Projet sur la cybercriminalité
www.coe.int/cybercrime

Division du crime économique
Direction générale des
droits de l'Homme et des affaires juridiques
Strasbourg, France
2 avril 2008

Lignes directrices pour la coopération entre organes de répression et fournisseurs de services internet contre la cybercriminalité

Ces lignes directrices sont le résultat de plusieurs débats entre les représentants du secteur et les organes de répression (forces de l'ordre), qui se sont rencontrés entre octobre 2007 et février 2008 sous les auspices du projet sur la cybercriminalité du Conseil de l'Europe. Il est complété par une étude détaillée.

Ce projet a fait l'objet de discussions complémentaires et a été adopté pendant la Conférence « Coopération contre la cybercriminalité (Conseil de l'Europe, Strasbourg, France) des 1er-2 avril 2008.

Il s'agit d'un outil non contraignant sur le plan juridique. Il pourra être diffusé et exploité pour aider les forces de l'ordre et les fournisseurs de services de tous les pays du monde à organiser leur coopération contre la cybercriminalité en respectant leurs rôles et responsabilités respectifs, ainsi que les droits des utilisateurs de l'internet.

Ce texte sera également soumis à l'examen du Comité de la Convention sur la cybercriminalité (T-CY) du Conseil de l'Europe.

Lignes directrices pour la coopération entre organes de répression et fournisseurs de services internet contre la cybercriminalité[1]

Introduction

1. La construction de la société de l'information fait appel au renforcement de la confiance envers les technologies de l'information et de la communication (TIC), à la protection des données à caractère personnel et à la confidentialité, ainsi qu'à la promotion d'une culture globale de cyber-sécurité dans un contexte mondial au sein duquel les sociétés deviennent de plus en plus dépendantes des TIC et donc, vulnérables à la cybercriminalité.

2. Les première et deuxième phases du Sommet mondial sur la société de l'information (Genève 2003 – Tunis 2005) ont pris l'engagement – entre autres – de construire une société de l'information inclusive au sein de laquelle chacun pourra créer, obtenir, utiliser et partager l'information et le savoir, mettre en œuvre ses potentialités et améliorer sa qualité de vie conformément aux buts et aux principes de la Charte des Nations Unies, et en respectant pleinement et mettant en œuvre la Déclaration universelle des Droits de l'Homme. Cette société de l'information fait appel à de nouvelles formes de partenariat et de coopération entre les États, le secteur privé, la société civile et les organisations internationales.

3. Les fournisseurs de services internet (FSI) et les organes de répression, ou forces de l'ordre, jouent un rôle crucial dans la réalisation de cette vision.

4. Des lois nationales conformes à la Convention sur la cybercriminalité du Conseil de l'Europe (Convention de Budapest) permettront aux États de créer une base juridique cohérente pour la coopération entre les secteurs public et privé, pour l'exercice des pouvoirs d'investigation ainsi que pour la coopération internationale.

5. Ces lignes directrices n'ont pas pour objectif de se substituer aux instruments juridiques existants ; elles présupposent que ceux-ci sont à même de fournir un système d'instruments d'investigation bien équilibrés ainsi que les clauses de sauvegarde et la protection des droits fondamentaux de l'être humain tels que la liberté d'expression, le droit au respect de la vie, du foyer et de la correspondance privés et le droit à la protection des données. Par conséquent, nous recommandons que les États adoptent ces dispositions dans leurs lois nationales afin de mettre en œuvre les dispositions de procédure de la Convention sur la cybercriminalité et de définir les obligations des autorités d'investigation et des forces de l'ordre tout en mettant en place les conditions et les sauvegardes prévues à l'article 15 de la Convention. Cela aura pour effet :

- d'assurer l'efficacité des activités des forces de l'ordre ;
- de protéger l'aptitude des fournisseurs de services internet à fournir des services ;
- de faire en sorte que les lois nationales soient conformes aux normes mondiales ;
- de promouvoir les normes mondiales au lieu de solutions nationales isolées ;
- de contribuer au bon fonctionnement du droit et notamment à l'application des principes de légalité, de proportionnalité et de nécessité.

[1] Ce document ne reflète pas nécessairement les positions officielles du Conseil de l'Europe. Pour de plus amples informations, contacter Alexander.seger@coe.int

6. Ces lignes directrices utilisent la définition du « fournisseur de services » de la Convention sur la cybercriminalité dans son article 1, qui en donne une acception large :

i toute entité publique ou privée offrant aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique, et

ii toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs.

7. Afin d'optimiser la cybersécurité, réduire l'utilisation des services à des fins illicites et renforcer la confiance envers les TIC, il est fondamental que les fournisseurs de services internet et les forces de l'ordre coopèrent efficacement avec toute la considération due à leurs rôles respectifs, aux coûts de cette coopération et aux droits des citoyens.

8. L'objectif de ces lignes directrices est d'aider les forces de l'ordre et les fournisseurs de services internet à structurer leurs interactions en lien avec les questions de cybercriminalité. Elles reposent sur des bonnes pratiques existantes et devraient être applicables dans tous les pays du monde en accord avec les lois nationales et dans le respect de la liberté d'expression, du droit au respect de la vie privée, à la protection des données personnelles et des autres droits fondamentaux des citoyens.

9. Par conséquent, nous recommandons aux États, aux forces de l'ordre et aux fournisseurs de services internet de prendre les mesures suivantes au niveau national :

Lignes directrices communes

10. Il conviendrait d'encourager les forces de l'ordre et les fournisseurs de services internet à s'engager dans des échanges d'information visant à renforcer leur capacité à identifier et combattre les types de cybercriminalité émergents. Les forces de l'ordre devraient tenir les fournisseurs de services informés sur les tendances de la cybercriminalité.

11. Les forces de l'ordre et les fournisseurs de services internet devraient développer une culture de la coopération – plutôt que de la confrontation – incluant le partage de bonnes pratiques. Il conviendrait d'encourager la tenue de réunions régulières en vue de l'échange des expériences et de la résolution des problèmes.

12. Les forces de l'ordre et les fournisseurs de services devraient développer conjointement des procédures de coopération écrites. Lorsque c'est possible, les deux parties devraient être invitées à se transmettre des retours d'information structurés sur le fonctionnement de ces procédures.

13. Il conviendrait d'envisager des partenariats formels entre les forces de l'ordre et les fournisseurs de services afin d'établir des relations à long terme avec les garanties réciproques appropriées, de façon à ce que le partenariat n'enfreigne pas les droits des acteurs du secteur ou qu'il n'interfère pas avec les pouvoirs d'application de la loi du côté des forces de l'ordre.

14. Tant les forces de l'ordre que les fournisseurs de services internet devraient protéger les droits fondamentaux des citoyens conformément aux normes des Nations Unies et aux autres normes européennes et internationales applicables, telles que la Convention des Droits de l'Homme et des Libertés fondamentales du Conseil

de l'Europe, le Pacte international de 1966 des Nations Unies, relatif aux droits civils et politiques, la Convention de 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, ainsi que les lois nationales. Cela place des limites raisonnables au niveau de coopération envisageable.

15. Il conviendrait d'encourager les forces de l'ordre et les fournisseurs de services internet à coopérer en vue de faire appliquer les normes de respect de la vie privée et de la protection des données au niveau national, mais également par rapport aux flux de données transfrontaliers. Les travaux du Conseil de l'Europe et de l'OCDE apportent des lignes de conduite à cet égard.

16. Les deux parties devraient être conscientes des coûts afférents à la génération de requêtes et aux réponses à apporter. Il conviendrait de développer des procédures tenant compte de l'impact financier de ces activités, ainsi que des questions de remboursement des coûts ou de juste compensation pour les parties concernées.

Mesures à prendre par les forces de l'ordre

17. Une coopération élargie et stratégique – encourager les forces de l'ordre à apporter leur assistance aux fournisseurs de services dans le cadre d'une coopération élargie et stratégique avec le secteur privé, ce qui impliquerait de conduire régulièrement des séminaires de formation juridique, ainsi que de faire remonter les informations collectées à l'occasion des plaintes enregistrées ou des renseignements obtenus par les fournisseurs de services sur des activités criminelles connues.

18. Procédures pour les requêtes pénales – encourager les forces de l'ordre à élaborer des procédures écrites, incluant les mesures appropriées d'application, pour l'émission et le traitement des requêtes pénales, et pour s'assurer que ces requêtes soient prises en charge dans le respect des procédures agréées.

19. Formation – encourager les forces de l'ordre à proposer des formations à une équipe désignée au sein de leur personnel sur la manière de mettre ces procédures en œuvre, y compris sur la manière d'obtenir les enregistrements auprès des fournisseurs de services et de traiter les informations reçues, mais également sur les technologies internet et leur impact en général ainsi que sur la manière de respecter les principes du droit et les droits fondamentaux des individus.

20. Ressources techniques – les personnels des forces de l'ordre responsables de la coopération avec les fournisseurs de services devraient s'équiper des ressources techniques nécessaires, et notamment d'un accès à internet, d'une adresse de messagerie qui mette en évidence l'identité du service, et d'autres ressources techniques leur permettant de recevoir, de la part des fournisseurs de services, des informations en toute sécurité par voie électronique.

21. Personnel et points de contact désignés – les interactions entre les forces de l'ordre et les fournisseurs de services devraient se limiter aux personnels dûment formés. Il conviendrait d'encourager les forces de l'ordre à désigner des points de contact pour la coopération avec les fournisseurs de services.

22. Autorité pour les requêtes – encourager les forces de l'ordre à définir clairement dans leurs procédures écrites quel personnel interne peut autoriser quel type de mesure et de requête auprès des fournisseurs de services internet et comment ces requêtes peuvent être validées/autorisées par ces derniers.

23. Encourager les forces de l'ordre à mettre à la disposition des fournisseurs de services internet des informations relatives à leurs procédures et, chaque fois que c'est possible, à indiquer quel personnel ou quel poste de travail désigné est responsable de la coopération avec les fournisseurs de services internet.

24. Vérification de la source de la requête – la source d'une requête émanant des forces de l'ordre doit être vérifiable par les fournisseurs de services :

- toute correspondance devrait inclure un nom de contact, un numéro de téléphone et une adresse de messagerie correspondant à celle de l'agent des forces de l'ordre sollicitant les enregistrements, de façon à ce que le fournisseur de services puisse contacter la personne à l'origine de la requête le cas échéant ;
- les fournisseurs de services ne devraient pas se voir demander de correspondre avec un agent au travers de son adresse de messagerie personnelle, mais plutôt par un compte de messagerie approprié, mis en place par le service ;

- toute correspondance devrait porter l'en-tête du service concerné et le numéro du central téléphonique principal du service, ainsi que son adresse web, de façon à ce que les fournisseurs de services puissent prendre les mesures nécessaires pour vérifier l'authenticité des requêtes s'ils estiment devoir le faire.

25. Requêtes – les requêtes des forces de l'ordre aux fournisseurs de services devraient être faites par écrit (ou par tout autre méthode électronique juridiquement acceptable) et être dûment consignées à des fins de traçabilité. Dans les cas d'extrême urgence, ou lorsque les requêtes orales sont acceptables, elles doivent être immédiatement suivies d'une confirmation écrite (ou autre méthode électronique juridiquement acceptable).

26. Format de requête standard – au niveau national, et international si c'est possible, il conviendrait d'encourager les forces de l'ordre à standardiser et à structurer le format employé pour envoyer des requêtes et y répondre. Au minimum, les requêtes devraient contenir les informations suivantes :

- un numéro d'enregistrement
- la référence aux textes juridiques de base
- les données spécifiques sollicitées
- les informations permettant de vérifier la source de la requête

27. Spécificité et précision des requêtes – encourager les forces de l'ordre : à s'assurer que les requêtes envoyées sont spécifiques, complètes et claires, et qu'elles sont suffisamment détaillées pour permettre aux fournisseurs de services d'identifier les données pertinentes ; à faire en sorte que les requêtes sont envoyées au fournisseur de services qui possède les enregistrements ; à éviter les requêtes concernant des données multiples et non spécifiées.

28. Encourager les forces de l'ordre à fournir autant de faits que possible quant aux investigations, sans mettre en danger l'enquête conduite ni des droits fondamentaux, afin de permettre aux fournisseurs de services d'identifier les données pertinentes.

29. Encourager les forces de l'ordre à fournir des explications et de l'assistance aux fournisseurs de services en matière de techniques d'investigation générales afin qu'ils puissent mieux comprendre comment leur coopération pourra déboucher sur des investigations plus efficaces pour lutter contre le crime et assurer une meilleure protection des citoyens.

30. Définition des priorités – encourager les forces de l'ordre à définir des priorités dans leurs requêtes, notamment pour celles concernant les gros volumes de données, afin de permettre aux fournisseurs de services de traiter d'abord les plus importantes. La définition des priorités sera meilleure si elle est cohérente sur l'ensemble des forces de l'ordre au niveau national et si possible, au niveau international.

31. Justification des requêtes – encourager les forces de l'ordre à être conscientes des coûts que les requêtes impliquent pour les fournisseurs de services et d'accorder à ces derniers des délais de réponse suffisants. Les forces de l'ordre devraient être conscientes du fait que les fournisseurs de services pourront avoir à répondre à des requêtes provenant d'autres autorités publiques ; elles devraient être encouragées à surveiller les volumes sollicités.

32. Confidentialité des données – Il conviendrait que les forces de l'ordre assurent la confidentialité des données réceptionnées.

33. Éviter les coûts inutiles et de perturber le bon déroulement des activités – encourager les forces de l'ordre à éviter de susciter des coûts inutiles et de perturber le bon fonctionnement des activités des fournisseurs de services et autres.

34. Encourager les forces de l'ordre à limiter le recours aux points de contact d'urgence aux cas extrêmement urgents de façon à éviter un recours abusif à ce service.

35. Encourager les forces de l'ordre à faire en sorte que les mesures conservatoires et autres mesures provisoires soient suivies, dans les temps, de mesures de divulgation, ou que le fournisseur de services internet soit informé à temps du fait que les données conservées ne sont plus requises.

36. Requêtes internationales – encourager les forces de l'ordre nationales à ne pas adresser de requêtes directes aux fournisseurs de services internet non nationaux, mais de faire appel aux procédures décrites dans les traités internationaux, comme la Convention sur la cybercriminalité et le réseau 24/7 des points de contact d'application de la loi pour les mesures urgentes, et ce notamment pour les mesures conservatoires.

37. Requêtes d'assistance juridique mutuelle internationale – encourager les forces de l'ordre et l'administration de la justice à prendre les mesures nécessaires pour que les requêtes de mesures conservatoires soient suivies de procédures internationales en vue d'une assistance juridique mutuelle, ou d'informer le fournisseur de services internet à temps de la caducité des mesures de conservation des données.

38. Coordination entre forces de l'ordre – encourager les forces de l'ordre à coordonner leur coopération avec les fournisseurs de services internet et à échanger leurs bonnes pratiques au niveau national et international. Au niveau international, elles devraient faire appel aux organes représentatifs internationaux chargés de ces aspects.

39. Programmes de conformité juridique – encourager les forces de l'ordre à organiser les interactions susmentionnées avec les fournisseurs de services sous forme de programme de conformité juridique et à fournir une description de ce programme aux fournisseurs de services, avec les éléments suivants :

- les informations nécessaires pour contacter le personnel des forces de l'ordre désigné pour prendre en charge le programme de conformité juridique, ainsi que les horaires auxquels ce personnel peut être contacté ;
- les informations nécessaires pour que le fournisseur de services soit en mesure de fournir des documents aux responsables du programme de conformité juridique ;
- les autres informations spécifiquement destinées aux responsables de ce programme (comme par exemple, les modalités de coopération internationale d'un organe de répression, les documents à traduire dans des langues données, etc.).

40. Audit du système de conformité – encourager les forces de l'ordre à suivre et à auditer le système de traitement des requêtes à des fins statistiques, de manière à

identifier les forces et les faiblesses du système et à en publier, le cas échéant, les conclusions.

Mesures à prendre par les fournisseurs de services

41. Coopération visant à réduire l'utilisation des services à des fins illicites – dans le respect des droits et des libertés, tels que la liberté d'expression, le respect de la vie privée et des autres lois nationales et internationales, ainsi que dans le respect des accords d'utilisation, il conviendrait d'encourager les fournisseurs de services à coopérer avec les forces de l'ordre afin de contribuer à la réduction de l'utilisation des services pour des activités criminelles telles que les définit le droit.

42. Encourager les fournisseurs de services à rendre compte aux forces de l'ordre des incidents illicites qui l'affectent et dont ils ont connaissance, sans que cela les oblige à rechercher activement les faits ou les circonstances indiquant l'existence d'activités illicites.

43. Encourager les fournisseurs de services à assister les forces de l'ordre en matière de formation et d'autres types de soutien portant sur leurs services et leur fonctionnement.

44. Suivi des requêtes émanant des forces de l'ordre – encourager les fournisseurs de services à réaliser tous les efforts raisonnables pour assister les forces de l'ordre dans l'exécution de leurs requêtes.

45. Procédures de réponse aux requêtes - encourager les fournisseurs de services à élaborer des procédures écrites, incluant les mesures appropriées d'application, pour le traitement des requêtes, et à faire en sorte que les requêtes font l'objet d'un suivi dans le respect des procédures agréées.

46. Formation – encourager les fournisseurs de services à s'assurer qu'ils ont apporté la formation appropriée à leur personnel responsable de la mise en œuvre de ces procédures.

47. Personnel et points de contact désignés – encourager les fournisseurs de services à désigner un personnel dûment formé pour faire office de point de contact pour la coopération avec les forces de l'ordre.

48. Assistance d'urgence – encourager les fournisseurs de services à mettre en œuvre les moyens permettant aux forces de l'ordre de contacter le personnel en charge de la conformité juridique en dehors des heures normales de travail, afin de répondre aux situations d'urgence ; encourager les fournisseurs de services à fournir aux forces de l'ordre les informations pertinentes en vue de l'assistance d'urgence.

49. Ressources – encourager les fournisseurs de services à fournir des points de contact ou du personnel responsable de la coopération avec les forces de l'ordre, dotés des ressources nécessaires pour répondre aux requêtes des forces de l'ordre.

50. Programmes de conformité juridique – encourager les fournisseurs de services à organiser leur coopération avec les forces de l'ordre sous forme de programmes généraux de conformité juridique, et à fournir une description de ces programmes aux forces de l'ordre, avec les éléments suivants :

- les informations permettant aux forces de l'ordre de contacter les responsables du programme de conformité juridique, ainsi que les horaires auxquels ils peuvent être contactés ;
- les informations permettant aux forces de l'ordre de fournir des documents aux responsables du programme de conformité juridique ;
- les autres informations spécifiquement destinées aux responsables du programme (par exemple, comment un fournisseur de services conduit ses activités dans plusieurs pays, les documents à traduire dans des langues données, etc.) ;
- afin que les forces de l'ordre puissent leur adresser des requêtes spécifiques et appropriées, encourager les fournisseurs de services à fournir des informations sur le type de service proposé aux utilisateurs, et notamment les liens vers les services et les informations complémentaires, ainsi que les détails de contact pour de plus amples informations ;
- encourager les fournisseurs de services internet à fournir la liste, lorsque c'est possible et sur demande des forces de l'ordre, des types de données pouvant être mis à disposition pour chaque service à la réception d'une requête de divulgation valide émanant des forces de l'ordre et acceptant que l'ensemble des données ne soit pas disponible pour toutes les enquêtes criminelles.

51. Vérification de la source des requêtes – encourager les fournisseurs de services à prendre les mesures nécessaires, dans la mesure du possible, pour vérifier l'authenticité des requêtes reçues des forces de l'ordre et lorsque c'est nécessaire, faire en sorte que les enregistrements de données relatives aux clients ne soient pas divulguées à des personnes non autorisées.

52. Réponse – encourager les fournisseurs de services à répondre sous forme écrite (ou tout autre moyen électronique juridiquement acceptable) aux requêtes émanant des forces de l'ordre, à faire en sorte que les requêtes et les réponses soient dûment archivées, et tout en acceptant que ce traçage ne contienne aucune donnée personnelle.

53. Format de requête standard – encourager les fournisseurs de services à standardiser le format d'envoi d'informations aux forces de l'ordre, en tenant compte du format des requêtes employé par les forces de l'ordre.

54. Encourager les fournisseurs de services à traiter les requêtes dans un délai raisonnable, conformément aux procédures écrites définies par leurs soins, et de tenir les forces de l'ordre informées des délais moyens de réponse aux requêtes.

55. Validation des informations envoyées – encourager les fournisseurs de services à ce que les informations transmises aux forces de l'ordre soient complètes, précises et protégées.

56. Confidentialité des requêtes – il conviendrait que les fournisseurs de services assurent la confidentialité des requêtes reçues.

57. Explications pour les informations non fournies – encourager les fournisseurs de services à fournir aux forces de l'ordre émettrices d'une requête des explications dans les cas de rejet ou d'impossibilité de fournir des informations.

58. Audit du système de conformité – encourager les fournisseurs de services à suivre et à auditer le système de traitement des requêtes à des fins statistiques, de

manière à identifier les forces et les faiblesses du système et d'en publier, le cas échéant, les conclusions.

59. Coordination entre fournisseurs de services – tout en gardant à l'esprit les lois antitrust et de la concurrence, il conviendrait d'encourager les fournisseurs de services à coordonner leur coopération avec les forces de l'ordre et à partager entre eux les bonnes pratiques, en faisant appel dans ce but, aux associations professionnelles de fournisseurs de services.