ces problèmes surviennent notamment dans le cadre de la prise de décision, qu'il s'agisse de décision politique [42] ou juridique.

Il n'est donc pas infondé de prétendre, comme on le fait ici, que la confiance et le risque sont au fondement des interactions virtuelles. Dans l'environnement électronique, en effet, les questions liées à la confiance et au risque deviennent très visibles, car elles sont d'emblée situées dans une *contextualité* nouvelle, simulatrice de l'ordre social pré-virtuel, où la construction d'une relation entre un événement possible et un capital valorisé se produit sans la co-présence physique des acteurs impliqués. On parlera alors de *risque virtuel*, non seulement s'agissant du commerce électronique, de contrats, de la rémunération de l'auteur de l'œuvre audiovisuelle ou de la protection des droits de la personnalité, mais aussi – et principalement – lorsqu'on « surfe » dans des espaces de cyberdéviance. Si les gens étaient déjà abandonnés dans « les turbulences de la société mondiale du risque » [43], ils sont aujourd'hui exposés également au risque virtuel. Sans compter que, sur le cyberespace, le risque est renforcé par l'anonymat.

L'anonymat et la responsabilité : « surfer » dans l'ombre du droit ?

Dans l'espace virtuel, l'anonymat peut signifier à la fois une simple protection des sources d'information et un danger. Certains psychologues estiment que l'anonymat est désirable lorsqu'il permet aux usagers du Net – les « netcitoyens » [44] – d'assumer différentes identités psychologiques. On a, par exemple, rappelé que ceux qui utilisent la

[39] *Ibid*., p. 342.

[40] Cf. U. Beck, « D'une théorie critique de la société vers la théorie d'une autocritique sociale », dans *Déviance et Société,* p.333-344., 1994, Vol. XVIII, N° 3, p. 333-344.

[41] *Ibid*., p. 334.

[42] *Ibid., eod. loc*.

[43] *Ibid*., p. 335.

[44] Ce terme, traduit de l'anglais « Netizens », fait référence aux textes de Jim Mcclellan, *Cyberspace : Judge Dread*, *Observer* (London), du 29 janvier 1995, p. 76. Voir aussi Howard Rheingold, "*Web*" *Spreads into a Wildfire*, *Denver Post*, du 13 janvier 1995, p. 22.

communication électronique aiment se déguiser, entrer dans un autre corps, être une autre personne, vivre dans un autre monde [45]. D'autres affirment que, dans le cyberespace, il serait bon de préserver l'anonymat, à cela près qu'il devrait être limité par le droit, notamment en raison de tout ce qui touche à la question de la responsabilité [46]. L'absence de responsabilité, en effet, encourage des comportements outrageants et incite à un manque de civilité [47].

Malgré les préoccupations concernant la responsabilité des internautes, ces dernières années ont témoigné d'une tendance au renforcement de l'anonymat sur le cyberespace, ce qui rend difficile le dévoilement des sources de bien des messages électroniques. Certains fournisseurs d'accès, en effet, ne permettent pas l'anonymat des usagers, afin de pouvoir les identifier et les réprimer en cas de besoin. D'autres, néanmoins, permettent aux utilisateurs de rester anonymes, l'une « des méthodes consistant dans l'attribution d'adresses à la volée qui autorise l'utilisateur à se faire adresser des messages à une adresse attribuée pour l'occasion tout en préservant son anonymat » [48].

Quoi qu'il en soit, les fournisseurs d'accès, même si, parfois, ils sont mis en position de censeurs [49], se trouvent, de toutes manières, placés face à un monde d'utilisateurs navigant sur différents réseaux interconnectés [50], ce qui rend encore plus complexe cette logique enchevêtrée qui fonde cette nouvelle branche de la sociologie, celle du réseau des réseaux, déjà bien développée dans la littérature anglo-saxonne, et qui traite notamment de la recherche de l'information, de la demande et de l'offre de services traversant l'espace et le temps.

Le réseau Internet n'est pas anonyme de par sa construction [51]. Néanmoins, même si un serveur Internet connaît par définition l'adresse de l'utilisateur et son nom de domaine, celui-ci peut toujours procéder par artifices (serveur anonyme) [52]. Là, joue la stratégie des acteurs virtuels. Par ailleurs, lorsqu'une entreprise est exposée à des agissements malveillants sur le Net, deux solutions peuvent être adoptées, soit l'isolation de l'ordinateur, ce qui empêche les utilisateurs de se servir de celui-ci pour naviguer sur l'ensemble du système informatique, soit la cryptographie, c'est-à-dire le codage des messages. Cette dernière solution, qui, sans nul doute, protège les données, rend par ailleurs plus difficile les contrôles et favorise l'anonymat en même temps que la criminalité organisée [53]. En fait, le système américain de cryptographie « PGP » (*Pretty Good Privacy*), garantit à ses utilisateurs un parfait anonymat, car il est alors

[45] Cf. Howard Rheingold, *The Virtual Community* (1993), cité par Anne Wells Branscomb, « Anonymity, Autonomy, and Accountability : Challenges to the First Amendment in Cyberspaces », dans *The Yale Law Journal*, Vol. 104, N° 7, mai 1995, p. 1639-1679.

[46] Cf. Anne Wells Branscomb, *op. cit.*, p. 1642.

[47] *Ibid., eod. loc.*

[48] *Internet. Enjeux juridiques*. Rapport au ministère délégué à la Poste, aux Télécommunications et à l'Espace et au ministre de la Culture, Mission Interministérielle sur l'Internet présidée par Isabelle Falque-Pierrotin, La Documentation française, 1997, p. 48.

[49] Cf. Anne Wells Branscomb, *op. cit.*, p. 1645.

[50] *Internet. Enjeux juridiques, op. cit.,* p. 8.

[51] *Ibid.*, p. 24.

[52] *Ibid.*, p. 26.

[53] Cf. Gérard Haas et Ivan Vassileff, « Délinquance numérique : l'attaque des Stad par les données », dans *Legicom. Revue trimestrielle du droit de la communication*, N° 12, 1996/2.

impossible de connaître leur identité, leur nationalité ni de savoir de quel continent ils émettent leurs messages [54]. L'adoption de cette solution est instamment sollicitée par commerçants et banquiers, inquiets du développement des « sniffeurs » [55] et des délits qui s'ensuivent en matière de paiement par carte bancaire sur le Net [56].

On voit que les possibilités d'anonymat sur le cyberespace sont immenses ; elles se présentent en raison des caractéristiques propres au réseau, notamment sa décentralité, sa transnationalité, sa fugacité et la volatilité des contenus, sa technologie infiniment évolutive, son protocole non propriétaire, et les stratégies singulières d'acteurs [57]. Mêmes les novices dans l'usage de ce système peuvent brouiller les pistes, en envoyant leurs messages vers des serveurs dont l'unique fonction est de réexpédier tout ce qu'ils reçoivent sans indication de provenance [58].

L'impact de l'anonymat est considérable dans un système en perpétuelle reproduction et en expansion constante, qui dépasse désormais le monde non marchand et clos des spécialistes et des initiés, atteignant progressivement un espace grand public. Ces changements de nature de l'Internet provoquent des effets pervers, la « socialisation » croissante de l'espace virtuel créant les conditions propices à l'installation d'interactions illégales, qu'elles soient marchandes ou non.

Confiance, risque, anonymat et responsabilité s'enchevêtrant au sein de la communauté virtuelle suivant un jeu d'interactions complexe qui engendre l'émergence d'un *champ criminel abstrait et systémique*. Comme on a pu le montrer, une part de fantasme et d'inquiétudes s'installe dans ce réseau méconnu, notamment sur « la capacité des États à faire en sorte que la délinquance et la criminalité, qui n'ont jamais épargné aucune société, soient cantonnées dans le monde virtuel comme ailleurs, dans des limites marginales » [59]. Et il est vrai que la littérature récente sur le Net témoigne d'une préoccupation croissante à l'endroit des nouvelles formes de criminalité virtuelle, exhortant ainsi les spécialistes en la matière à une réflexion renouvelée.

II. — LES TRAFIQUANTS DU VIDE

La prétendue neutralité du cyberespace est mise en question par l'existence des « net-criminels » ou des « netdéviants ». La plupart du temps, on se borne à déclarer que « les autoroutes de l'information peuvent être le moyen de la réalisation de nouvelles formes de délits » [60]. Il faut aller plus loin : le cyberespace n'est pas seulement un *moyen* ou un *support* pour l'action criminelle ; il constitue un véritable *champ autonome* où se déploie une action criminelle systémique et abstraite. La distinction

[54] *Ibid., eod. loc.*

[55] Programmes informatiques permettant d'aspirer les données fournies par les clients au moment de régler leurs transactions.

[56] Cf. par ex. *Le Monde*, suppl. Multimedias, 25/26 octobre 1998, p. 34.

[57] *Internet. Enjeux juridiques, op. cit.,* p. 47.

[58] Voir *Le Monde*, dimanche 19 -lundi 20 mai 1996.

[59] Cf. Nicolas Brault, « Le Droit applicable à Internet. De l'abîme aux sommets », *op. cit.*

[60] Cf. Gérard Haas et Ivan Vassileff, « Délinquance numérique : l'attaque des Stad par les données », *op. cit.*

entre *support* et *champ* est essentielle pour la compréhension de ces nouveaux phénomènes.

La notion de *support* renvoie à l'idée d'une simple utilisation des ordinateurs comme outils au moyen desquels des actes malveillants peuvent se concrétiser [61]. McLuhan, en affirmant que « le moyen est le message », avait surtout montré que la technologie et l'automatisme finissent par façonner nos vies et deviennent une extension de nous-mêmes [62]. L'idée selon laquelle l'Internet n'est pas seulement un *support* pour les activités criminelles s'impose en raison de la dynamique propre à ce système et de l'intensité même des transformations qui peuvent y être observées. Il faut également compter avec les stratégies d'acteurs virtuels, dont la mise en œuvre contribue au dépassement d'une conception de l'Internet comme seul *moyen* de commettre des infractions.

En fait, les acteurs virtuels sont des co-constituants [63] de ces systèmes. Ils produisent et reproduisent en permanence des *contextes matériels réels* où se concrétisent aussi des relations illicites. Ils engendrent, pour ce qui nous intéresse ici, une véritable communauté d'action virtuelle interactive illégale. Et cette communauté se fonde, on l'a constaté, sur l'interaction complexe d'éléments qui se trouvent à la base de ce système abstrait, notamment la confiance, le risque, l'anonymat et la responsabilité.

Ce contexte matériel accueille volontiers des jeux d'interactions désincarnées dans divers domaines, y compris celui de la criminalité. Il devient, alors, un lieu privilégié de l'offre et de la demande de services illicites, créant ainsi un environnement unique et maintes fois protégé par l'anonymat. Dans ce champ prolifèrent les activités criminelles virtuelles qui passent par les interstices et les lacunes du système qui constitue un environnement radicalement différent où se recrutent ceux qui veulent s'engager dans des activités criminelles. C'est ici, également, que se disséminent de nouvelles « techniques criminelles » [64]. Certes, l'obtention de profits illégaux à travers les innovations industrielles n'est-elle pas, en soi, une pratique nouvelle. Néanmoins, le fait que ces innovations soient transmises et diffusées en temps réel et immédiat et réutilisées comme techniques illicites caractérise de manière radicalement nouvelle le *champ criminel* virtuel [65], sans compter la flexibilité du système et l'absence d'un contrôle central [66] – ce qui contribue à dérouter les juristes.

S'agissant d'appréhender ces phénomènes, c'est alors l'affolement dans la communauté scientifique. À cet égard, on distingue, historiquement, quatre phases de réflexion. La première couvre une trentaine d'années, entre 1946 et 1976, où les scientifiques nord-

61 Plusieurs auteurs s'expriment dans ces termes, voir notamment Gérard Haas et Ivan Vassileff, lorsqu'ils affirment que « les autoroutes de l'information peuvent être le moyen de la réalisation de nouvelles formes de délits » : cf. « Délinquance numérique… », *op. cit.* ; cf. aussi David Mann et Mike Sutton, lorsqu'ils affirment : « The Internet is a particularly effective medium for criminal recruitment and the dissemination of criminal techniques » (« Netcrime. More Change in the organization of Thieving », dans *British Journal of Criminology*, Vol. 38, N° 2, 1998, p. 201).

62 L'expression de McLuhan est la suivante, dans l'original : « The medium is the message ». *Apud* David Mann et Mike Sutton, *op. cit.*, p. 205.

63 Cf. Anthony Giddens, *The Constitution of Society*, Polity Press, 1984.

64 David Mann et Mike Sutton, *op. cit.*, p. 201.

65 *Ibid., eod. loc.*

66 *Ibid.*, p. 203.

américains essayèrent de déceler la *nature* de cette criminalité émergente. La période suivante peut être caractérisée comme celle de la *criminalisation* de ces phénomènes, et s'étend de 1977 à 1988 : on s'efforce, alors, de fixer des mesures correctives à l'abus électronique. Suit une étape de *diabolisation*, entre 1988 et 1993 : les efforts portent sur l'identification des « *hackers* » et des « *crackers* », et l'on cherche les sanctions qui seraient les mieux adaptées. À partir de 1993, on rentre dans la période de la *censure*, qui correspond au développement intense de l'information et de la communication électroniques, notamment par l'Internet [67].

Les dernières années ont témoigné, en fait, d'un glissement d'une déviance parfois provocatrice commise à l'intérieur du système informatique vers une criminalité virtuelle de plus en plus sophistiquée. Dans un premier moment, en effet, des actes malveillants s'introduisent dans les systèmes informatiques, avec l'inoculation de virus et la contamination de ces systèmes, interpellant la sécurité des ordinateurs eux-mêmes. Les préoccupations majeures étaient alors centrées sur la piraterie électronique : appropriation des informations stratégiques, viol de la confidentialité des fichiers des institutions étatiques et des entreprises, destruction des données ou des programmes, infiltration d'internautes malhonnêtes dans les serveurs, puis dans les réseaux auxquels ils donnent accès [68]. À la fin des années 1970, la « criminalité par ordinateur » était déjà devenue un véritable problème social, suscitant la création de nouvelles catégories juridiques capables de rendre compte de ces phénomènes. Une régulation juridique fut alors produite dans ce domaine, aux États-Unis surtout, mais également en Europe [69].

Aujourd'hui, les *hackers* « vieux jeu » cèdent la place à une criminalité « hi-tech » tournée notamment vers les profits financiers. Il ne s'agit plus de *comportements problématiques,* mais de *comportements réellement délictueux* [70]. Certains auteurs s'efforcent alors de comprendre la structure de ce qu'on appelle les *newsgroups,* ces messageries collectives ouvertes où n'importe qui peut déposer des messages, en toute liberté. Normalement, ces *newsgroups* se forment pour des échanges, scientifiques ou autres, sans connotation criminelle. On parle souvent, dans ce cas, de « forums ». Les grands serveurs des universités américaines, par exemple, gèrent de milliers de *newsgroups* à vocation mondiale, en anglais. Ils sont regroupés en grandes catégories thématiques, et les principales (sciences, informatique, société, divertissement, débats, etc.) sont assez bien organisés. Mais on trouve des forums sur des sites beaucoup plus modestes, dans diverses langues. Les messages sont surveillés par des modérateurs, qui s'efforcent de maintenir l'ordre du réseau, sur la base d'une auto-gouvernance. Dans ce type de réseau, un *newsgroup* ne se crée, généralement, qu'à l'issue d'une procédure complexe, sanctionnée par un vote [71].

Néanmoins, des *newsgroups* peuvent aussi apparaître dans un espace d'anarchie virtuelle, qu'on nomme les « alt », c'est-à-dire les espaces alternatifs. C'est ici que s'insinuent et s'installent les sectes religieuses, les extrémistes politiques, les groupes racistes et xénophobes, les amateurs de pornographie, les groupes plus « durs » qui

67 *Ibid.*, p. xviii.

68 *Ibid., eod. loc.* Voir aussi Richard C. Hollinger (sous la dir. de) *Crime, Deviance and the Computer*, Aldershot, Brookfield USA, Singapore, Sydnei, Dartmouth, 1997.

69 Voir Richard C. Hollinger, *Introduction, op. cit.*

70 Cf. Nicolas Brault, « Le droit applicable à Internet », *op. cit.*

71 Cf. *Le Monde* du 19-20 mai 1996.

interagissent dans des domaines d'activité criminelle [72]. Or, les membres de ces *newsgroups* agissent comme membres d'une association dans le sens le plus traditionnel du terme [73]. Du point de vue psychologique, certains estiment que les *hackers* expriment un sentiment d'aventure, presque héroïque, antiétatique et antibureaucratique – celui qui caractérisait, autrefois, les conquérants de « nouvelles frontières ». Les netdéviants pourraient ainsi être comparés aux « cow-boys », ils seraient les « *techno*-cowboys » des sociétés post-modernes [74].

Considérations psychologiques mises à part, il faut bien constater que l'anarchie virtuelle existe. Il faut alors établir une distinction selon les *contenus* des messages circulant parmi les membres de ces *newsgroups* pour déterminer le degré de nuisance de leurs actions. Là, l'Europe a pris des mesures précises. En 1997, la Commission n° 7 (Europe des citoyens, recherche, culture, jeunesse et consommateurs) a soumis au Comité des Régions deux études traitant de la circulation de contenus illicites sur le Net : le « Livre vert sur la protection des mineurs et la dignité humaine dans les services audiovisuels et d'information », et la « Communication de la Commission sur le contenu illégal et préjudiciable sur Internet » [75]. Ces textes distinguent clairement les contenus illicites et les contenus préjudiciables affirmant « qu'il s'agit d'objectifs distincts posant des problèmes différents et appelant des solutions différentes » [76]. Mais il faut bien noter que ces textes parlent de l'Internet comme d'un « support » pour la diffusion des contenus illégaux et préjudiciables. Ce faisant, l'Europe se prive, dès l'origine, d'un contrôle réellement efficace, ignorant, par là même, la nature spécifique de ce qu'elle cherche à maîtriser.

Le Livre vert affirme que sont illicites « les contenus pouvant faire l'objet d'une interdiction générale, quel que soit l'âge des destinataires potentiels, comme par exemple ceux relatifs à la pornographie infantile » [77]. Les contenus préjudiciables sont, selon ces textes, ceux qui sont susceptibles de nuire à l'épanouissement physique, mental ou moral des mineurs, et qui, dès lors, ne devraient être accessibles qu'aux adultes » [78]. Au Parlement européen, la Commission des libertés publiques et des affaires intérieures affirme, par ailleurs, que « le réseau Internet est utilisé de manière croissante pour diffuser la pornographie enfantine et, dans la mesure où il constitue un marché pratiquement incontrôlable, (qu'il est) exploité pour les perversions les plus inimaginables ». Et, aussi, que « la pornographie audiovisuelle et le tourisme sexuel sont des pratiques favorisant le passage à l'acte pédophilique en levant les tabous » [79].

[72] Cf. David Mann et Mike Sutton, « Netcrime. More Change in the organization of Thieving », *op. cit.*, p. 201. Ces auteurs ont proposé une typologie des comportements sur le Net.

[73] *Ibid.*, p. 213.

[74] Cf. notamment Sterling (1992), cité par David Mann et Mike Sutton, « Netcrime. More Change in the organization of Thieving », *op. cit.,* p. 206.

[75] *Journal officiel* n° C 215 du 16/07/1997, p. 0037.

[76] *Ibid., eod. loc.*

[77] *Ibid., eod. loc.*

[78] *Ibid., eod. loc.*

[79] Cf. Parlement européen, Travaux préparatoires de la Commission des libertés publiques et des affaires intérieures, *Journal officiel* n° C 358 du 24/11/1997.

La pornographie et la pédophilie suscitent la mobilisation effective des instances de contrôle non seulement en Europe, mais aussi aux États-Unis [80]. Pourtant, dans ce pays, défenseur acharné de la libre expression, les « entrepreneurs de la morale », choqués spécialement par la transmission des images illicites d'enfants, demandent au Congrès national d'élargir et de renforcer la législation sur ce sujet [81]. En réalité, les nouvelles technologies virtuelles sont en train de créer de nouveaux cadres de « dilemmes moraux » concernant le langage sexuel sur le Net, les vices virtuels comme la cyberprostitution [82] et autres cyberdélits [83].

Plusieurs *newsgroups* apparemment moins nocifs s'infiltrent également sur le Net, comme ceux qui s'organisent autour d'une industrie émergente de jeux interactifs (« *Internet Gambling* ») dont l'impact, dans certaines sociétés, est considérable. En 1997, par exemple, l'Institut de criminologie d'Australie et l'Institut australien pour la recherche sur les jeux ont proposé un colloque sur ce thème, étant donné la diffusion de ces pratiques dans ce pays [84]. D'autres, beaucoup plus dangereux, se rencontrent également sur le Net, comme des terroristes, des trafiquants de drogue ou des membres de communautés transnationales criminelles. N'importe qui peut, à partir de l'expression « blanchiment d'argent », trouver des sites proposant ouvertement des solutions avantageuses !

Interdits ou non, les *newsgroups* peuvent être facilement consultés. Pour ce faire, et au cas où le *newsgroup* recherché ne serait pas relayé par le serveur de son fournisseur d'accès, il suffit de se connecter directement sur un serveur public, dont certains autorisent non seulement la lecture mais aussi l'envoi des messages. Le serveur américain Zippo [85], par exemple, offre un accès direct aux *newsgroups* via le World Wide Web, y compris à ceux qui sont très controversés et regroupés dans une catégorie à part nommée « alt.*restricted » [86].

La criminalité virtuelle est donc bien devenue une *question sensible* pour la société globalisée, les sociétés nationales européennes n'étant pas à l'abri de ces méfaits. En 1998, par exemple, la cyberpolice française a décelé 424 affaires criminelles virtuelles [87]. La presse écrite et télévisée a, relativement récemment, pris conscience de ces problèmes et commence à informer l'ensemble de la population qui, dans sa majorité, ne navigue encore sur le Net. L'Union européenne propose des mesures restrictives pour contrer ces activités délictueuses virtuelles, et suggère la mise en place d'une instance de coopération internationale. On a affaire à un débat sur le cybercontrôle.

[80] Une vaste littérature nord-américaine existe sur ce sujet.

[81] Voir Richard C. Hollinger, *Introduction, op. cit.*, p. xxviii.

[82] Cf. James D. Nahikian, « Learning to love "the ultimate peripheral" : virtual vices like "cyberprostitution" suggest a new paradigm to regulate online expression », dans *John Marshall Journal of Computer and Information Law*, N° 4, du 01/07/1996.

[83] Cf. Michele Wilson, « Community in the Abstract : A Political and Ethical Dilemma ?», dans Cf. David Holmes (sous la dir. de), *Virtual Politics. Identity and Community in Cyberspace, op. cit.*

[84] Cf. Jan Mcmillen et Peter Grabosky, « Internet Glambling », dans *Trends and Issues in Crime and Criminal Justice*, Australian Institute of Criminology, N° 88, 1998.

[85] http ://www.zippo.com

[86] Tout au plus, l'abonnement est-il réservé aux plus de dix-huit ans.

[87] Information télévisée d'octobre 1998. Voir aussi Marc Pinguet, « La douane et la cyber-délinquance », *La Gazette du Palais*, du 25/10/1996.

III. — LE CYBERCONTRÔLE, POUR QUELLE RÉGULATION ?

On ne peut, ici, que se borner à mentionner l'existence d'un débat qui devient de plus en plus central dans la société contemporaine, celui du *cybercontrôle*. Une véritable *Lex Informatica* concernant notamment les questions liées à la preuve, à la procédure, à la responsabilité pénale [88] est en train de se développer. Et l'on peut dire, de ce point de vue, que le cyberespace n'est plus une zone de non droit. On l'a écrit, d'ailleurs : « le mythe du vide juridique véhiculé par certains à propos de l'Internet ne semble pas être très réaliste » [89]. L'application du droit interne ne poserait pas de difficulté majeure en plusieurs domaines comme ceux de la propriété littéraire et artistique et de la propriété industrielle, mais « les véritables questions (seraient) posées par l'internationalité du réseau », et « des interrogations évidentes demeure(raie)nt sur la détermination des responsables » [90].

Mais quel contrôle ? Parmi les caractéristiques du réseau Internet que l'on dénombrait plus haut, la *transnationalité*, la *fugacité*, la *volatilité des contenus* et les *stratégies d'acteurs* dans la communauté virtuelle ont un impact direct sur les questions pénales. La *transnationalité*, en particulier, est une source de difficulté d'application du droit pénal [91], à commencer par les aspects liés à la responsabilité pénale [92] – notamment la délicate question de l'imputabilité d'un délit commis sur l'Internet [93]. En France, par exemple, les fournisseurs d'accès se sont considérés comme les victimes de la méconnaissance technologique des autorités judiciaires [94].

En réalité, il convient de faire intervenir également les caractères de *fugacité* et de *volatilité des contenus*, car les diffuseurs affirment qu'il est matériellement impossible pour un fournisseur d'accès de contrôler l'ensemble du contenu des messages transmis par les groupes qui se présentent dans la communauté virtuelle [95]. À ce propos, en France, un Rapport de la Mission Interministérielle sur l'Internet a montré que la fugacité et la volatilité des contenus est une source de difficultés pour les enquêtes pénales et pour l'application de certains textes [96].

En outre, les *stratégies d'acteurs virtuels* sont malaisées à saisir dans un monde abstrait en rapide mutation, où le statut et le rôle des acteurs sont extrêmement variables. Un usager peut être à la fois serveur, éditeur, consommateur, témoignant d'une grande confusion de rôles dans la communauté virtuelle. Cela rend très laborieuse non seulement l'appréhension de l'infraction virtuelle mais aussi la définition des catégories sur

[88] Cf. Aron Mefford, « Lex Informatica : Foundations of Law on the Internet », dans *Indiana Journal of Global Legal Studies*, vol. 5 (I), 1997.

[89] Cf. Nicolas Brault, « Le Droit applicable à Internet. De l'abîme aux sommets » dans *Legicom. Revue Trimestrielle du droit de la communication*, *op. cit.*

[90] *Ibid., eod. loc.*

[91] *Internet. Enjeux juridiques, op. cit.,* p. 47.

[92] Cf. Anne Wells Branscomb, « Anonymity, Autonomy and Accountability…», *op. cit.,* p. 1645.

[93] Cf. Frédéric Gras, « Internet et la responsabilité pénale », dans *Legicom. Revue Trimestrielle du droit de la communication*, N° 12, 1996/2.

[94] *Ibid., eod. loc.*

[95] *Ibid., eod. loc.*

[96] *Internet. Enjeux juridiques, op. cit.,* p.50-52.

lesquelles est fondée l'approche juridique. En outre, la confusion des rôles rend elle-même parfois impossible la détermination de la règle de droit applicable [97].

Dans le cas d'activités délictueuses par Internet, l'enquête pénale se trouve dans un état de confusion s'agissant de l'identification de l'auteur de l'infraction et de l'établissement de l'existence de ses éléments constitutifs. Outre le fait que le message litigieux risque de disparaître, l'auteur peut toujours se défendre en soutenant qu'il a été modifié, voir dénaturé et falsifié par un tiers [98]. Par ailleurs, selon le Rapport, le simple témoignage d'une personne ayant vu le message, ou son enregistrement par un utilisateur, n'ont pas la même force probante qu'un procès verbal constatant l'infraction [99].

Il n'empêche. Le droit se met en marche pour tenter de rattraper une criminalité virtuelle qui pourra atteindre les 200 millions de personnes dont les statistiques disent qu'elles seront prochainement rattachées au système Internet [100]. Plusieurs pays essayent de réguler le cyberespace, à commencer par les États-Unis eux-mêmes, où le nombre des foyers connectés sur l'Internet sera, en l'an 2000, de 35,2 millions (soit un tiers des foyers du pays) [101]. Néanmoins, là-bas, un débat passionné a pris corps, prenant pour point d'appui le premier amendement de la Constitution américaine et la libre expression [102], et ce sont les propositions d'auto-contrôle de ce système abstrait qui paraissent séduire la société américaine.

Au nombre des diverses tentatives de régulation proposées, on se doit de mentionner celles qui régissent la diffusion de la pornographie. L'importance et la visibilité d'une criminalité virtuelle à caractère pornographique, concernant notamment les enfants, a, en effet, provoqué l'adoption, en février 1996, du *Communications Decency Act*. En ce qui concerne la protection des mineurs, ce texte propose non seulement la mise en place de dispositifs techniques dans les programmes audiovisuels, mais encore l'extension de cette protection à tout message à caractère « indécent » [103]. Dans l'article 223, le *Decency Act* sanctionne d'une amende et d'une peine de prison la diffusion des contenus obscènes concernant des mineurs. Néanmoins, la législation nord-américaine n'incrimine pas les usagers ni les fournisseurs de services qui, dans la mesure où ils agissent de bonne foi et prennent les dispositions pour limiter les contenus jugés obscènes, ne sont pas tenus responsables de violation du premier amendement de la Constitution [104]. La responsabilité des internautes est limitée aux cas où l'opérateur autorise l'utilisation de ses infrastructures en sachant qu'elles sont employées pour des activités illicites (*Communications Decency Act,* articles 223a-2, et 223d-2). Par ailleurs, les employeurs ne sont pas tenus pour responsables des actes commis par des employés hors de leurs activités professionnelles [105].

[97] *Ibid.*, p. 53.
[98] *Ibid.*, p. 50.
[99] *Ibid., eod. loc.*
[100] *Ibid.*, p. 7. Ce rapport affirme que, en l'an 2000, près de 200 millions de personnes seront raccordées à l'Internet.
[101] Selon le Cabinet Jupiter Communication, cité par le Rapport au ministère délégué à la Poste, aux Télécommunications et à l'Espace et au ministre de la Culture, Mission Interministérielle sur l'Internet, *op. cit.,* p. 57.
[102] La littérature américaine est abondante sur ce sujet.
[103] Cf. *Internet. Enjeux juridiques, op. cit.*, p. 57.
[104] *Ibid., eod. loc.*.
[105] *Ibid.*, p. 59.

Ce texte, il faut le préciser, a été la cible de critiques dans une société fondée sur la primauté de la libre expression. Certains dispositifs du *Decency Act* font l'objet aujourd'hui d'un recours en constitutionnalité pour violation du premier amendement de la Constitution des États-Unis, et l'entrée en vigueur des dispositions les plus controversées semble actuellement compromise [106].

En France, le cybercontrôle se présente autrement. Il est vrai qu'en matière d'Internet ce pays est « à la queue du peloton européen » [107], selon l'expression du Rapport interministériel lui-même [108]. Même si un effort est fait pour développer rapidement le réseau, les résistances à l'impulsion de ce nouvel espace social sont clairement perceptibles au sein de la société française. L'élaboration de nouvelles règles de comportement y a provoqué d'emblée une grande inquiétude sociale et juridique, notamment à l'endroit de ce qu'on qualifie de « nouvelle civilité » [109]. D'une part, les conceptions traditionnelles de vie en société se trouvent par trop bouleversées là où les communications prévirtuelles l'emportent. Par ailleurs, l'attachement humaniste aux valeurs qui se trouvent au fondement des droits de la personne et des libertés de chacun y sont primordiales. Le respect inconditionnel de ces valeurs exigé de la communauté virtuelle a pour conséquence que, à l'échelle nationale, la jurisprudence française incrimine les fournisseurs d'accès dès lors qu'ils transportent le message litigieux. Le nouveau code pénal intègre ces décisions jurisprudentielles [110], notamment lorsqu'il réprime, en son article 227-24, « le fait soit de fabriquer, de transporter, de diffuser par quelque moyen que ce soit et quel qu'en soit le support un message à caractère violent ou pornographique ou de nature à porter gravement atteinte à la dignité humaine, soit de faire commerce d'une telle image… » [111]. Selon la conception française, le cyberespace doit être, certes, un espace de libre expression, mais surtout « un outil de progrès et d'enrichissement plutôt que synonyme de danger » [112].

En matière de cybercontrôle étatique, une « démarche purement nationale est illusoire » [113]. Par son caractère transnational et décentralisé, par la fugacité et la volatilité de ses contenus, le cyberespace ne peut s'organiser et définir des règles communes de fonctionnement qu'à partir d'une coopération internationale sans faille. Dans ce sens, l'adoption de principes communs est essentielle pour permettre l'entraide judiciaire à l'échelle planétaire, et l'Union européenne, en ce domaine, commence à marquer sa place en tant qu'instance supranationale déterminante pour ce nouveau type de contrôle. Elle entend établir une déontologie minimale permettant de fonder les choix nationaux [114].

Pourtant, le cyberespace, par sa structure, ses caractéristiques et son mode de fonctionnement, n'est guère le lieu où puisse aisément s'ériger un type de contrôle *a priori* ; un système de normes coercitives d'autorisations et d'obligations de contenus à respecter

106 *Ibid., eod. loc.*

107 L'Internet est un réseau anglo-saxon, car 80 % des serveurs sont nord-américains, et 90 % des échanges se font en anglais. Cf. *Internet. Enjeux juridiques, op. cit.,* p. 12.

108 *Ibid.*, p. 9.

109 *Ibid., eod. loc.*

110 Cf. Frédéric Gras, « Internet et la responsabilité pénale », *op. cit.*

111 Cf. code pénal, art. 227-24.

112 *Ibid., eod. loc.*

113 Cf. Voir *Internet. Enjeux juridiques, op. cit.,* p. 8.

114 *Ibid.*, p. 11.

n'est, en effet, pas envisageable ici comme, par exemple, dans l'audiovisuel – une comparaison qui se fait pourtant volontiers. Le cybercontrôle ne peut se produire qu'à deux moments : celui de l'offre ou de la demande de services, par des mesures d'autorégulation ; ou bien *a posteriori* [115].

L'autorégulation du cyberespace est, d'ailleurs, un thème de grande actualité. L'autocontrôle des acteurs internautes peut se faire, notamment, soit par une autocensure de la part des fournisseurs, soit par des dispositifs de classification des services ou de filtrage parental [116]. Comme le virtuel prend une place prédominante dans la vie des gens, et comme l'information et la communication sont désormais au cœur du lien social, la famille est appelée à jouer de nouveau un rôle central de contrôle, d'éducation et de socialisation dans la communauté virtuelle, malgré son éclatement et une démission sociale certaine dans l'espace pré-virtuel – que maîtrisent souvent mieux les enfants que les parents.

On observe, alors, une transformation des concepts traditionnels d'espace public et d'espace privé. Pour rationaliser ou limiter les abus du cyberespace, ce sont des éléments moraux, véhiculés déjà par la société bourgeoise issue des Lumières [117], qui sont réintroduits dans les systèmes abstraits. L'Internet, « espace public restauré », fait émerger un « espace privé transfiguré », à la fois limitatif du premier et très ouvert à lui [118]. À la sphère privée, l'on demande de contraindre les abus de la sphère publique tout en la co-constituant, ce qui mène, sans doute, à un débat sur la cyberdémocratie [119], qui dépasse les limites des quelques réflexions ici présentées. On ne peut, cependant, passer sous silence les nouveaux canons de cette civilité virtuelle, règles minimales concernant le respect des droits de la personne : utilisation d'un langage courtois, non incitation à la violence politique et sexuelle, accentuation du droit des consommateurs, abstention de comportements criminels dans cet espace. Les professionnels du virtuel sont invités à élaborer un code de déontologie, comme ces codes de conduite qui se multiplient actuellement dans l'espace globalisé des échanges industriels, commerciaux et financiers. Un tel code pourrait établir les règles de transparence, de responsabilité et de respect du cadre légal en vigueur. Ce qui tend à se passer en France, d'ailleurs, avant la lettre, les fournisseurs d'accès, prévenus par la mise en examen de certains d'entre eux, pratiquant une sévère autorégulation en censurant à la source les sites présentant les plus grands risques d'illicéité [120].

115 *Ibid.*, p. 9.
116 *Ibid.*, p. 10.
117 *Ibid.*, p. 561.
118 Cf. Gérard Sutter et Hervé Zécler, « Internet : espace public, espace privé ? » dans *Revue de la Recherche Juridique Droit Prospectif*, Presses Universitaires d'Aix-Marseille, 1998-2, p. 561-575.
119 Cf. Mark Poster, « Cyberdemocracy, The Internet and the Public Sphere », dans David Holmes (ed.), *Virtual Politics…*, *op. cit.*, p. 212-227.
120 Cf. Nicolas Brault, « Le Droit applicable à Internet. De l'abîme aux sommets », *op. cit.* Voir aussi *Le Monde* du 19-20 mai 1996.

Or, l'impact de ces transformations dans le champ criminel et dans celui du contrôle, interroge non seulement le Droit dans son ensemble, mais aussi et surtout, très précisément en l'occurrence, le droit pénal et la pensée criminologique.

* *
*

On souhaiterait, en guise de conclusion, introduire quelques brèves réflexions sur les mutations du champ criminologique, sans aucune prétention d'épuiser le sujet. On sent bien, ne serait-ce que par les développements qui précèdent, que la criminologie est un champ épistémologique en pleine mutation. Les troubles provoqués par l'émergence de la criminalité virtuelle ne peuvent pas ne pas avoir un impact sur la pensée criminologique. Ce savoir, construit depuis un siècle pour répondre aux désordres de la société industrielle, a été critiqué et déconstruit, depuis, d'abord par les courants marxistes [121], ceux-ci étant à leur tour révisés par les criminologues critiques [122]. À l'heure actuelle, ces cadres de pensée développés au sein des sociétés pré-virtuelles ne sont plus capables d'expliquer ces nouveaux phénomènes qui caractérisent la criminalité immatérielle. La pensée criminologique doit être aujourd'hui soumise à une problématisation renouvelée.

La visée fondamentale de la criminologie a été le comportement criminel dans sa version la plus individualisée et « corporelle » : le crime était perçu comme conséquence génétique. Le corps de l'individu a été placé par l'école lombrosienne au cœur du phénomène criminel. Cette matrice criminologique positiviste initiale se modifia avec le recadrage opéré par les théories de la réaction sociale, attribuant aux institutions de contrôle une part de responsabilité dans la production sociale de la déviance et du délit. Les courants marxistes, à leur tour, ont développé et développent une criminologie critique, soucieuse de dénoncer le capitalisme et l'État comme source criminogène. Comme conséquence de ces visions critiques, des pratiques alternatives de contrôle ont été mises en place, en Angleterre notamment, ce qui a contribué, comme l'a bien montré Stanley Cohen, à étendre le contrôle étatique [123].

Où en est la criminologie ? La situation empirique actuelle de la criminologie est riche de micro-études réalisées sur les thèmes les plus variés. Les réflexions criminologiques sur la différenciation entre les sexes est, par exemple, significative dans la littérature anglo-saxonne, où elle tend à remplacer, en quelque sorte, l'essor des études marxistes des années 1970-80. Du point de vue de son développement théorique, on a eu, déjà, l'occasion de montrer, au travers de l'examen de l'émergence d'un *système criminel transnational*, qu'un recadrage de la problématique du crime a, déjà, été réalisée en raison de l'émergence de nouvelles formes de criminalité transterritoriales. On a fait alors remarquer, notamment, que l'enjeu ne consistait plus en une réflexion en termes de *criminologie comparative* [124], même si cette dernière avait constitué un pas en avant par

121 Voir spécialement Walton, Taylor et Young, *The New Criminology*, Londres, 1973.
122 Cf. Stanley Cohen, *The Social Control*, Polity Press, 1985.
123 *Ibid., eod. loc.*
124 La *criminologie comparative* est la discipline consacrée à l'étude transculturelle du crime et la justice criminelle dans deux ou plusieurs sociétés. Cf. W. Thornton, L. Voigt, *Delinquency and Justice*, Mc Graw-Hill, 1992, p. 460.

rapport aux criminologies développées à l'intérieur des espaces nationaux, dépassant « l'attitude insulaire » des chercheurs [125]. Avec l'émergence d'un *champ criminologique nouveau* [126], notamment avec les *relations transnationales criminelles*, on a vu qu'il s'agissait de *redimensionner* la question criminelle à l'échelle mondiale. Ce champ présentant une dimension inédite, celle de l'extension *globale* du phénomène criminel ; c'est déjà d'un *changement de paradigme* qu'il s'agissait [127], de la nécessité de l'adoption, en criminologie, d'un *paradigme systémique transnational*. Ce paradigme, qui se réfère aux activités criminelles exigeant, pour leur réalisation, un « terrain sûr », un « espace terrain », même s'il est dé-territorialisé, un type de relation de co-présence, est désormais cantonné aux sociétés non virtuelles. Les activités criminelles virtuelles, elles, répétons-le, n'ont pas besoin du face à face : elles sont « désincarnées ». Un ajustement de ce paradigme s'impose donc si l'on veut qu'il se révèle capable de rendre compte de ce glissement vers l'immatériel et d'encadrer une réflexion criminologique novatrice à l'orée du XXI[e] siècle. Aux spécialistes du champ, il appartiendra de développer un *paradigme systémique abstrait* faute duquel on continuera de sauter dans le vide pour mieux retomber dans le chaos virtuel !

[125] *Ibid*., p. 459 et s.

[126] G.T. Marx, « Europe in 1992 *:* Some Implications for research on Policing Across national Borders », dans *On Complexity and Socio-legal Studies : Some European Examples*, , A.-J. Arnaud (éd.), Onati Proceedings, n° 14, 1993, p. 71-88.

[127] Voir mon étude sur ce thème, parue dans *Droit et Société*, n° 35, 1997, sous le titre « La transnationalisation du champ pénal : Réflexions sur les mutations du crime et du contrôle ».