

CONSEJO PERMANENTE DE LA  
ORGANIZACIÓN DE LOS ESTADOS AMERICANOS

Grupo Especial encargado de dar cumplimiento a las  
Recomendaciones de las Reuniones de Ministros  
de Justicia o de Ministros o Procuradores Generales  
de las Américas

OEA/Ser.G  
GE/REMJA/doc.15/99 corr. 1  
1 Junio 1999  
Original: inglés

CUESTIONARIO PREPARADO DURANTE  
LA PRIMERA REUNIÓN DE EXPERTOS GUBERNAMENTALES  
SOBRE DELITO CIBERNÉTICO

(Aprobado en su sesión celebrada el 12 de mayo de 1999)

CUESTIONARIO PREPARADO DURANTE  
LA PRIMERA REUNIÓN DE EXPERTOS GUBERNAMENTALES  
SOBRE DELITO CIBERNÉTICO

1. ¿Qué entidades investigadoras, fiscales o de otra índole de su país tienen experiencia en delitos cibernéticos (actividades delictivas contra las computadoras o la información computarizada, o el uso de computadoras como medio para cometer un delito)?
2. ¿Se han cometido alguna vez o es común que se cometan en su país delitos cibernéticos como los que se enumeran a continuación?
  1. el uso de computadoras por delincuentes para almacenar información relativa a la comisión de un delito
  2. el uso de computadoras por delincuentes como medio de comunicación con otros delincuentes, con sus víctimas o con otras personas
  3. actividades delictivas en las que el uso de una computadora es parte sustancial del acto delictivo
  4. actividades delictivas contra computadoras e información electrónica, como el acceso no autorizado a sistemas de informática
3. ¿Alguna vez presentó o recibió usted una solicitud de asistencia jurídica internacional en un caso penal cibernético? ¿Qué mecanismos se usaron para prestar la asistencia y con qué rapidez se prestó?
4. ¿Define su legislación penal los sistemas de informática? En caso afirmativo, sírvase incluir la definición y la referencia a los artículos e incisos pertinentes de su Código Penal.
5. ¿Define su legislación penal los datos de computadora? ¿Incluye la definición los programas o codificaciones similares? Si tiene usted una definición, sírvase incluirla, con la referencia a los artículos e incisos pertinentes de su Código Penal.
6. ¿Sanciona su legislación penal la destrucción, modificación, alteración, acceso, uso o interferencia similar de un sistema o programa de computadora?
7. ¿Sanciona su legislación penal la eliminación, alteración, bloqueo, adquisición u otra interferencia similar de la información o los datos de un sistema o programa de computadora?
8. ¿Sanciona su legislación penal la interceptación no autorizada de la transmisión, por algún medio o modalidad, de datos o información de computadora?
9. ¿Se exige intencionalidad para la configuración de los delitos descritos en las preguntas 6, 7 y 8?
10. ¿Dan lugar a procesamiento los delitos descritos en las preguntas 6, 7, y 8?
11. ¿Se admite la extradición en los casos de los delitos descritos en las preguntas 6, 7 y 8?

12. ¿Tendría su país jurisdicción en la conducta que configura delito cibernético, conforme a las descripciones de las preguntas anteriores,
  - a) si el delito es cometido únicamente en su territorio, si uno o más de los elementos que lo constituyen se producen dentro de su territorio nacional, y si el delito causa daños en su territorio?
13. La legislación de algunos países sólo admite que las autoridades investigadoras secuestren elementos tangibles. ¿Admite la legislación de su país el secuestro de datos de computadora intangibles (por ejemplo, mediante la impresión o la copia de datos en papel o diskette, que posteriormente son secuestrados), o debe secuestrarse el medio físico en el que están almacenados los datos (por ejemplo, un diskette o la propia computadora)?
14. ¿Admite su legislación el registro por acceso directo a sistemas de computadora domésticos? En caso afirmativo, ¿respecto de qué tipo de delitos?
15. ¿Puede una empresa de telecomunicaciones o un proveedor de servicios de Internet suministrar voluntariamente a las autoridades investigadoras datos relacionados con el uso de servicios telefónicos o de computadora (por ejemplo, las facturas u otras constancias de uso, o la identidad de los suscriptores)?
16. ¿Permite la legislación de su país obligar a una empresa de telecomunicaciones o a un proveedor de servicios de Internet a revelar la información mencionada en la pregunta 15?
17. ¿Obliga la legislación de su país a) al sospechoso o b) a terceros a brindar acceso (incluida la revelación de la contraseña) a un sistema de computadora o datos que son objeto de un allanamiento o registro legal?
18. Dado que los sistemas de computadora pueden contener un gran volumen de datos, ¿permite la legislación de su país que las autoridades investigadoras que realizan el registro de un sistema de computadora secuestrar:
  - a) datos relacionados con la investigación pero no especificados en la orden judicial o de otra índole que autoriza el allanamiento o registro, datos relacionados con un delito distinto del que se está investigando y está especificado en la orden judicial o de otra índole que autoriza el allanamiento o registro y, sin orden judicial o de otra índole, datos que corren riesgo de desaparición o destrucción?
19. En relación con la pregunta 18, ¿pueden las autoridades investigadoras secuestrar esos datos sin obtener otra orden judicial?
20. ¿Permite la legislación de su país que las autoridades investigadoras realicen allanamientos o registros para recabar, interceptar u obtener por otros medios de a) un sistema de telecomunicaciones o b) de un sistema de computadora, datos sobre el origen o destino de una comunicación telefónica o por computadora contemporáneamente con su creación en el presente o en el futuro?
21. ¿Permite la legislación de su país que las autoridades investigadoras intercepten las comunicaciones telefónicas o por computadora con el propósito de obtener la información que contienen?

22. ¿Dispone su legislación la autoridad u obligación jurídica de que las empresas de telecomunicaciones o los proveedores de servicios de Internet efectúen o ayuden a efectuar interceptaciones u obtengan los datos referidos en las preguntas 20 y 21?
23. ¿Admite su legislación que las empresas de telecomunicaciones o los proveedores de servicios de Internet controlen el contenido de las comunicaciones? En caso afirmativo, ¿pueden esas comunicaciones ser entregadas voluntariamente a las autoridades investigadoras?
24. ¿Dispone su legislación la obligación de que las empresas de telecomunicaciones o los proveedores de servicios de Internet preserven la información relacionada con la identidad de los suscriptores y sobre las comunicaciones establecidas por estos (por ejemplo, fecha, hora, número de teléfono o dirección de Internet con la que se estableció la comunicación)?
25. ¿Pueden las autoridades investigadoras obligar a las empresas de telecomunicaciones o a los proveedores de servicios de Internet a preservar la información relacionada con la identidad de los suscriptores y sobre las comunicaciones establecidas por estos (por ejemplo, fecha, hora, número de teléfono o dirección de Internet con la que se estableció la comunicación) si esa información fue previamente obtenida por la empresa o el proveedor?
26. ¿Lleva su país estadísticas del número de los delitos cibernéticos
- a) denunciados por las víctimas
  - b) denunciados a la policía
  - c) procesados por la justicia?
27. ¿Ofrece su país programas de capacitación en delincuencia cibernética a
- a) la policía
  - b) las procuradurías y fiscalías
  - c) la justicia?
28. Enumerar los mecanismos de cooperación técnica en materia de delito cibernético;
29. ¿Qué medidas se han tomado en materia de revisión de los instrumentos interamericanos de cooperación jurídica y judicial?