

CONSELHO PERMANENTE DA
ORGANIZAÇÃO DOS ESTADOS AMERICANOS

Grupo Especial Encarregado de Dar Cumprimento às
Recomendações das Reuniões de Ministros
da Justiça ou de Ministros ou Procuradores-Gerais
das Américas

OEA/Ser.G
GE/REMJA/doc.15/99 corr. 1
1 junho 1999
Original: inglês

QUESTIONÁRIO PREPARADO DURANTE A PRIMEIRA
REUNIÃO DOS PERITOS GOVERNAMENTAIS SOBRE DELITOS CIBERNÉTICOS

(Aprovado em sua sessão realizada em 12 de maio de 1999)

QUESTIONÁRIO PREPARADO DURANTE A PRIMEIRA
REUNIÃO DOS PERITOS GOVERNAMENTAIS SOBRE DELITOS CIBERNÉTICOS

1. Que entidades de investigação, ação penal ou de outro tipo em seu país têm experiência na área do delito cibernético (atividade criminal que visa a computadores e informações ou que usa computadores como meio para cometer delitos)?
2. Seu país tem experimentado algum tipo ou um volume significativo de delitos cibernéticos, como:
 - a) uso de computadores por delinqüentes para armazenar informações relacionadas com o cometimento delitos?
 - b) uso de computadores por delinqüentes como meio de comunicação com outros delinqüentes, suas vítimas ou outras pessoas?
 - c) atividade criminal em que o uso de computadores é parte significativa do cometimento de delitos?
 - d) atividade criminal que visa a computadores e informações eletrônicas, como acesso sem autorização a sistemas de computação?
3. Você alguma vez procurou ou recebeu algum pedido de assistência jurídica internacional em casos de delito cibernético? Que mecanismos foram usados para prestar a ajuda e com que presteza ela foi oferecida?
4. A legislação penal do seu país define um sistema de computação? Em caso afirmativo, favor fornecer a definição e a referência aos respectivos parágrafos/artigos de seu código.
5. A legislação penal do seu país define dados computadorizados? Tal definição abrange programas ou codificações semelhantes? Se tiver uma definição, favor fornecê-la, bem como a referência aos respectivos parágrafos/artigos de seu código.
6. A legislação penal do seu país pune a destruição, modificação, alteração, acesso, uso ou outra interceptação semelhante não autorizados no que diz respeito a um sistema ou programa de computador?
7. A legislação penal do seu país pune o destruição, modificação, alteração, acesso, aquisição ou outra interceptação semelhante não autorizados no que diz respeito a informações ou dados de um sistema ou programa de computação?
8. A legislação penal do seu país pune a interceptação não autorizada de qualquer forma ou maneira de transmissão de dados ou informações computadorizados?
9. No tocante aos delitos descritos nas perguntas 6, 7 e 8, requer-se intenção específica?
10. Os delitos descritos nas perguntas 6, 7 e 8 constituem crime?

11. Os delitos descritos nas perguntas 6, 7 e 8 constituem delitos extraditáveis?
12. Seu país teria jurisdição sobre condutas que representem crimes cibernéticos, segundo as descrições acima,
 - a) quando cometidos apenas dentro do seu território;
se um ou mais dos elementos constituintes ocorreram no seu território nacional; e
se o crime provocou danos em seu território?
13. A legislação de alguns países permite apenas a apreensão de materiais tangíveis pelas autoridades de investigação. A legislação do seu país permite a apreensão de dados computadorizados intangíveis (por exemplo, mediante a impressão ou gravação de dados em papel ou disquete, subseqüentemente apreendido), ou precisa ser apreendido o meio físico no qual os dados estão armazenados (por exemplo, um disquete de computador ou o próprio computador)?
14. A legislação do seu país permite a busca *on-line* de sistemas domésticos de computação? Em caso positivo, para que tipos de crimes?
15. Uma empresa de telecomunicações ou um provedor de serviços de Internet podem fornecer voluntariamente dados sobre o uso de serviços de telefone ou computador (por exemplo, contas ou outros registros de uso ou dados sobre a identidade do assinante) às autoridades de investigação?
16. A legislação do seu país permite que uma empresa de telecomunicações ou um provedor de serviços de Internet sejam obrigadas a fornecer as informações referidas na pergunta 15?
17. A legislação do seu país obriga: a) um suspeito; ou b) um terceiro a darem acesso (inclusive o fornecimento de senhas) a um sistema ou a dados de computação que sejam alvo de sindicância legal?
18. Considerando que os sistemas de computação podem conter grandes volumes de dados, a lei do seu país permite que as autoridades de investigação encarregadas de uma sindicância em um sistema de computador apreendam
 - a) dados relevantes a uma investigação mas que não tenham sido especificados no âmbito de um mandato judicial ou outro que autorize a sindicância;
dados relacionados com um crime que não seja o que está sendo investigado e tenha sido especificado no mandato judicial ou outro que autorize a sindicância; e
dados, sem um mandato judicial ou de outra natureza, sob risco de remoção ou destruição?
19. No caso da pergunta 18, as autoridades de investigação podem apreender tais dados sem outro mandato judicial?
20. A legislação do seu país permite a sindicância por parte das autoridades de investigação a fim

de coletar ou interceptar (ou de outra forma obter), de: a) um sistema de telecomunicações; ou b) um sistema de computação dados sobre a fonte ou o destino de uma comunicação telefônica ou eletrônica em tempo real, no presente ou no futuro?

21. A lei do seu país permite a interceptação, por autoridades de investigação, de comunicações telefônicas ou eletrônicas a fim de obter as informações delas constantes?
22. A legislação autoriza ou obriga uma empresa de telecomunicações ou um provedor de serviços de Internet a executarem ou apoiarem a interceptação ou obtenção dos dados referidos nas perguntas 20 e 21?
23. A legislação permite que uma empresa de telecomunicações ou um provedor de serviços de Internet monitorem o conteúdo das comunicações? Em caso positivo, essas comunicações podem ser fornecidas voluntariamente às autoridades de investigação?
24. A legislação obriga uma empresa de telecomunicações ou um provedor de serviços de Internet a manterem registros de dados sobre a identidade de um assinante, bem como dados relativos a transações de comunicação (por exemplo, data, hora, número do telefone ou endereço eletrônico contatado)?
25. As autoridades de investigação podem obrigar uma empresa de telecomunicações ou um provedor de serviços de Internet a manterem registros de dados sobre a identidade de um assinante, bem como dados relativos a transações de comunicação (por exemplo, data, hora, número do telefone ou endereço eletrônico contatado) se esses dados tiverem sido coletados anteriormente por essa empresa ou provedor?
26. São mantidas estatísticas sobre o número de casos de crimes cibernéticos
 - a) notificados pelas vítimas?
 - b) notificados pela polícia?
 - c) levados a julgamento?
27. Seu país oferece programas de treinamento em crimes cibernéticos para
 - a) policiais?
 - b) servidores da promotoria?
 - c) servidores do Judiciário?
28. Quais os mecanismos de cooperação técnica em matéria de delito informático?
29. Que medidas foram tomadas em matéria de revisão dos instrumentos interamericanos de cooperação jurídica e judicial?