Nations Unies A/CONF.187/L.10

Dixième Congrès des Nations Unies pour la prévention du crime et le traitement des délinquants

Vienne, 10-17 avril 2000

Distr.: Limitée
16 avril 2000

Français
Original: Anglais

Point 5 de l'ordre du jour
Prévention efficace de la criminalité: comment suivre le rythme des innovations

Rapport de la Commission II

Atelier sur les délits liés à l'utilisation du réseau informatique

Introduction

1. Organisé par l'Institut pour la prévention du crime et le traitement des délinquants en Asie et en Extrême-Orient, l'atelier sur les délits liés à l'utilisation du réseau informatique s'est tenu le 15 avril 2000. Il était saisi d'un document d'information sur la question (A/CONF.187/10).

2. Le Directeur de l'Institut, M. Mikinao Kitada, a fait une déclaration liminaire.

3. Dans un discours introductif, M^me^ Anne McLellan, Ministre de la justice et Procureur général du Canada, a souligné la gravité croissante des délits informatiques nationaux et transnationaux et la nécessité d'élaborer des lois et procédures efficaces pour y faire face sans compromettre les effets bénéfiques et légitimes des nouvelles technologies.

4. L'atelier a tenu une série de tables rondes. La première table ronde a passé en revue la criminologie des délits informatiques. La deuxième a examiné une étude de cas sur les questions techniques et juridiques découlant de la perquisition et de la saisie de données dans des réseaux informatiques. La troisième a porté sur une étude de cas concernant la localisation des communications informatiques dans les réseaux multinationaux. La quatrième et dernière a traité de la relation existant entre la répression, d'une part, et l'industrie des ordinateurs et l'Internet, d'autre part. Au cours des débats, les représentants de 9 gouvernements et 17 experts ont fait des déclarations.[*]

Débat général

5. Il a été signalé que le développement des nouvelles technologies avait offert de nouvelles possibilités aux délinquants. L'expression "délit lié à l'utilisation du réseau informatique" a été élargie afin d'englober, d'une part, les formes entièrement nouvelles de criminalité dirigées contre les ordinateurs, les réseaux et leurs utilisateurs et, d'autre part, les formes traditionnelles de criminalité actuellement perpétrées en utilisant le matériel informatique ou avec l'aide de matériel informatique. Les mesures prises sur le plan juridique pour lutter contre ces nouveaux délits ont été passées en revue. À cet égard, il a été souligné que, compte tenu de la facilité avec laquelle ces délits pouvaient être

[*]La liste des experts figure à l'annexe I du présent rapport.

commis à travers les frontières nationales, il importait d'élaborer dans chaque pays une législation pénale adéquate.

6. On a fait observer que le nouvel environnement créé par les réseaux informatiques remettait en question nombre des postulats traditionnels des systèmes juridiques. On a débattu de la nécessité de moderniser les lois afin de suivre le rythme des progrès technologiques. On a souligné que des concepts juridiques tels que ceux de propriété, de vol et de possession étaient tous couramment utilisés en droit pénal mais n'avaient pas forcément de sens lorsque l'on avait affaire à des données informatiques, par nature immatérielles. La facilité avec laquelle des données pouvaient être modifiées avait également créé de nouveaux problèmes juridiques liés à leur collecte, à leur conservation et à leur utilisation en tant qu'éléments de preuve lors de procédures pénales.

7. On a fait remarquer que les pouvoirs et les compétences techniques nécessaires pour mener des enquêtes efficaces sur les réseaux informatiques suscitaient également de vives préoccupations eu égard aux droits fondamentaux et à la vie privée des personnes, tant en raison de leur capacité de porter atteinte à la vie privée que du grand volume d'informations personnelles et autres stockées et transmises sur ces réseaux. Il a été admis qu'une des questions essentielles auxquelles les gouvernements étaient confrontés à présent et seraient confrontés à l'avenir était la nécessité de trouver le juste équilibre entre le droit des personnes au respect de leur vie privée et les intérêts de la justice. Des questions touchant à la vie privée pourraient surgir dans un certain nombre de situations. On a par ailleurs fait observer que, dans certains pays, la loi établissait une distinction entre rechercher et intercepter des données en cours de transmission d'une part, et rechercher des données stockées d'autre part, tandis que cette différence était parfois floue dans d'autres pays. On a fait remarquer que, dans le cas où des données étaient considérées comme étant en cours de transmission, et qu'elles étaient donc susceptibles d'être interceptées plutôt que saisies, il pourrait être nécessaire de prévoir des dispositions plus strictes concernant l'obtention des autorisations voulues et des garanties pour mener les recherches. À cet égard, on a estimé que les éléments de preuve recherchés par les services de répression risquaient de se trouver mêlés à d'autres données, telles que des informations professionnelles ou médicales sur la personne en cause ou sur un tiers.

8. On a fait observer que de nombreuses questions se posaient lorsque les services de répression cherchaient à obtenir des informations auprès de fournisseurs de services Internet, notamment une question pratique, à savoir comment trouver, parmi le personnel travaillant pour ce fournisseur, une personne à contacter en cas de besoin et une autre question d'ordre juridique, à savoir un fournisseur pouvait-il divulguer des informations volontairement ou non. On a souligné que dans certains pays les lois relatives à la protection de la vie privée ou à la protection des données interdisaient aux fournisseurs de services Internet de divulguer, en l'absence d'un décision de justice, certaines informations ou toutes les informations concernant les communications effectuées par leurs clients, et que la loi n'indiquait pas toujours très clairement si les fournisseurs devaient tenir un registre des transactions ou du contenu des messages qui pourrait par la suite être utilisé pour une enquête, en cas de besoin.

9. Un certain nombre de participants ont fait observer que, lorsque les éléments de preuve recherchés par les services de répression se trouvaient dans le système informatique d'une entreprise légitime, les recherches risquaient de porter préjudice à l'entreprise si elles perturbaient le fonctionnement du système informatique. Il a été admis que, dans ce cas, il fallait effectuer les recherches de façon efficace mais sans gêner le fonctionnement normal de l'entreprise.

10. On a estimé que la dimension transnationale d'un grand nombre de délits informatiques pourrait donner lieu à des problèmes encore plus complexes, en particulier du point de vue de la juridiction. Les questions relatives aux lois applicables, au pouvoir d'enquête en vue d'obtenir des éléments de preuve et de localiser ou identifier les délinquants, et au pouvoir d'extrader les délinquants puis de les traduire en justice dépendaient toutes, dans une plus ou moins grande mesure, du lieu où l'infraction avait été commise. Or, ce lieu était difficile à déterminer lorsque l'infraction avait été commise en plus d'un endroit, grâce à l'utilisation d'un réseau informatique. On a ainsi cité l'exemple d'un site Internet se trouvant dans un pays donné et sur lequel on trouvait des informations falsifiées concernant une entreprise dont les actions étaient cotées en bourse dans un autre pays; selon les lois des pays concernés, on pouvait considérer que l'infraction avait eu lieu dans l'un des pays, dans l'autre, dans les deux ou dans aucun d'entre eux.

11. On a fait observer que les opérations de perquisition et de saisie devenaient compliquées lorsque les enquêteurs étaient situés dans une juridiction et que les éléments de preuve se trouvaient dans une autre juridiction. Par exemple, une perquisition sur un réseau pouvait permettre de trouver des éléments de preuve stockés dans un autre pays, ce qui posait la question de savoir si la permission des autorités dans le deuxième pays était nécessaire pour obtenir ces éléments de preuve ou s'il fallait signaler auxdites autorités qu'une perquisition était en cours. On a noté que, lorsqu'il était nécessaire de demander une aide judiciaire par la voie officielle, l'obtention de cette aide pourrait prendre beaucoup de temps. Le point de savoir comment accélérer cette procédure pouvait être déterminant dans le cas d'un délit informatique en cours, ou lorsque les éléments de preuve risquaient d'être détruits pendant le temps nécessaire à l'obtention d'une aide judiciaire par la voie existante.

12. On a fait remarquer qu'un autre problème posé par la nature transnationale des délits informatiques et par la facilité avec laquelle des preuves électroniques pouvaient être modifiées était lié à la détermination de l'authenticité des éléments de preuve obtenus dans le cadre d'une perquisition transfrontière. Cette détermination pourrait exiger la mise en place de procédures ou de protocoles applicables aux perquisitions informatiques afin de s'assurer de l'authenticité des données recherchées, ainsi que de procédures transparentes et sûres permettant d'établir l'authenticité. On a fait observer que, dans certains pays, des conditions de forme officielles pourraient entraver l'utilisation comme éléments de preuve de données électroniques.

13. De l'avis général, les États devraient s'employer à harmoniser, le cas échéant, les dispositions pertinentes relatives à la criminalisation, aux preuves et aux procédures.

Conclusion

14. L'atelier est parvenu aux conclusions suivantes:

a) Les délits informatiques devraient être criminalisés;

b) Des règles de procédure appropriées étaient nécessaires dans le cadre des enquêtes et des poursuites visant les cyberdélinquants;

c) Les gouvernements et le secteur industriel devraient œuvrer conjointement en vue de la réalisation d'un objectif commun: prévenir et combattre les délits informatiques de manière à garantir la sûreté de l'Internet;

d) Le renforcement de la coopération internationale est nécessaire pour retrouver les délinquants sur l'Internet;

e) L'Organisation des Nations Unies devrait prendre d'autres mesures en vue de fournir une coopération et une assistance techniques face aux délits liés à l'utilisation des réseaux informatiques.

Annexe I

Experts ayant participé aux tables rondes

M. Shri L. C. Amarnathan, Sikkim Police Headquarters, Inde

M. Cormac Callanan, European Internet Service Provider Association, Irlande

M. Peter N. Grabosky, Institute of Criminology, Australie

M. Masahito Inoue, Université de Tokyo, Japon

M. Nigel Jones, Association of Chief Police Officers, Royaume-Uni de Grande-Bretagne et d'Irlande du Nord

M. Ekkehart Kappler, Office fédéral de lutte contre la criminalité, Allemagne

M. Henrik W. K. Kaspersen, Professeur, Vrije Universiteit Amsterdam, Pays-Bas

M^me^ Margo L. Langford, Barrister and Solicitor, Canada

M. Victor Lo, Services de police de Hong Kong, Chine

M. Keith Mitchell, London Internet Exchange, Royaume-Uni de Grande-Bretagne et d'Irlande du Nord

M. Hans G. Nilsson, Conseil de l'Union européenne

M. Donald K. Piragoff, Ministère de la justice, Canada

M^me^ Mary Riley, United States Secret Service, États-Unis d'Amérique

M. Gregory P. Schaffer, Computer Security Consultant, États-Unis d'Amérique

M. Ulrich Sieber, Université de Munich, Allemagne

M. Vittorio Stanca, Service national pour les délits informatiques, Italie

M. Michael Sussmann, Department of Justice, États-Unis d'Amérique