SÉCURITÉ ET LIBERTÉ SUR L'INTERNET

Jacques VINCENT-CARREFOUR (55),

France Télécom,

(ancien délégué interministériel pour la sécurité des systèmes d'information)

Une introduction à la sécurité sur Internet

C'est devenu un lieu commun que de reprocher à l'Internet son manque de sécurité. Que l'on cherche à dénigrer ce réseau ou que l'on en fasse une analyse objective, la sécurité vient en effet au tout premier rang des qualités dont on déplore l'absence. Mais que désigne-t-on sous ce vocable de sécurité ? Il est bon de s'attarder un peu ici car le sens de ce mot varie suivant les disciplines et les milieux.

Pour *Larousse*, la *sécurité*, c'est la confiance résultant de la pensée qu'il n'y a pas de *péril* à redouter. Une définition tout à fait analogue, avec la même référence au péril, suit le mot *sûreté*. C'est en fait sur la nature de ce péril que les cindyniciens, les experts des sciences du danger, distinguent sécurité de sûreté : la sécurité est considérée comme la confiance d'être protégé vis-à-vis de la malveillance, c'est-à-dire des attaques d'origine humaine, alors que la sûreté se réfère aux menaces d'origine naturelle (inondation, incendie...) ou accidentelle (pannes) (1). C'est ainsi que l'on parle de sûreté nucléaire.

Pour l'Internet, il s'agit bien de sécurité au sens précédent. Ce qui est en cause, ce sont toutes les actions des "pirates informatiques" qui, à travers le réseau, accèdent aux ordinateurs raccordés, prenant ainsi connaissance d'informations confidentielles ou utilisant leur puissance de traitement, voire perturbent les systèmes informatiques, et ce sur leur seule initiative et sans en avoir reçu l'autorisation. Ce sont également les écoutes et pièges divers qui permettent à ces mêmes pirates d'intercepter ou modifier les messages qui circulent sur le réseau, parfois de créer de faux messages. Ce serait s'écarter de l'objet de cet article que de trop détailler ce point. Disons simplement que ces faits, qualifiés en France par le nouveau code pénal d'*accès frauduleux aux systèmes de traitement automatisé de données*, sont réprimés par les lois de tous les grands pays.

Il est aussi bon de savoir que jusqu'à maintenant la très grande majorité de ces "accès frauduleux" a été le fait de personnes qui cherchent à "arrondir leurs fins de mois", avec le plus souvent une complicité interne à l'entreprise spoliée. Il n'y a pas de raison qu'il en soit autrement sur l'Internet, dès lors qu'il y aura matière à s'enrichir de cette façon. En l'état actuel de la sécurité sur l'Internet, il est donc tout à fait prévisible que ces attaques vont se développer, à la fois en fréquence et en importance, au fur et à mesure que se développera le commerce électronique et plus généralement tous les échanges mettant directement ou indirectement en jeu des sommes d'argent – à moins évidemment que des mesures rigoureuses de sécurité ne soient prises.

Ce phénomène d'insécurité sur l'Internet est-il un phénomène nouveau ? Les réseaux de télécommunications, même électroniques, existent depuis des décennies ; les réseaux informatiques de leur côté ne sont pas une innovation récente : on pourrait donc penser qu'il n'en est rien. Il y a cependant de bonnes raisons pour que l'Internet offre une sécurité encore inférieure à celle des réseaux qui l'ont précédé :

– dans un réseau classique de télécommunication, les données échangées lors de la communication et les données de gestion du réseau (y compris celles nécessaires à l'acheminement de la communication) empruntent deux chemins différents, totalement séparés ; il est donc difficile à l'utilisateur de perturber le fonctionnement du réseau. Par ailleurs, les fonctions de gestion sont confiées à des machines spécialisées (au moins dans la partie publique du réseau). Au contraire, dans l'Internet, messages et données de gestion sont intimement mêlés, ce qui fait de toute personne connectée au réseau un pirate potentiel. Par ailleurs, il est possible de perturber l'acheminement des messages en profitant de faiblesses dans des logiciels tout à fait indépendants des logiciels qui assurent les fonctionnalités du réseau ;

– sur un autre plan, l'Internet conduit par nature à une standardisation généralisée des interfaces et modes de traitement des échanges ; cette situation est jusqu'à un certain point souhaitable et même indispen-

(1) Il est bon de signaler que tous ne partagent pas ce choix. Ainsi, pour les experts du tunnel sous la Manche, la sûreté vise au contraire la malveillance et la sécurité les accidents et pannes.

sable. Elle favorise cependant grandement le travail des pirates qui ont ainsi plus facilement la connaissance des systèmes qu'ils veulent attaquer et peuvent travailler sur une grande échelle ;
– enfin, un élément important de la sécurité est la peur du gendarme ; sur l'Internet, cet élément modérateur est très difficile à mettre en place : la mondialisation du réseau rend tout contrôle global extrêmement difficile, compte tenu de l'inévitable existence de paradis juridiques. Les actions de la justice deviennent très vite internationales, ce qui, même au sein de l'Union européenne, soulève d'immenses problèmes. Rappelons que les actions contre le célèbre *Chaos computer club* n'ont pu réellement commencer qu'après que l'Allemagne se fut dotée d'une loi adéquate. Certains prônent l'autodiscipline, à l'instar de ce qui se passe dans les milieux de la recherche ; c'est tout à fait illusoire lorsqu'on est face à des actions émanant d'individus qui restent (ou croient rester) anonymes, ou bien qui font un "coup" puis disparaissent.

La sécurité, fondement des échanges internationaux

Il est donc évident que, si l'on veut que le magnifique outil qu'est l'Internet devienne un outil de progrès, non un outil d'anarchie, il faut impérativement le doter de moyens permettant d'assurer sa sécurité. L'existence d'un certain niveau de confiance est en effet le fondement de tous les échanges nationaux et à un degré beaucoup plus fort encore des échanges internationaux. Plus concrètement, doter le réseau de sécurité c'est assurer, face à la menace qu'est la malveillance, la permanence de trois propriétés de l'information :
– la *confidentialité*, qui veut que l'information ne soit accessible qu'aux personnes autorisées, qu'un message ne soit lisible que par ses seuls destinataires ;
– l'*intégrité*, qui assure que l'information n'a été modifiée ni dans son contenu, ni dans son expéditeur, ni dans son destinataire ; l'authentification et la non-répudiation apparaissent ainsi comme des éléments de l'intégrité. La signature permet d'assurer l'authentification de l'expéditeur ;
– la *disponibilité* enfin qui veut que l'information soit effectivement accessible au moment où l'utilisateur en a le besoin, qui veut aussi que le destinataire d'un message puisse être atteint en permanence.

Ces fonctionnalités s'appliquent aussi bien aux informations échangées sur le réseau qu'aux informations présentes dans les machines qui jouent le rôle de nœud ou de terminal.

Quelques exemples montrent bien l'importance de ces fonctionnalités et l'étendue du besoin. Le premier et le plus complet est évidemment celui du *commerce électronique*. Le problème dans ce domaine est d'instaurer une relation de confiance entre les partenaires d'une transaction ; le fournisseur doit avoir confiance dans la solvabilité de son client – dans certains cas, il doit de plus avoir des assurances quant à son habilitation à passer la commande. À l'inverse, le client doit avoir confiance dans l'aptitude du fournisseur à faire face à ses engagements. Dans le commerce électronique, ces problèmes de confiance présentent une acuité à laquelle même le Minitel ne nous a pas préparés.

La nature même de l'Internet fait que ce commerce devient mondial : il est hors de question pour le client de recourir à un représentant proche ni même à une procédure judiciaire. Il y aura inévitablement des États de "non-droit", des lieux d'exception. Une difficulté analogue se pose pour le fournisseur, bien que dans ce cas elle puisse se résoudre par l'assurance. Le discours libéral classique en la matière qui consiste à dire que seuls les bons survivront ne s'applique plus lorsque l'on est à l'échelle mondiale. Il sera en effet facile pour le grand banditisme ou même pour l'indélicat d'occasion de ramasser des sommes importantes, par exemple grâce à des promesses fallacieuses, puis de disparaître avec son butin. Il suffira d'un très petit nombre de tels pirates pour rendre rapidement le système impossible. Des dispositions sécuritaires devront donc être impérativement prises pour pallier ces inconvénients, authentifier les correspondants, valider les transactions et chaque fois que c'est utile assurer leur confidentialité. La sécurité des *transactions de paiement* pose des problèmes très voisins de ceux du commerce électronique.

Les serveurs peuvent d'ailleurs contenir de fausses informations susceptibles d'avoir des conséquences graves sur le plan économique, social ou politique : déceler et rendre inoffensives ces informations pose des problèmes difficiles, qui dépassent le cadre de cet article.

La protection de la *propriété intellectuelle* est un autre exemple, tout aussi important. Lorsque les informations circulent sans protection dans le réseau, il n'est plus possible de faire valoir un quelconque droit de propriété, chacun pouvant y avoir accès. L'information, quelle qu'elle soit, devient ainsi une *res nullius*, ce qui est sans doute propre à satisfaire certains juristes, mais va conduire à l'effondrement de notre économie de plus en plus fondée justement sur la valeur de l'information. Il faut donc contrôler l'accès à l'information et protéger sa confidentialité lorsqu'elle sera transmise dans le réseau. C'est ainsi que certains ont proposé que la vente des logiciels soit remplacée par celle des clefs donnant accès à des données chiffrées librement accessibles. Plus généralement, des solutions de ce type devront être trouvées pour la *commercialisation de l'information*. Dans les débuts de l'Internet, on a pu trouver sur le réseau certains télégrammes de l'agence France Presse. On imagine la réaction de l'Agence !

La protection des données personnelles et des données commerciales pose des problèmes similaires, avec des solutions voisines, bien que les objectifs soient de natures un peu différentes.

Le dernier exemple est tiré d'une fonction régalienne ; il montre pourquoi les États ont quelques frémissements d'inquiétude. Dans tous les pays, une bonne part des ressources budgétaires provient de taxes mises sur les transactions commerciales, la TVA étant la plus connue mais non la seule. Un commerce sans frontières sur les réseaux pourrait progressivement rendre impossibles de telles impositions – c'est évident pour le commerce d'objets immatériels, informations ou logiciels ; c'est également vrai pour les objets matériels que l'on pourra commander par l'Internet et recevoir par voie postale. Tant que ce commerce électronique restera minoritaire, ce problème pourra être traité à la marge. On sent bien cependant qu'à terme on va, soit vers un commerce totalement libre et sans taxe – l'impôt devant alors se reporter sur d'autres assiettes, ce qui pourrait être socialement insupportable –, soit vers une certaine harmonisation des taux de contribution, concrétisée par un "scellement" des transactions attestant que ces contributions ont bien été prises en compte. Ici encore, ce sont les techniques de sécurité qui peuvent apporter la solution.

Ces différents exemples montrent bien qu'un large emploi de l'Internet dans le secteur économique présuppose un ordre nouveau qui ne peut exister qu'avec la mise en place de dispositions sécuritaires, juridiques, techniques et organisationnelles.

Les moyens de la sécurité : la cryptologie

Il serait difficile de parler sécurité dans la revue de l'X sans faire un peu de technique, c'est-à-dire sans évoquer la cryptologie. Avant d'aborder ce sujet, il faut souligner une erreur trop fréquente qui tend à réduire la sécurité à la technique, à croire que la sécurité peut être acquise par la seule addition d'un produit miracle, matériel ou logiciel – cette illusion fait le bonheur des pirates. Nous sommes ici dans le domaine de la malveillance ; l'imagination ne saurait avoir de limite, et la théorie de l'information enseigne que la sécurité absolue n'existe pas : la seule façon absolument sûre de faire passer un message à une autre personne est que cette personne ait déjà le message en sa possession ! La sécurité ne peut être obtenue que par un processus fondé sur une analyse précise des menaces contre lesquelles on veut se protéger, suivie de la mise en œuvre de mesures permettant de faire face à ces menaces ; ces mesures sont de trois types : mise en place de moyens techniques appropriés (disons 20 % de la sécurité), administratives (c'est l'administration et la méthodologie de mise en œuvre de la sécurité, 30 % de la sécurité), humaines enfin (la sécurité repose sur la confiance que l'on met dans les hommes, 50 % de la sécurité). Chacune de ces mesures est indispensable, mais chacune d'elles, prise isolément, est inutile. L'ensemble doit être évidemment correctement harmonisé et associé : la sécurité ne s'improvise pas, c'est une affaire de spécialiste.

Ceci dit, qu'en est-il de la cryptologie ? Là encore, une consultation du *Larousse* est pleine d'enseignement : le mot n'y figure pas ! On n'y trouve en effet que le mot cryptographie, science des écritures cachées. C'est que pendant des millénaires, il s'est uniquement agi de tenir secret le contenu de messages. Les premiers cryptogrammes connus remontent à l'Égypte ancienne ; Jules César chiffrait les messages qu'il échangeait avec ses informateurs. Cet aspect de la cryptographie a été popularisé par Jules Verne qui l'a prise pour fondement de l'un de ses romans, *La Jangada*.

C'est lors de la guerre de 1939-1945 que la cryptographie a véritablement conquis ses lettres de noblesse. Grâce à l'apport de la mécanique tout d'abord, puis de l'électronique et de l'informatique, grâce surtout à l'apport de mathématiciens de renom, au premier rang desquels il faut placer Alan Turing (2), elle est devenue une science à part entière, méritant ainsi le nom de cryptologie. Aujourd'hui des colloques et des revues lui sont consacrés, et l'on ne peut douter que prochainement *Larousse* reconnaîtra son existence !

Il est hors de l'objet de cet article d'entrer dans les détails de la cryptologie (3). Disons simplement que l'obtention d'un message chiffré Mch à partir d'un message clair Mcl et l'opération inverse s'effectuent grâce à des fonctions de la forme : Mch = F(Mcl,Clé)

Mcl = F'(Mch,Clé')

F et F' sont deux fonctions inverses, réalisées en matériel ou logiciel, choisies pour minimiser la corrélation entre Mch et Mcl ; elles sont souvent largement connues. Ce sont les variables Clé et Clé' qui constituent la *convention secrète* que les deux correspondants ont dû préalablement échanger ; lorsque Clé = Clé', on obtient un système dit à *clés secrètes*. Il est aussi possible de faire en sorte que Clé soit connu de tous, Clé' restant secret et connu de son seul propriétaire. Il est ainsi le seul à pouvoir lire un message que n'importe qui peut lui avoir envoyé, ou être le seul à avoir pu envoyer un message que chacun peut déchiffrer. On obtient alors un système de chif-

(2) Alan Turing est plus connu pour la machine qui porte son nom. C'est que ses travaux en cryptologie, effectués durant la Seconde Guerre mondiale, étaient entourés d'une extrême confidentialité.

(3) Le lecteur intéressé pourra consulter le livre *Sécurité dans les réseaux informatiques* de D. W. Davies et W. L. Price, livre qui a l'avantage d'être publié par l'AFNOR dans une traduction en français coordonnée par Marc Girault.

frement dit à *clés publiques*. Évidemment, Clé et Clé' ne peuvent pas être indépendants l'un de l'autre ; la fonction qui les uni doit donc être une fonction très difficilement inversible. Le système le plus connu est le RSA (4) qui repose sur l'extrême difficulté de décomposer un très grand nombre en facteurs premiers – on utilise aujourd'hui des nombres ayant jusqu'à 300 chiffres décimaux.

Aujourd'hui, la technologie, s'appuyant sur les progrès de la cryptologie, permet de réaliser des moyens de chiffrement adaptés à tous les problèmes de sécurité qui peuvent se poser, tant en nature (confidentialité, signature, disponibilité) qu'en force de résistance aux attaques. Des normes existent pour l'élaboration de ces produits et pour l'évaluation de leur sécurité. Des schémas de délivrance de *certificats de sécurité* ont été mis en place et fonctionnent dans différents pays, dont la France.

Sécurité et liberté sur Internet

Transposant ce qui précède aux problèmes de l'Internet, on pourrait donc estimer que les solutions existent et s'étonner qu'elles n'aient pas encore été mises en œuvre, ou du moins que la quasi-totalité des expériences soit américaine. C'est qu'il y a un mais, et un mais de taille. De tout temps, les États ont en effet vu d'un très mauvais œil que leurs citoyens puissent communiquer secrètement entre eux ; une communication chiffrée avec un pays étranger est même, pour beaucoup d'États, en soi un acte d'espionnage et réprimé en tant que tel. Il faut se garder de croire qu'il s'agit d'idées ou d'agissements périmés : de nos jours encore, espionnage et terrorisme sont florissants et font largement usage de la cryptologie.

Cependant, l'obstacle majeur n'est sans doute pas là : il est du côté de la justice. En effet, l'écoute des communications a toujours été, et est de plus en plus, un outil essentiel des enquêtes judiciaires. S'y ajoute maintenant l'interprétation des fichiers informatiques saisis lors de ces enquêtes. Si ces deux moyens d'information venaient à être coupés, police et justice devraient se limiter à d'autres moyens, plus traditionnels peut-être, mais plus risqués à la fois pour les enquêteurs et pour les cibles des enquêtes. Il est par ailleurs tout à fait certain qu'une large proportion des enquêtes qui trouvent aujourd'hui leur bon aboutissement devrait alors être classée sans solution.

On conçoit donc aisément que Défense, police et justice aient grand intérêt à ce que l'usage de la cryptologie soit contrôlé, et souhaitent maintenir un contrôle qui existe déjà, d'une façon ou d'une autre, dans la plupart des pays. Il est souvent informel, la seule possession d'un équipement de cryptologie pouvant même conduire à la prison dans certains pays. Heureusement, il résulte de dispositions législatives et réglementaires dans les grandes démocraties. Ces dispositions visent essentiellement les seuls moyens de cryptologie qui assurent la confidentialité de l'information. Aux États-Unis, le commerce et l'usage de ces moyens sont juridiquement libres. Par contre, seule est autorisée l'exportation des moyens qui offrent un niveau de protection inférieur à un certain seuil. Au sein de la Communauté européenne, un règlement communautaire soumet à autorisation préalable la circulation de ces moyens même entre les différents États membres.

En France, une loi de 1990 soumet à autorisation préalable du Premier ministre la fourniture, l'utilisation et l'exportation des moyens et prestations de cryptologie lorsqu'ils assurent la confidentialité de l'information ; ces autorisations sont éventuellement délivrées après examen d'un dossier technique expliquant de façon détaillée le fonctionnement du moyen en cause. Tout contraignante qu'elle soit, cette loi était déjà une libéralisation certaine, puisque, auparavant, la cryptologie était systématiquement considérée comme matériel de guerre. Elle a été modifiée en 1996 pour introduire la notion de Tiers de confiance sur laquelle nous reviendrons.

Besoin des citoyens de protéger leurs données personnelles, médicales par exemple, contre les indiscrets ; besoin des entreprises de protéger leurs données commerciales contre leurs concurrents ; besoin de la justice d'accéder à ces informations, même s'il s'agit de cas rares et prévus par la loi. Voilà l'équation fondamentale qu'il faut résoudre.

C'est une équation à la fois sociale, juridique et technique. Sociétale et juridique car elle sous-tend en fait un choix de société. Sur l'Internet lui-même, de nombreuses personnes revendiquent ainsi la "liberté de crypter", considérant que communiquer librement en toute confidentialité est l'un des droits fondamentaux de la personne auquel même la justice ne peut porter atteinte. Cette argumentation correspond tout à fait au choix sociétal américain et si l'on n'y prend pas garde, l'Internet va être un outil qui va progressivement l'imposer au détriment d'un choix plus conforme aux usages européens. Ce point mérite qu'on s'y attarde.

La loi américaine repose pour sa part sur quelques grandes idées fondamentales. Deux nous intéressent ici : la première est une liberté totale de l'individu qui conduit en matière de sécurité au principe *"défends-toi toi-même"*. Le poids du lobby des armes aux États-Unis est bien connu. Le traitement de la cryptologie procède de la même idée : cette technologie est donc d'usage libre à l'intérieur des frontières du pays, la police fédérale faisant "ce qu'elle peut" et devant accepter bon gré mal gré de ne pas pouvoir avoir accès à certaines informations. Le

(4) Du nom de ses auteurs, Rivest, Shamir et Adleman.

corollaire est d'ailleurs une forte suspicion des citoyens américains à l'égard d'au moins certains services de leur administration. La deuxième idée est encore plus simple : il y a les États-Unis d'une part, le reste du monde d'autre part, et ce qui se fait aux États-Unis est un modèle pour le reste du monde. C'est ainsi que la loi américaine est censée avoir le pas sur toutes les autres (5). C'est ainsi que seuls les citoyens américains peuvent se protéger efficacement. L'évidente conclusion est que l'Internet ne saurait exister que conforme à la loi et aux usages américains.

L'attitude européenne procède de traditions différentes ; elle est tout à fait à l'opposé dans ces deux cas. On considère de ce côté de l'Atlantique que le citoyen ne peut se défendre que dans des cas exceptionnels ; *c'est à l'État de protéger le citoyen* et l'État doit avoir les moyens de le faire. Par ailleurs, les relations entre États sont fondées sur une égalité totale, le droit de chaque pays s'appliquant seul sur son territoire.

Il faut enfin observer qu'au sein de l'Union européenne la situation est encore floue. La difficulté tient, comme nous venons de le voir, à ce qu'il faut arbitrer entre commerce et justice, c'est-à-dire entre des piliers différents du traité de Maastricht. Ceci entraîne d'inévitables conflits entre Commission et États, mais aussi entre les États eux-mêmes qui ont des conceptions différentes sur la façon de procéder à ces arbitrages, différences cachant souvent des approches incompatibles sur les modalités d'exercice de la justice. Ceci conduit à compliquer encore l'énoncé de l'équation fondamentale : chaque État doit pouvoir accéder à l'information, totalement indépendamment des autres, même lors d'une communication transfrontière.

Il ne faut cependant pas croire que l'Europe s'est contentée de doctes disputes sur le sujet. La plupart des pays de l'Union sont très conscients de la nécessité de trouver une solution au problème et, entraînés par les principaux d'entre eux, se sont attachés à étudier les aspects technique et juridique à notre équation, comme nous allons le voir. On peut même dire qu'un accord devrait être prochainement trouvé.

Un regard sur l'avenir ; les Tiers de confiance

La première tentative de solution a été américaine : c'était le *Clipper chip*, bien connu des experts du domaine. Le fonctionnement de ce composant repose sur la connaissance d'une clé, déposée dans un organisme d'État. Cette solution provoqua un tollé général, marque du peu de confiance de nos amis américains en un État dépositaire de toutes les clés de chiffrement.

Aujourd'hui, c'est la solution *Tiers de confiance* qui paraît la plus prometteuse : les clés de chiffrement sont élaborées par des organismes, publics ou privés, qui en sont en même temps les séquestres et les remettent aux organismes habilités, dans les conditions prévues par la loi de chaque pays ; il s'agit en quelque sorte de *cybernotaires* qui peuvent avoir parallèlement d'autres fonctions, par exemple la certification de clés ou l'enregistrement de messages, métiers qui existent déjà aux États-Unis. Cette solution est beaucoup plus facilement acceptée, ne serait-ce que parce que chacun pourra librement choisir son Tiers de confiance, métier du domaine concurrentiel. Des dispositions techniques sont prises pour que, dans le cas d'une communication internationale, chaque pays puisse accéder à l'information.

Cette solution est étudiée en Europe depuis plusieurs années, un préalable ayant été d'en vérifier la faisabilité technique. La Commission de Bruxelles vient de lancer un appel d'offres en vue de son expérimentation. Il semblerait par ailleurs qu'elle soit en passe d'être recommandée par l'OCDE. Le Japon, longtemps réticent, s'y est rallié en 1996. Les États-Unis paraissent également favorables à cette solution. Il faut cependant mentionner l'existence d'une solution concurrente, étudiée par des constructeurs informatiques, dite de *key recovery* : les clés sont systématiquement jointes aux messages, chiffrées grâce à une clé maître dont seul l'État dispose.

En France, les Tiers de confiance ont été introduits dans la réglementation de la cryptologie par un amendement à la loi voté en 1996. Le métier de Tiers de confiance est soumis à l'agrément du Premier ministre (service central de la sécurité des systèmes d'information) ; en contrepartie, l'utilisation de la cryptologie est totalement libre lorsque l'on a recours à cet intermédiaire pour élaborer les clés de chiffrement.

Il faudra encore du temps avant que les Tiers de confiance soient installés sur l'Internet. Ceci ne pourra se faire que si un bon équilibre est trouvé entre les diverses contraintes, l'équilibre financier étant sans doute un objectif majeur. En effet, trop d'incertitude à ce sujet conduira à limiter étroitement le nombre de Tiers de confiance et à jeter le doute sur cette profession, ce qui conduira à son rejet.

La seule autre solution serait alors une utilisation totalement libre de la cryptologie, solution qui n'est souhaitable pour personne, ni pour les États qui verraient leurs objectifs bafoués, ni même pour les utilisateurs, car une liberté totale conduirait inévitablement à l'existence de moyens de qualités très diverses et à l'impossibilité pour la plupart des utilisateurs de s'y retrouver dans une jungle où chacun à intérêt à tromper tout le monde. ■

(5) Les accords du GATT sont un bon exemple de ce principe, puisque seuls les États-Unis ne sont pas liés par ces accords.