

16 mai 2000 - Seul le prononcé fait foi

[Télécharger le .pdf](#)

Déclaration de M. Jacques Chirac, Président de la République, sur la lutte contre la cybercriminalité organisée par les Etats en partenariat avec les entreprises et les associations, Paris le 16 mai 2000.

Monsieur le ministre de l'Intérieur,
Madame et Messieurs les Chefs de Délégation,
Messieurs les Parlementaires,
Mesdames et Messieurs les Délégués,
Mesdames, Messieurs,

Je suis heureux de vous accueillir ce soir et de souhaiter la bienvenue à l'ensemble des participants au dialogue organisé par le G8, sous présidence japonaise - l'ambassadeur du Japon me permettra de le saluer particulièrement à ce titre - , entre le secteur privé et les pouvoirs publics sur le thème de la cybercriminalité.

Hommes et femmes d'entreprises, élus, responsables d'associations, magistrats, policiers, diplomates, administrateurs, vous poursuivez les mêmes objectifs : étendre au cyber-espace le droit fondamental à la sécurité, assurer la confiance indispensable à son développement. La réunion annuelle des chefs d'Etat et de gouvernement de nos huit pays permet de donner à la régulation internationale, à la maîtrise et à l'humanisation de la mondialisation, des impulsions qui sont nécessaires. N'oublions jamais en effet que, derrière le rêve d'une nouvelle économie sans frontière ni entrave, se profilent trois grands dangers qui doivent être pris en compte et maîtrisés : l'accroissement des inégalités entre riches et pauvres, la dégradation de l'écosystème planétaire et l'expansion de la criminalité internationale.

L'internet, réseau planétaire de communication et d'échanges, se révèle l'un des principaux vecteurs de la globalisation. Il jouera un rôle croissant dans la vie quotidienne des hommes et des femmes de nos pays. Il est donc de notre responsabilité d'en assurer le fonctionnement harmonieux.

Je souhaite que vos travaux provoquent cette prise de conscience grâce à laquelle il est plus aisé ensuite de parvenir aux solutions qu'impose l'intérêt commun de l'humanité et de la planète. Depuis plusieurs années, nous défrichons les terrains inconnus de la lutte contre le crime de haute technologie. Nous expérimentons des solutions nouvelles. Dès le Sommet de Lyon, du G7/G8, en 1996, puis à Washington et à Moscou, nous avons engagé nos Etats dans des coopérations opérationnelles.

Cette démarche nous conduit aujourd'hui à nouer un dialogue plus étroit avec les entreprises et avec les associations. Les Etats ne peuvent assurer la sécurité sur internet sans jeter, avec elles, les bases d'une authentique corégulation, nationale et internationale.

*

* *

Mesdames, Messieurs,

L'internet, dont la construction s'est nourrie des idéaux de liberté et de solidarité universelle, met notre droit et nos institutions à l'épreuve. Il nous oblige à nous interroger sur le rôle de l'Etat, sur la conception que nous avons de l'Etat de droit et la manière de le faire vivre.

... la conception que nous avons de l'Etat et de la manière de le faire vivre.

L'usage des réseaux numériques est un fait de société. L'information et la communication, la culture et la connaissance, le commerce et toutes les formes d'échanges en sont ou en seront affectés.

Nous ne percevons encore que les balbutiements des technologies de l'information. Les conséquences qu'elles auront demain, nous sommes bien en peine de toutes les appréhender. D'ailleurs, à vouloir tout prévoir, nous ferions probablement fausse route. Il ne faut pas figer, il faut accompagner.

Nous pressentons la puissance de ces nouveaux outils pour revitaliser et développer nos structures économiques, multiplier les échanges, relier les hommes, leur donner un accès plus démocratique au savoir. C'est pour cela que les responsables, du Sud aussi bien que du Nord, veulent encourager l'usage de l'internet sur leur territoire.

Comment construire une société de l'information qui soit une société de confiance ? Une société harmonieuse fondée sur un juste équilibre entre la liberté d'expression, principe intangible, et la sécurité des personnes et des biens. Une société de progrès, où les citoyens se sentent rassurés, confortés dans leurs initiatives, incités à épanouir leurs talents. Une société de justice, qui garantisse l'égalité des chances et le respect de la loi.

Certains qualifient le "cyber-espace" de nouveau monde, de monde virtuel, mais il ne faut pas s'y tromper. Il n'y a pas deux mondes différents par nature, le réel et le virtuel : il n'y a qu'un seul et même monde, dans lequel doivent s'appliquer et être respectées les mêmes valeurs, la liberté, l'égalité, la dignité de la personne humaine. Souhaiter que s'applique sur la Toile un état d'exception au nom du bel idéal de liberté qu'elle incarne reviendrait en réalité à y maintenir l'état sauvage, c'est-à-dire la loi du plus fort.

Vous le savez mieux que quiconque : les cyber-criminels ne sont pas des criminels virtuels ! Ils développent sur la Toile, comme ailleurs, leurs funestes forfaits.

Les tentatives de fraude et d'escroquerie en ligne représentent, en France, je crois, la moitié des litiges relatifs à l'usage des cartes bancaires. Comment accroître la sécurité des transactions, condition indispensable au développement du commerce électronique ?

Comment protéger les données personnelles et la vie privée des internautes de la curiosité envahissante d'autrui, que l'intrusion provienne d'un particulier, d'une entreprise ou d'un organisme public ? Comment éviter l'identification et le fichage de ceux qui consultent un site sur Internet ?

Comment empêcher l'usage des réseaux par les mafias, les proxénètes, les pédophiles, qui profitent de l'anonymat, de l'universalité et de la fugacité d'internet pour se livrer à des pratiques illicites, trafics de personnes, de biens, de stupéfiants ?

Comment préserver la sécurité nationale face à toutes les formes de terrorisme ? Face aussi aux agressions menées contre nos systèmes de défense et nos services publics ?

Comment combattre ces piratages, ces sabotages qui menacent les entreprises et les particuliers ? Comment réagir à la propagation instantanée de virus informatiques, gangrène de nos systèmes d'information ?

Pour prévenir et réprimer le crime, nos sociétés démocratiques ne connaissent qu'un seul acteur légitime, l'Etat, et une seule méthode, l'application de la loi.

Exercé dans le respect des libertés publiques, ce rôle de l'Etat constitue l'un des grands progrès de la civilisation. Chacun renonce aux vengeances individuelles, à l'usage privé de la force, au profit d'une discipline collective. C'est ainsi que l'on s'émancipe de l'arbitraire, de l'oppression, des féodalités qui résultent nécessairement de l'absence d'Etat.

Rien ne justifierait que nous y renoncions dans le cyber-espace. Mais les Etats sont-ils encore capables d'assumer cette mission ? Sauront-ils, pourront-ils ajouter la dimension du réseau à leurs modes traditionnels de fonctionnement et accroître les coopérations ?

Certains craignent que l'internet, de par son développement spontané, décentralisé, foisonnant, se révèle une zone de non-droit ou en tout cas un univers livré à des réglementations réduites, allégées, tronquées.

Comment en effet appliquer le droit, conçu pour régler des réalités tangibles et permanentes, au

royaume de l'immatériel et de l'éphémère?

Législateurs, policiers et juges ne sont-ils pas quelque peu désarmés face à l'extraterritorialité des réseaux ?

Les concepts sur lesquels sont fondés nos ordres juridiques -l'identité, la preuve, l'authenticité- sont-ils encore valides, alors qu'ils sont confrontés à des technologies numériques qui permettent la reproduction parfaite et presque gratuite, la transmission instantanée, la manipulation des signes, la falsification ?

Face à un formidable progrès technologique, gouvernements et parlements doivent acclimater nos législations nationales à l'internet, les soumettre à un véritable audit. Conduit dans un souci d'harmonisation internationale, cet audit inspirera la modernisation de nos lois.

Dans son champ de compétence, l'Union européenne s'y est résolument engagée. Ses directives sur la valeur de la signature électronique, la protection des données personnelles, et à présent le commerce électronique, en témoignent.

Sous la Présidence française, la Commission présentera, à notre demande, une communication sur la sécurité de l'internet et nous proposerons d'étendre les missions d'Europol à la protection des réseaux.\

Contre la cybercriminalité, l'Etat ne pourra jouer son rôle qu'en partenariat avec les acteurs de l'internet, les entreprises mais aussi les associations d'usagers.

La corégulation, c'est un contrat moral passé entre l'Etat et les entreprises. Un contrat fondé sur le partage des responsabilités.

Responsabilité des entreprises d'abord. Dans la tradition juridique latine, reconnaître que des acteurs privés et des mécanismes librement consentis peuvent être plus efficaces que la puissance publique et la loi, comme sources et garants du droit, ce n'est pas une évidence.

Mais ce n'est pas une révolution non plus. Qu'on songe, en France, aux responsabilités dévolues aux ordres professionnels dans l'organisation de certaines professions libérales.

De la même manière, pour assurer la sécurité des réseaux et affermir la confiance, encourageons l'établissement, par les entreprises, de chartes de bonne conduite, de codes déontologiques, établis sur mesure, transnationaux, évolutifs, et dont la police sera assurée par les intéressés eux-mêmes. Dans ce domaine, la bonne règle naît de la libre adhésion.

Les acteurs de l'internet ont compris l'intérêt d'une telle démarche. Etendue, elle garantira le bon fonctionnement des réseaux. Elle évitera des réglementations, pointilleuses et figées, qui risqueraient d'entraver le processus créatif, qui est la richesse de l'internet.

La présence parmi nous ce soir de tant de représentants de grands groupes français et internationaux l'atteste : nous pourrions faire confiance aux entreprises, à leur créativité, leur dynamisme, leur sens de l'éthique professionnelle, pour imaginer, en matière de sécurité, des dispositifs adaptés et efficaces.

Mais la privatisation du droit atteint ses limites lorsque des tricheurs entrent dans le jeu. Alors s'affirme le besoin d'Etat, le besoin d'un arbitre, le besoin d'une puissance publique, qui permette aux règles d'être respectées.

L'Etat doit inscrire son action sous le signe de la subsidiarité.

Avec les entreprises et les associations, il développera d'abord une approche de prévention et de sensibilisation. Prévenir les cyber-commerçants des enjeux de sécurité sur le Net. Prévenir les internautes des risques auxquels ils s'exposent à parcourir les réseaux. Prévenir les fournisseurs d'accès et d'hébergement du caractère éventuellement illicite des contenus qu'ils diffusent.

Prévenir les apprentis pirates du caractère délictueux de ce qu'ils considèrent souvent comme un exploit. Prévenir les parents : pas plus qu'ils ne laisseraient leurs enfants se promener seuls la nuit dans les rues d'une grande ville, ils ne doivent les laisser naviguer, sans conseil ni précaution, sur les réseaux.

Tous, les informer des solutions possibles : elles naissent de la technologie elle-même, qu'il s'agisse du bon usage de la cryptologie ou d'autres protections informatiques.

Avec les entreprises et les associations, l'Etat encouragera les démarches de certification. La labellisation des sites, par des tiers de confiance, personnes publiques ou privées, banques,

assurances, associations professionnelles, offrira une meilleure garantie de sécurité aux utilisateurs.

L'Etat soutiendra les initiatives spontanées ou institutionnalisées de cyber-médiation. Une bonne médiation vaut toujours mieux qu'un long procès. Ce principe se vérifie particulièrement sur des réseaux internationaux en pleine évolution.

Dans un domaine cependant, la responsabilité d'agir incombe uniquement à l'Etat. Lorsqu'il s'agit de prononcer une sanction et de la faire appliquer, seul l'Etat, qui dispose du pouvoir de contraindre, est pleinement légitime.

Comme plusieurs de ses partenaires du G8, la France a fait de la lutte contre la cybercriminalité une priorité. Le Ministre de l'intérieur vous l'a, je le sais, rappelé. La création d'un office central de lutte contre la criminalité liée aux technologies de l'information a été annoncée. Le Secrétariat général de la Défense nationale s'est vu confier une mission de veille et de conseil. Une structure d'alerte et d'assistance sur internet, chargée de répondre aux attaques informatiques, vient de se mettre en place dans le cadre d'un réseau mondial de gestion des urgences informatiques.

Nous devons, dans les années qui viennent, intensifier notre effort, financier et humain, pour disposer d'une puissance d'intervention accrue à la hauteur des défis que pose aujourd'hui la cybercriminalité aux sociétés démocratiques. Nous devons dans ce but construire une coopération efficace entre entreprises et administrations, facilitant l'échange d'expériences et d'informations et l'aboutissement des enquêtes. Nous devons affirmer la mission d'Interpol, pour disposer, au niveau mondial, de l'indispensable instance d'entraide policière.

Car, à l'évidence, cette action des Etats, des entreprises, n'est véritablement pertinente, véritablement crédible, qu'au niveau mondial.

D'ores et déjà, au sein du G8, nous avons identifié les conditions d'une coopération internationale efficace. La France, et le ministre de l'Intérieur en particulier, ont été très actifs en ce domaine.

Nous devons d'abord surmonter l'obstacle qui provient de la différence entre nos législations. Les criminels en jouent. Ils en exploitent les failles. Chacun d'entre nous est légitimement attaché à ses lois. Elles sont l'expression d'une histoire nationale, d'une culture, des valeurs d'un peuple, d'une conquête de la liberté. En témoignent nos débats transatlantiques sur l'étendue de la liberté d'expression. L'Amérique la voudrait absolue, dans la tradition des pères fondateurs. L'Europe, traumatisée par la Shoah, se méfie des excès criminels auxquels elle peut conduire. Aujourd'hui, nous apprenons à harmoniser nos lois. Nous apprenons à établir des mécanismes de conciliation. Nous apprenons à construire, là où c'est nécessaire, une loi fondamentale de portée mondiale. Je ne prendrai qu'une illustration de ce processus de longue haleine : le travail exemplaire que conduisent l'Europe et les Etats-Unis pour assurer la protection des données personnelles et de la vie privée sur internet.

Nous devons ensuite remédier à la lenteur et au formalisme des procédures de coopération et d'entraide judiciaire qui permettent parfois aux criminels de passer entre les mailles des filets. L'efficacité commande de trouver de nouvelles procédures, plus rapides, presque instantanées, et d'instaurer des automatismes, des obligations de coopération et de transparence.

Mais le respect des libertés, de la vie privée, de la présomption d'innocence, impose des garde-fous, des protections contre l'action publique. Où est le bon équilibre ? Quels seront les recours des citoyens contre un appareil judiciaire et policier qui déploiera ses effets en dehors de son territoire ? Comment sera respectée la présomption d'innocence ?

Nous voulons lutter efficacement contre le crime de haute technologie. Mais à aucun prix nous ne voulons édifier un système répressif international qui menacerait les libertés publiques si chèrement acquises par nos peuples. C'est pour nous tous une lourde responsabilité et une priorité.

Ce dont nous avons besoin, c'est d'un Etat de droit international, un cadre juridique universel à la mesure du caractère mondial de l'internet. Un cadre qui, dans le respect des souverainetés des Etats, définisse les infractions et fixe les procédures admises pour les établir et les réprimer.

Le Conseil de l'Europe s'est attelé à la tâche en liaison avec les autres Etats du G8. Il prépare une convention qui sera pionnière. Elle permettra à chacun de disposer d'une loi internationale sur

convention qui sera promulguée. Elle permettra à chacun de disposer d'une loi internationale sur laquelle fonder ses actions contre les criminels qui prennent l'internet pour vecteur ou pour cible, et ceci où qu'ils soient.

Je souhaite que ce traité voie le jour rapidement et que tous les pays intéressés puissent s'y associer. Nous y parviendrons si nous savons ménager l'avenir.

Ménager l'avenir, c'est établir un texte qui reconnaisse sa nature innovante, c'est-à-dire incertaine. Il devra prévoir des mécanismes de révision particulièrement souples et rapides. Sans quoi nous risquerions un traité mort-né, dépassé avant même son entrée en vigueur.

Ménager l'avenir, c'est s'ouvrir au dialogue avec les autres Etats. Je ne pense pas seulement aux pays développés, mais, tout autant, aux pays en développement, confrontés eux aussi à cette forme de délinquance. D'aucuns ont déjà démontré qu'ils sont des partenaires essentiels dans l'émergence d'une nouvelle économie. Je pense à l'Inde, pour ne citer qu'elle. Que signifierait un texte international auquel elle serait étrangère ?

Monsieur le ministre,

Mesdames et messieurs,

A Okinawa, les chefs d'Etat et de gouvernement devront tirer les conclusions de vos débats et orienter les travaux de nos pays pour l'avenir. Je sais que le Japon, M. l'Ambassadeur, y sera particulièrement attentif, et je ne doute pas un instant de son efficacité.

Sans préjuger de vos recommandations et des suites du dialogue inédit que vous avez engagé à Paris, il me semble que quatre orientations se dessinent.

Cette dimension nouvelle, extraterritoriale, qui naît de l'internet, doit être civilisée. Là comme ailleurs, il faut des lois pour assurer la liberté et la sécurité de tous. Il faut des institutions et des procédures pour les faire respecter. Première orientation.

Deuxième orientation : il revient aux Etats d'assumer ensemble les responsabilités qui leur incombent pour maintenir l'ordre et la sécurité publics, dans le respect des principes de l'Etat de droit. Ils assumeront leur mission en étroite concertation avec les utilisateurs des réseaux. Une corégulation devra s'établir, par laquelle entreprises et organismes publics s'épauleront au service de la loi.

Troisième orientation : les Huit ont une responsabilité particulière. Ils devraient intensifier leurs travaux en commun, pour élaborer les instruments du respect de la loi dans le cyber-espace : construction des cadres juridiques nationaux et internationaux appropriés, consolidation des dispositifs de coopération opérationnelle pour la prévention et la répression du cyber-crime, effort de formation des agents potentiellement touchés par la menace.

Enfin, quatrième orientation, les Huit doivent associer l'ensemble des Etats à cet effort. Pour que tous, et notamment le monde en développement, soient à armes égales face au danger. Pour prévenir la prolifération à travers le monde des "paradis informatiques", sanctuaires des cyber-criminels. Pour que la loi que nous établirons, respectueuse de la diversité des traditions juridiques, fonde son efficacité sur son universalité.

C'est avec cet espoir et cette détermination que nous abordons cette nouvelle phase de l'évolution de nos sociétés. Ensemble nous mettrons l'internet au service de l'homme, de tous les hommes.

Je vous remercie.