Proyecto sobre la ciberdelincuencia
www.coe.int/cybercrime

División de Delitos Económicos
Dirección General de Derechos Humanos
y Asuntos Jurídicos
Estrasburgo (Francia)
2 de abril de 2008

Directrices para la cooperación entre las autoridades responsables de velar por el cumplimiento de la ley y los proveedores de servicios de Internet en la lucha contra la ciberdelincuencia

Adoptadas por la Conferencia Mundial de Cooperación en la Lucha contra la Ciberdelincuencia
Consejo de Europa, Estrasburgo, 1-2 de abril de 2008

Estas directrices son el resultado de diversos debates celebrados entre los representantes del sector y las autoridades responsables de velar por el cumplimiento de la ley (las fuerzas del orden), que se reunieron entre octubre de 2007 y febrero de 2008 bajo los auspicios del Proyecto sobre la ciberdelincuencia del Consejo de Europa. Están complementadas por un estudio detallado.

Las directrices fueron examinadas con mayor detenimiento y adoptadas por la Conferencia Mundial "Cooperación en la lucha contra la ciberdelincuencia" (Consejo de Europa, Estrasburgo (Francia)), el 1-2 de abril de 2008.

Las directrices son un instrumento no vinculante que puede difundirse y utilizarse en la actualidad para ayudar a las fuerzas del orden y a los proveedores de servicios de todos los países del mundo a organizar su cooperación en la lucha contra la ciberdelincuencia, respetando al mismo tiempo sus respectivos papeles y responsabilidades, así como los derechos de los usuarios de Internet.

Directrices para la cooperación entre las autoridades responsables de velar por el cumplimiento de la ley y los proveedores de servicios de Internet en la lucha contra la ciberlincuencia[1]

Introducción

1. La construcción de una sociedad de la información exige el fortalecimiento de la confianza en las tecnologías de la información y las comunicaciones (TIC), la protección de los datos personales y la confidencialidad, y la promoción de una cultura global de ciberseguridad en un contexto en el que las sociedades de todo el mundo dependen cada vez más de las TIC, por lo que son más vulnerables a la ciberdelincuencia.

2. La primera y segunda fases de la Cumbre Mundial sobre la Sociedad de la Información (Ginebra, 2003, y Túnez, 2005) –entre otras cosas- se comprometieron a construir una sociedad de la información inclusiva, en la que todas las personas puedan crear, obtener, utilizar y compartir información y conocimientos, explotar su potencial y mejorar su calidad de vida, de conformidad con los objetivos y principios de la Carta de las Naciones Unidas, y respetando plenamente y defendiendo la Declaración Universal de Derechos Humanos. Esta sociedad de la información exige nuevas formas de alianzas y cooperación entre los gobiernos, el sector privado, la sociedad civil y las organizaciones internacionales.

3. Los proveedores de servicios de Internet y las autoridades responsables de velar por el cumplimiento de la ley desempeñan un papel fundamental a la hora de hacer realidad esta visión.

4. La conformidad de la legislación nacional con el Convenio sobre la ciberdelincuencia (el "Convenio de Budapest") ayuda a los países a establecer una sólida base legal para la cooperación público-privada, el ejercicio de los poderes de investigación y la cooperación internacional.

5. Estas directrices no pretenden sustituir ningún instrumento jurídico existente, sino que presuponen la existencia de unos instrumentos jurídicos adecuados que proporcionan un sistema equilibrado de instrumentos de investigación, así como salvaguardias conexas y una protección de derechos humanos fundamentales como la libertad de expresión, el respeto de la vida privada, del hogar y de la correspondencia, y el derecho a la protección de los datos. Por lo tanto, se recomienda que los Estados adopten disposiciones en su legislación nacional con miras a aplicar plenamente las disposiciones de procedimiento del Convenio sobre la ciberdelincuencia, y a definir las obligaciones de las autoridades de investigación y de las fuerzas del orden, estableciendo al mismo tiempo las condiciones y salvaguardias previstas en el artículo 15 del Convenio. De este modo,

- se asegurará la labor eficiente de las fuerzas del orden;
- se protegerá la capacidad de los proveedores de servicios de Internet para prestar servicios;
- se asegurará que la legislación nacional está en consonancia con las normas mundiales;
- se promoverán las normas mundiales, en lugar de soluciones nacionales aisladas, y
- se ayudará a asegurar el debido procedimiento legal y el Estado de derecho, incluidos los principios de legalidad, proporcionalidad y necesidad.

[1] El presente documento no refleja necesariamente las posiciones oficiales del Consejo de Europa. Para más información, diríjase a Alexander.seger@coe.int .

6. A los efectos de estas directrices, utilizamos la definición de proveedor de servicios contenida en artículo 1 del Convenio sobre la ciberdelincuencia, en el que se define el término "proveedor de servicios" de un modo general, como:

i toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático, y

ii cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios del mismo;

7. Con objeto de aumentar la ciberseguridad, reducir al mínimo la utilización de los servicios con fines ilegales y fortalecer la confianza en las TIC, es esencial que los proveedores de servicios de Internet y las fuerzas del orden cooperen entre sí de un modo eficiente, tomando debidamente en consideración sus respectivos papeles, el coste de dicha cooperación y los derechos de los ciudadanos.

8. El objetivo de las presentes directrices es ayudar a las fuerzas del orden y a los proveedores de servicios de Internet a estructurar sus interacciones en lo tocante a cuestiones relativas a la ciberdelincuencia. Éstas se basan en buenas prácticas existentes y deberían ser aplicables en cualquier país del mundo de conformidad con la legislación nacional y el respeto de la libertad de expresión, la confidencialidad, la protección de los datos personales y otros derechos fundamentales de los ciudadanos.

9. Por lo tanto, se recomienda que los Estados, las fuerzas del orden y los proveedores de servicios de Internet adopten las siguientes medidas a nivel nacional:

Directrices comunes

10. Debería alentarse a las autoridades responsables de velar por el cumplimiento de la ley y a los proveedores de servicios de Internet a participar en el intercambio de información con miras a desarrollar su capacidad para identificar y combatir nuevos tipos de ciberdelincuencia. Debería invitarse a las fuerzas del orden a informar a los proveedores de servicios de Internet sobre las tendencias de la ciberdelincuencia.

11. Las fuerzas del orden y los proveedores de servicios de Internet deberían promover una cultura de cooperación –en lugar de una cultura de confrontación–, incluido el intercambio de buenas prácticas. Se les alienta a organizar reuniones periódicas orientadas al intercambio de experiencias y la resolución de problemas.

12. Se debería alentar a las autoridades responsables de velar por la observancia de la ley y a los proveedores de servicios a establecer procedimientos por escrito para la cooperación mutua. Cuando sea posible, se debería invitar a ambas partes a intercambiar información estructurada sobre el funcionamiento de estos procedimientos.

13. Se debería contemplar la posibilidad de crear alianzas entre las fuerzas del orden y los proveedores de servicios, con miras a establecer unas relaciones a más largo plazo con garantías apropiadas para ambas partes de que la alianza no infringirá ningún derecho legal de los actores de la industria ni interferirá en los poderes legales de las fuerzas del orden.

14. Tanto las autoridades responsables de velar por el cumplimiento de la ley como los proveedores de servicios de Internet deberían proteger los derechos fundamentales de los ciudadanos de conformidad con las normas de las Naciones Unidas y otras normas europeas e internacionales aplicables, como el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, de 1950, del Consejo de Europa, el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas, de 1966, y el Convenio para la Protección de las Personas con respecto al tratamiento automatizado de datos de

carácter personal, de 1981, del Consejo de Europa, así como la legislación nacional. Esto impone unos límites razonables al nivel de cooperación posible.

15. Se invita a las fuerzas del orden y los proveedores de servicios de Internet a cooperar entre sí con miras a reforzar las normas sobre la protección de la confidencialidad y los datos, pero también en lo que respecta a los flujos de datos transfronterizos. La labor del Consejo de Europa y de la OCDE proporciona orientación en este sentido.

16. Ambas partes deberían ser conscientes de los costes que conlleva generar solicitudes y responder a las mismas. Los procedimientos deberían establecerse teniendo en cuenta los efectos financieros de estas actividades, así como las cuestiones de reembolso de los costes o de indemnización justa a las partes pertinentes.

Medidas que deben adoptar las fuerzas del orden

17. Una cooperación amplia y estratégica – Se debería alentar a las fuerzas del orden a prestar asistencia a los proveedores de servicios, en el marco de una cooperación amplia y estratégica con el sector, que incluiría organizar de manera periódica seminarios de formación técnica y jurídica, y a proporcionar información acerca de las investigaciones llevadas a cabo sobre la base de las quejas presentadas por los proveedores de servicios o de la información recopilada a raíz de la actividad delictiva conocida notificada por los proveedores de servicios.

18. Procedimientos para las solicitudes legalmente vinculantes – Se debería invitar a las fuerzas del orden a establecer procedimientos por escrito, que incluyan medidas apropiadas de diligencia debida, para la emisión y tramitación de las solicitudes legalmente vinculantes, y a asegurar que las solicitudes se gestionan de conformidad con los procedimientos acordados.

19. Formación – Se debería alentar a las fuerzas del orden a impartir formación a un equipo seleccionado de miembros de su personal sobre cómo poner en práctica estos procedimientos, incluido el modo en que pueden obtenerse registros de los proveedores de servicios y el modo de procesar la información recibida, pero también sobre las tecnologías de Internet y sus efectos en general y sobre cómo respetar el debido procedimiento legal y los derechos fundamentales de las personas.

20. Recursos técnicos – Los agentes de las fuerzas del orden responsables de cooperar con los proveedores de servicios deberían equiparse de los recursos técnicos necesarios, incluido el acceso a Internet, una dirección de correo electrónico creada por el organismo de que se trate, y otros recursos técnicos que les permitan recibir información de un proveedor de servicios por vía electrónica y en condiciones de seguridad.

21. Personal y puntos de contacto seleccionados – La interacción entre las fuerzas del orden y los proveedores de servicios de Internet debería limitarse al personal debidamente cualificado. Debería alentarse a las autoridades responsables del cumplimiento de la ley a designar a puntos de contacto para su cooperación con los proveedores de servicios.

22. Autoridad para las solicitudes – Se debería alentar a las autoridades responsables de velar por el cumplimiento de la ley a definir claramente en sus procedimientos por escrito qué miembros de las fuerzas del orden pueden autorizar qué tipo de medidas y solicitudes a los proveedores de servicios de Internet, y cómo estas solicitudes pueden ser validadas/autenticadas por los proveedores de servicios de Internet.

23. Se debería invitar a las fuerzas del orden a proporcionar información a los proveedores de servicios de Internet sobre sus procedimientos y, en la medida de lo posible, sobre qué miembros del personal o qué cargos designados son responsables de la cooperación con los proveedores de servicios de Internet.

24. Verificación de la fuente de la solicitud – Los proveedores de servicios de Internet deberían poder verificar la fuente de una solicitud proveniente de las fuerzas del orden:

- toda correspondencia debería incluir el nombre de contacto, el número de teléfono y la dirección de correo electrónico del agente de las fuerzas del orden que solicite los registros, para que el proveedor de servicios pueda ponerse en contacto con el solicitante en su caso;
- no debería pedirse a los proveedores de servicios que mantengan correspondencia con un agente a través de la dirección personal de correo electrónico del agente, sino

de una cuenta de correo electrónico apropiada proporcionada por el organismo de que se trate, y

- toda correspondencia debería llevar el membrete del organismo de que se trate, el número de teléfono de la central telefónica principal del organismo y la dirección de su sitio Web, a fin de que los proveedores de servicios puedan tomar las medidas necesarias para comprobar la autenticidad de las solicitudes si lo estiman oportuno.

25. Solicitudes – Las solicitudes provenientes de las fuerzas del orden deberían presentarse por escrito (o por otro método electrónico legalmente aceptable) y estar debidamente firmadas para asegurar su identificación y seguimiento. En los casos de extrema urgencia en los que las solicitudes orales son aceptables, éstas deben ir seguidas inmediatamente de una confirmación por escrito (u otro método electrónico legalmente aceptable).

26. Formato normalizado de solicitud – A nivel nacional y, si es posible, a nivel internacional, se debería alentar a las fuerzas del orden a normalizar y estructurar el formato utilizado para el envío de las solicitudes y para la tramitación de las mismas. Las solicitudes deberían contener, como mínimo, la siguiente información:

- el número de registro;
- la referencia a una base jurídica;
- los datos específicos solicitados, y
- la información para verificar la fuente de la solicitud.

27. Especificidad y precisión de las solicitudes – Se debería invitar a las fuerzas del orden a asegurarse de que las solicitudes enviadas son específicas, claras y completas, y proporcionan suficiente información detallada para que los proveedores de servicios puedan identificar los datos pertinentes. Se les debería alentar a asegurarse de que las solicitudes se envían al proveedor de servicios que dispone de los registros. Deberían evitarse las solicitudes de datos múltiples y no especificados.

28. Se debería invitar a las fuerzas del orden a proporcionar todos los datos posibles sobre la investigación, sin poner en peligro la investigación realizada ni los derechos fundamentales, para que los proveedores de servicios puedan identificar los datos pertinentes.

29. Se debería alentar a las autoridades responsables de cumplimiento de la ley a proporcionar explicaciones y asistencia a los proveedores de servicios en lo que respecta a las técnicas de investigación generales (no relacionadas con casos específicos), para que comprendan en qué medida su cooperación se traducirá en unas investigaciones más eficaces para luchar contra el crimen y proteger mejor a los ciudadanos.

30. Establecimiento de prioridades – Se debería invitar a las fuerzas del orden a establecer prioridades en lo que respecta a sus solicitudes, en particular aquéllas relacionadas con grandes volúmenes de datos, para que los proveedores de servicios puedan tramitar las más importantes en primer lugar. El establecimiento de prioridades será mejor si es coherente entre todas las autoridades responsables de velar por el cumplimiento de la ley a nivel nacional y, si es posible, a nivel internacional.

31. Conveniencia de las solicitudes – Se debería alentar a las fuerzas del orden a tomar conciencia de los costes que conlleva la tramitación de las solicitudes para los proveedores de servicios, y conceder a estos últimos tiempo suficiente para gestionarlas. Deberían tener en cuenta que los proveedores de servicios tal vez deban atender asimismo solicitudes provenientes de otras autoridades responsables de velar por el cumplimiento de la ley, y se les debería alentar a supervisar atentamente los volúmenes presentados.

32. Confidencialidad de los datos – Las fuerzas del orden deberían asegurar la confidencialidad de los datos recibidos.

33. Evitar costes innecesarios y la perturbación de la buena marcha de las operaciones empresariales – Se debería alentar a las fuerzas del orden a evitar costes innecesarios y la perturbación de las operaciones realizadas por los proveedores de servicios u otros tipos de empresas.

34. Se debería invitar a las fuerzas del orden a limitar la utilización de puntos de contacto de emergencia a los casos de extrema urgencia, para evitar el abuso de este servicio.

35. Se debería alentar a las fuerzas del orden a asegurarse de que las medidas de conservación y otras medidas provisionales vayan seguidas oportunamente de medidas de divulgación, o de que se comunique oportunamente al proveedor de servicios de Internet que ya no se necesitan los datos conservados.

36. Solicitudes internacionales – En lo que respecta a las solicitudes dirigidas a proveedores de servicios de Internet no nacionales, se debería alentar a las autoridades responsables de velar por el cumplimiento de la legislación nacional a no enviar solicitudes directamente a proveedores de servicios de Internet nacionales, sino a seguir los procedimientos descritos en los tratados internacionales, como el Convenio sobre la ciberdelincuencia y la red 24/7 de puntos de contacto de observancia de la legislación para medidas urgentes, inclusive las solicitudes/medidas de conservación.

37. Solicitudes de asistencia jurídica mutua internacional – Se debería alentar a las autoridades responsables de velar por el cumplimiento de la ley y a las autoridades de la justicia penal a tomar las medidas necesarias para asegurar que las solicitudes de medidas provisionales van seguidas de procedimientos internacionales orientados a una asistencia jurídica mutua, o a informar oportunamente al proveedor de servicios de Internet de que ya no se necesitan los datos conservados.

38. Coordinación entre las autoridades responsables de velar por el cumplimiento de la ley – Se debería invitar a las fuerzas del orden a coordinar su cooperación con los proveedores de servicios de Internet y a intercambiar buenas prácticas entre sí, tanto a nivel nacional como internacional. En el plano internacional, deberían recurrir a los organismos internacionales representativos pertinentes a tal efecto.

39. Programas de cumplimiento de la legislación penal – Se debería alentar a las fuerzas del orden a organizar sus interacciones arriba mencionadas con los proveedores de servicios, de tal modo que adopten la forma de un amplio programa de cumplimiento de la legislación penal, y a proporcionar una descripción de dicho programa a los proveedores de servicios, inclusive:

- la información necesaria para ponerse en contacto con el personal seleccionado de las fuerzas del orden responsable de velar por el cumplimiento de la legislación penal, y las horas en que dicho personal está disponible;
- la información necesaria para que el proveedor de servicios pueda proporcionar documentación al personal encargado de velar por el cumplimiento de la legislación penal, y
- otras informaciones específicamente destinadas al personal responsable de velar por el cumplimiento de la legislación penal (como el grado en que las fuerzas del orden cooperan con múltiples países, documentos que han de traducirse a una lengua particular, etc.).

40. Auditoría del sistema de cumplimiento – Se debería invitar a las fuerzas del orden a realizar un seguimiento y auditar el sistema de tramitación de las solicitudes con fines estadísticos, para identificar los puntos fuertes y débiles, y publicar los resultados si procede.

Medidas que deben adoptar los proveedores de servicios

41. Cooperación para reducir al mínimo la utilización de los servicios con fines ilegales – Teniendo debidamente en cuenta los derechos y libertades aplicables, como la libertad de expresión, la confidencialidad y otras leyes nacionales o internacionales, así como acuerdos de usuario, se debería alentar a los proveedores de servicios a cooperar con las fuerzas del orden a fin de reducir al mínimo la utilización de los servicios para la realización de actividades delictivas definidas por la ley.

42. Se debería alentar a los proveedores de servicios a notificar a las fuerzas del orden todo incidente delictivo que afecte a un proveedor de servicios que llegue a su conocimiento. Esto no obliga a los proveedores de servicios a buscar activamente datos o circunstancias que indiquen la realización de actividades ilegales.

43. Se debería alentar a los proveedores de servicios a ayudar a las fuerzas del orden en lo que respecta a la educación, formación y todo otro apoyo prestado en relación con sus servicios y operaciones.

44. Seguimiento de las solicitudes provenientes de las fuerzas del orden – Se debería invitar a los proveedores de servicios a no escatimar esfuerzos para ayudar a las fuerzas del orden en la ejecución de sus solicitudes.

45. Procedimientos para responder a las solicitudes – Se debería alentar a los proveedores de servicios a preparar procedimientos por escrito, que incluyan medidas apropiadas de debido procedimiento legal, para la tramitación de solicitudes, y a asegurase de que las solicitudes se tramitan de conformidad con los procedimientos acordados.

46. Formación – Se debería invitar a los proveedores de servicios a asegurarse que se imparte suficiente formación a su personal responsable de poner en práctica estos procedimientos.

47. Personal y puntos de contacto seleccionados – Se debería alentar a los proveedores de servicios a designar a miembros del personal y puntos de contacto para su cooperación con las fuerzas del orden.

48. Asistencia de emergencia – Se debería invitar a los proveedores de servicios a establecer un medio que permita a las fuerzas del orden ponerse en contacto con su personal responsable de velar por el cumplimiento de la legislación penal fuera de horas de trabajo para tratar situaciones de emergencia. Se debería alentar a los proveedores de servicios a proporcionar a las fuerzas del orden información pertinente para prestar asistencia de emergencia.

49. Recursos – Se debería alentar a los proveedores de servicios a proporcionar a los puntos de contacto o miembros del personal responsables de la cooperación con las fuerzas del orden los recursos necesarios para que puedan atender las solicitudes presentadas por las fuerzas del orden.

50. Programas de cumplimiento de la legislación penal – Se debería alentar a los proveedores de servicios a organizar su cooperación con las fuerzas del orden de tal modo

que adopte la forma de amplios programas de cumplimiento de la legislación penal, y a proporcionar una descripción de dichos programas a las fuerzas desorden, inclusive:

- la información necesaria para ponerse en contacto con el personal seleccionado de los proveedores de servicios responsable de velar por el cumplimiento de la legislación penal, y las horas en que dicho personal está disponible;
- la información necesaria para que las fuerzas del orden puedan proporcionar documentación al personal encargado de velar por el cumplimiento de la legislación penal;
- otras informaciones específicamente destinadas al personal seleccionado de los proveedores de servicios responsable de velar por el cumplimiento de la legislación penal (como el grado en que un proveedor de servicios actúa en múltiples países, documentos que han de traducirse a una lengua particular, etc.);
- a fin de que las fuerzas del orden puedan presentar solicitudes específicas y apropiadas, se debería alentar a los proveedores de servicios a proporcionar información sobre el tipo de servicios ofrecidos a los usuarios, incluidos enlaces Web a los servicios e información adicional, así como puntos de contacto para obtener más información, y
- cuando sea posible, se debería invitar al proveedor de servicios de Internet a proporcionar una lista, previa solicitud, de los tipos de datos que podrían facilitarse a las fuerzas del orden para cada servicio tras recibir una solicitud válida de divulgación de las fuerzas del orden en la que se acepte que no todos estos datos estarán disponibles para toda investigación penal.

51. Verificación de la fuente de las solicitudes – Se debería alentar a los proveedores de servicios a tomar medidas para verificar la autenticidad de las solicitudes presentadas por las fuerzas del orden en la medida de lo posible y de lo necesario para asegurar que los registros del cliente no se revelan a personas no autorizadas.

52. Respuesta – Se debería invitar a los proveedores de servicios a responder por escrito (o por otro medio electrónico legalmente aceptable) a las solicitudes presentadas por las fuerzas del orden, y a asegurarse de que puedan identificarse las solicitudes y las respuestas y realizarse un seguimiento de las mismas, aceptando que dicho seguimiento tal vez no incluya datos personales.

53. Formato normalizado de las respuestas – Teniendo en cuenta el formato de las solicitudes utilizado por las fuerzas del orden, se debería invitar a los proveedores de servicios a normalizar el formato para proporcionar información a las fuerzas del orden.

54. Se debería alentar a los proveedores de servicios a tramitar las solicitudes de una manera oportuna, en consonancia con los procedimientos que ellos mismos han establecido por escrito, y a proporcionar orientaciones a las fuerzas del orden sobre los plazos promedio para la tramitación de las solicitudes.

55. Validación de la información enviada – Se debería alentar a los proveedores de servicios a asegurarse de que la información transmitida a las fuerzas del orden es completa y precisa, y está protegida.

56. Confidencialidad de las solicitudes – Los proveedores de servicios de Internet deberían asegurar la confidencialidad de las solicitudes recibidas.

57. Explicaciones por la información no proporcionada – Se debería invitar a los proveedores de servicios a proporcionar explicaciones a las fuerzas del orden que presentan una solicitud, si se rechaza la solicitud, o si no puede proporcionarse la información solicitada.

58. Auditoría del sistema de cumplimiento – Se debería invitar a los proveedores de servicios a realizar un seguimiento y a auditar el sistema de tramitación de las solicitudes con fines estadísticos, para identificar los puntos fuertes y débiles, y publicar los resultados si procede.

59. Coordinación entre los proveedores de servicios – Teniendo en cuenta las normas antimonopolio/de competencia, se debería alentar a los proveedores de servicios a coordinar su cooperación con las fuerzas del orden y a intercambiar buenas prácticas entre sí, y a recurrir a las asociaciones de proveedores de servicios a tal efecto.