FERNANDO JOSÉ DA COSTA

LOCUS DELICTI NOS CRIMES INFORMÁTICOS

Tese de Doutorado apresentada à Banca Examinadora da Faculdade de Direito da Universidade de São Paulo, como exigência parcial para a obtenção do título de Doutor em Direito, sob orientação da Professora Titular Ivette Senise Ferreira

FACULDADE DE DIREITO DA USP
SÃO PAULO
2011

BANCA EXAMINADORA

_____

_____

_____

_____

_____

À minha esposa e minhas filhas que, por conta de meus sonhos acadêmicos, por alguns anos tiveram-me em convívio familiar distanciado; a meu pai amigo certo nas horas incertas; e aos meus colegas de escritório Pedro Guedes de Souza Campanella e Daniel Antonio de Souza Silva pelo apoio e ajuda nesta difícil e longa tarefa.

AGRADECIMENTOS

A Deus, fonte inspiradora em meus momentos de dificuldade e insegurança.

À Professora Doutora Ivette Senise Ferreira, meu eterno agradecimento pelas preciosas orientações, pela amizade paciente, pelo incentivo e por ter me ofertado a oportunidade de, como seu orientando, apesar de minhas limitações, concluir esta empreitada na Faculdade de Direito.

Aos Doutores Antonio Scarance Fernandes e Vicente Greco Filho pelos imprescindíveis comentários e sugestões apontados a partir de meu exame de qualificação.

Ao professor Renato de Mello Jorge Silveira, da mesma forma como seu pai em minha empreitada quando da dissertação de mestrado, pelo rico apoio, carinho e amizade.

A todos os demais professores que, sempre de braços abertos, me acolheram e me franquearam preciosos comentários.

"Internet deve ser um meio de comunicação entre os povos que contribua à paz mundial e que o principal objetivo da alta tecnologia é melhorar o nível de vida das pessoas." (Larry Ellison)

RESUMO

Aborda a introdução do computador e da internet na sociedade e sua relação com o direito. Discorre sobre o uso da informática para a prática de crime, observando que o delito penal deixou de ser local e ganhou dimensões internacionais, porquanto seu resultado não se dê necessariamente no mesmo local onde foi praticada a conduta. Chama a atenção ao fato de que os princípios delimitadores da validade da lei penal no espaço podem não ser suficientes para dirimir eventuais conflitos de jurisdição, se interpretados como tradicionalmente se tem feito. Analisa e classifica as espécies de crimes informáticos de forma exemplificativa, bem como os agentes criminais da era digital. Reúne e comenta as leis e projetos de leis nacionais, bem como as leis estrangeiras e convenções sobre crimes informáticos. Ao final, aponta, em sede de conclusão, critério de solução para a resolução do conflito de jurisdição para os crimes praticados no ciberespaço, sugerindo, de *lege ferenda,* a persecução de uma lei dirimente de eventual conflito.

Palavras-chave: *Internet*, *Locus delicti*, Teoria da Ação, Jurisdição, Crimes por Computador, Direito Penal

ABSTRACT

Discusses the advent of the computer and the internet in society and their relation with the law. Considers the use of information technology in committing crime, observing that a penal offence is no longer local, since it has acquired international dimensions. Therefore, its resolution does not necessarily happen in the same locality where it was practiced. Draws attention to the fact that the principles that delimit the validity of the penal law might not be sufficient to dispel possible conflicts of jurisdiction, if interpreted in the usual traditional way. By giving examples, it analyses and classifies types of electronic crimes as well as the criminal agents of the digital age. Gathers and comments laws and projects of law, both national and international, as well as conventions on electronic crimes. Finally, it presents criteria of solution for resolving the conflict of jurisdiction for crimes practiced in cyberspace, suggesting, of *lege ferenda*, the pursuit of a law which would eliminate such conflicts.

Key words: Internet, *Locus delicti,* Action theory, Jurisdiction, Computer Crime, Criminal law

RIASSUNTO

Esamina l'introduzione del computer e dell'internet nella società e il loro rapporto con il diritto. Discorre dell'uso dell'informatica per la pratica del reato e osserva che il delitto penale non è più locale, dato che ha preso dimensioni internazionali. Perciò, la soluzione di un reato non si fa necessariamente nello stesso luogo dove è stato praticato. Fa notare che, se interpretati tradizionalmente, i principi che stabiliscono la validità del diritto penale possono essere insufficienti per dissipare eventuali conflitti di giurisdizione. Con esempi, analizza e classifica i delitti informatici e gli agenti criminali dell'era digitale. Raccoglie e commenta su le leggi e progetti di leggi, nazionali ed internazionali, e le convenzioni su il reato informatico. Finalmente, presenta criterio per risoluzione dei conflitti di giurisdizione verso i reati in ciberspazio e suggerisce, de *lege ferenda*, la ricerca di una legge per eliminare conflitti eventuali.

Parole chiave: Internet, *Locus delicti*, Teoria dell'azione, Jurisdizione, Reati attraverso il "computer" Diritto penale

SUMÁRIO

INTRODUÇÃO

O presente trabalho científico tem o escopo de abordar a informática e sua relação com o direito penal, mais especificamente com o *locus delicti* para definir a competência do julgador.

O trabalho se inicia discorrendo sobre o surgimento e a evolução tecnológica do computador e da *internet*. Nele, questões técnicas como o seu manuseio, provedor, servidor, *web*, IP[1], dentre outras, são abordadas com vistas a facilitar o entendimento das complexas questões enfrentadas na era digital. O estudo, em síntese, analisa também a ciência cibernética.

Discorre-se sobre novas modalidades de condutas delituosas – as praticadas por meio do computador – ponderando-se que muitas delas são passíveis de amoldamento às condutas já tipificadas pelo direito penal, razão pela qual é discutível na doutrina a necessidade de legislação específica.

Adota-se uma linha de raciocínio que levará à conclusão de que as condutas taxadas de crimes informáticos puros merecem tipificação específica, ao passo que as taxadas de crimes impuros devem ser tratadas pela lei penal já existente.

Enfrenta este trabalho as mudanças surgidas com a informática, apresentando as modalidades delitivas mais comuns após o surgimento da era digital, bem como as suas respectivas consequências.[2]

Faz-se uma compendiada apresentação das legislações e projetos de lei sobre crimes informáticos, nacionais e alienígenas.

Passa-se à distinção entre o agente criminoso comum e o informático, analisando-se a distinção entre os traços de personalidade, comportamento e intelectualidade entre ambos.

---

[1]Internet Protocol: trata-se do endereço que indica o local onde está situado o computador, em uma rede privada ou pública.

[2]WikLeaks e o apagão da *internet* no Egito, ocorrido na última semana de janeiro de 2011, propositadamente causado pelo Governo a fim de inibir os protestos contra o então presidente Hosni Mubarak, causando prejuízos de milhões de reais.

Sobre o provedor, discorre-se sobre sua essencial função no mundo digital e nas condutas ilícitas através dele praticadas, para posteriormente enfrentar sua relação com a conduta e o resultado delitivo e, mais precisamente, sua relação ou não com o *locus delicti.*

Um dos temas mais complexos enfrentados após o surgimento da era informática está relacionado com a responsabilidade do provedor, mais precisamente com o *locus delicti* quando este se situa em local diverso do local da conduta e do resultado.

Tem-se pela frente um problemático conflito de jurisdição entre nações, oriundo da inexistência de legislação específica que estabeleça qual ou quais as nações estarão aptas a apurar e punir infração praticada por meio de um computador ligado em rede, quando mais de uma nação estiver envolvida com o delito. Para tanto, o estudo adentra a teoria da territorialidade e da extraterritorialidade como sendo nortes seguros para a aplicação do direito interno às condutas praticadas em terras estrangeiras.

Sustenta-se que a teoria do local do crime e os conceitos dela decorrentes são bastantes para dirimir os conflitos existentes entre jurisdições estrangeiras. Tais preceitos apenas merecem uma releitura e reflexão mais aprofundada para dirimir o conflito que pode surgir quando o crime informático se desenvolve em mais de um país. Conclui-se o presente trabalho enfrentando o tema e propondo ao exegeta uma solução e uma contribuição *de lege ferenda*.

CAPÍTULO I. O COMPUTADOR

1. Conceito

O termo computador vem do latim *computadore* – aquele que faz cálculos. A primeira máquina a fazer cálculos foi o ábaco, surgida há 2000 anos a.C., e ainda hoje utilizada em alguns países do Oriente.[3]

No entanto, a evolução do mundo digital teve início, segundo Alcântara Pereira, há cerca de 400 anos.

Uma nova baliza surgiu com a criação do computador.[4] Foi na década de 40 que começaram a ser desenhadas as primeiras linhas desta máquina que mais tarde seria interligada a outras e que, como instrumento, tinha o objetivo de facilitar a vida do homem.

Houve um grande processo de evolução até chegar-se a uma linguagem natural, acessível e com alta velocidade de processamento de dados.

Temos hoje cinco gerações de computadores. A primeira surgiu na Segunda Guerra Mundial. Urgia encontrar meios para controlar os estoques de materiais bélicos e para calcular a tabela de artilharia para cada lote de munição.

A IBM (International Business Machines Corporation), associada à marinha americana e ao grupo Ultra, na Inglaterra, implementando projeto de Haward Aiken e Konrad Zuze, na Alemanha, criou o primeiro computador eletromecânico, o ASSCC, Automatic Sequence Controlled Calculator (Calculadora Automática de Sequência Controlada), recebendo a denominação "Mark I".[5]

Jonh Presper Eckert e Jonh W. Mauchly, na Universidade da Pensylvania, com o escopo de resolver problemas balísticos, entre 1934 e 1946 desenvolveram o primeiro computador eletrônico de grande porte denominado Electronic, Numeric, Integrator and

---

[3]PEREIRA, Ricardo Alcântara. *Direito eletrônico*. Bauru, SP: EDIPRO, 2001. p. 23.
[4]ROSSINI, Augusto. *Informática, telemática e direito penal*. São Paulo: Memória Jurídica Ed., 2004.
[5]SILVA, Rita de Cássia Lopes da. *Direito penal e sistema informático.* São Paulo: Ed. Revista dos Tribunais, 2003. p. 17-19.

Calculator (Eniac). Esta máquina tinha 17.468 válvulas de 16 tipos, com um tamanho de 30 metros de largura por 3 metros de altura e um consumo de 140kW de energia.[6]

Foi em 1951 que surgiu o Universal Automatic Computer I (Univac I), primeira geração de computadores por válvulas eletrônicas. Ele foi desenvolvido a partir de um modelo experimental chamado Electronic Discrete Variable Automatic Computer (Edvac), que armazenava o programa em forma codificada, dentro de uma memória interna.[7]

A terceira geração de computadores surgiu na década de 60, com a utilização de circuitos integrados. Esta passagem das válvulas para os transistores foi muito relevante e popularizou sua utilização e evolução. Surgiram, então, os minicomputadores com execuções de tarefas diversas daquelas realizadas pelas máquinas de médio e grande porte.[8]

Outra importante transformação sucedeu na própria programação com a multiprogramação, consistente na execução, em apenas uma unidade central, de processamento de mais de um programa e do teleprocessamento, que significa o processamento à distância.[9]

A quarta geração de computadores foi marcada pelo aumento da capacidade de armazenamento de dados, rapidez e precisão no desenvolvimento do processamento de dados. Isto se deu graças aos circuitos integrados em escalas superiores de integração.[10]

Os microprocessadores e o *mainframe*, computador de grande porte, denominam a quarta geração de computadores. Eles foram desenvolvidos com a tecnologia de circuitos integrados em escalas superiores de integração.[11]

A quinta geração foi marcada pela evolução dos *hardwares*, *softwares* e telecomunicações. A simplificação e miniaturização do computador com a possibilidade de obtenção de recursos ilimitados foram os grandes avanços desta fase.[12]

---

[6]CHAVES, Antônio. *Computação de dados: conceitos fundamentais. apud* SILVA, Rita de Cássia Lopes da. op. cit., p. 17.
[7]PIRAGIBE, Célia. *Indústria da informática*: desenvolvimento brasileiro e mundial. Rio de Janeiro: Campus, 1985. p. 22.
[8]Id., loc. cit.
[9]KANAAN, João Carlos. *Informática global*: tudo o que você precisa saber sobre informática. São Paulo: Pioneira, 1998. p. 30.
[10]Id., loc. cit.
[11]Id. Ibid., p. 31.
[12]Id., loc. cit.

Em outubro de 1973, John Atasanoff, da Universidade de Iowa, foi considerado pela justiça norte-americana o verdadeiro inventor do computador. Ele foi o responsável pela construção, em 1939, de um calculador binário denominado ABC, diferenciando-se do Eniac por ser não automático e não programável.[13]

As máquinas de computador invadiram, na década de 80, o setor de serviços, tais como as instituições financeiras, os estabelecimentos comerciais e industriais, além dos centros acadêmicos.

Em pouco tempo chegou ao consumidor final nos termos em que conhecemos hoje. Foi uma mudança radical de hábitos. O homem, que num passado não muito distante registrava acontecimentos em pedras, passou a registrá-los em máquinas com processadores de dados.

Assim, a escrita e a leitura em papel estão sendo substituídas por uma tela de cristal líquido de um computador, de um telefone móvel ou de um *ipad*[14].

As informações processadas na máquina, no entanto, eram estanques. Não havia transmissão de dados entre um computador e outro. Cada computador tinha sua memória e não a compartilhava com outro. Hoje, através do teleprocessamento estes dados são transmitidos a outras máquinas a milhares de quilômetros de distância, em fração de segundos.

Inimaginável, nos dias atuais, o funcionamento de qualquer estabelecimento como um hospital ou de uma instituição financeira, sem a utilização do computador. Da mesma forma, o registro da história humana é hoje feito e armazenado em microprocessadores, quer pela escassez de papel, quer pela falta de espaço físico para armazenagem.

2. Cibernética

Cibernética é uma palavra de origem grega, *Kibernetes,* que significa a arte do timoneiro. Trata-se da ciência geral dos sistemas informantes e, especificamente, dos sistemas de informação.[15]

---

[13]PIMENTEL, Alexandre Freire. *O direito cibernético*: um enfoque teórico e lógico-aplicativo. Rio de Janeiro: Renovar, 2000. p. 12-13.

[14]*Ipad* é definido como uma plataforma móvel com uma tela de cristal líquido e *touch screen* para armazenamento de dados e aplicativos com navegação na *web*.

[15]CHAVES, Antônio. Aspectos jurídicos da juscibernética: direito de autor do programador. *Revista de Informação Legislativa*, Brasília, ano 19, n. 73, p. 280, jan./mar. 1982.

A cibernética é uma ciência que estuda não só as máquinas, mas também o homem. Dedica-se a entender o seu sistema nervoso e seu cérebro, bem como a relação entre o homem e a máquina. O computador foi criado respeitando os princípios da cibernética, portanto não se pode confundir computador com cibernética.

Nosso cérebro e o nosso sistema nervoso recebem e processam informações que enviam estímulos aos órgãos motores e músculos. Estes combinam a informação recebida com aquela acumulada de modo a influir nas ações futuras.[16]

Assim como os membros do corpo humano realizam movimentos a partir de comandos do cérebro, o computador, que é um sistema de processamento de dados e informações com capacidade de enviar e realizar comandos pré-determinados pelo homem, executa tarefas a partir de comandos externos.

Analisando a Cibernética, Antônio Limongi França aponta que o deixar cair uma pedra ao solo mostra que o sistema homem-pedra-solo não pode ser reconhecido como sistema cibernético porque nada pode influenciar esta queda. Trata-se da lei da gravidade.[17]

Diversamente, se um homem pega a pedra e a coloca no solo, realiza a ação de mover o braço em direção ao chão com um controle do cérebro que, ao encostar a pedra ao solo, enviará um comando para que a mão largue a pedra. Nesta ação cibernética temos um controle de movimentos comandados por um sistema denominado cérebro.

Na análise do sistema informático do computador, este é alimentado por dados que, através de uma gerência humana, direta ou indireta, receberá comandos que produzirão um resultado esperado.

Enquanto o computador é um processador de dados, a cibernética é a ciência dos sistemas da informática. Não se pode com precisão definir seu campo de estudo, já que se encontra em constante transformação.

Para Carraza[18], trata-se da ciência das máquinas, do cérebro e do sistema nervoso do homem. Tem como escopo a descoberta de seu funcionamento, analisando o modo de realização das coisas.

---

[16]WIENER, Norbert. *Cibernética e sociedade*: uso humano de seres humanos. São Paulo: Cultrix, 1954. p. 16-17.

[17]FRANÇA, Antonio de S. Cibernética jurídica. *Revista de Direito Civil, Imobiliário, Agrário e Empresarial*, São Paulo, ano 10. p. 118-135, jul./set. 1986.

[18]CARRAZA, Roque Antonio. Aplicações da cibernética ao direito em outras nações (Experiências e resultados. Opinião dos juristas). *Justitia*, São Paulo, ano 36, v. 94, p. 56, jan./mar. 1974.

O sistema informático, sob o ponto de vista cibernético, analisa a informação, a comunicação e o controle da vida humana, quer no seu mundo interior, quer no exterior[19].

Para Norberto Wiener[20], a cibernética compara o funcionamento do cérebro humano e do computador eletrônico, chegando à conclusão de que não existe diferença essencial entre dar uma ordem a uma pessoa ou a um computador. Justifica-se apontando que ambos possuem receptores sensórios que captam informações, sendo irrelevante, para a relação da informação através de sinal, o fato de a informação ter passado pela máquina ou pelo homem.

O homem é igualmente uma máquina de processar informações. Através do cérebro e do sistema nervoso envia estímulos aos órgãos motores e músculos.

Volvendo ao conceito de sistema cibernético de Limongi França,[21] uma pedra solta ao chão não pode ser considerada um sistema cibernético, porque pela lei da gravidade nada impedirá que ela caia ao chão. Todavia, se o homem coloca a pedra no chão, há uma ação de movimento do braço em direção ao solo com orientação do cérebro que determinará a distância entre a pedra e o chão. Apenas no momento em que a pedra encontrar o solo o cérebro enviará mensagem para largar a pedra.

Esse sistema formado pelo cérebro, braço, mão e o chão, alimentado pelos órgãos sensitivos, é denominado sistema cibernético.

Desta forma, no sistema informático, com integração do sistema de informação e do computador, o homem alimenta a máquina com dados, que irão produzir um resultado ocasionado em razão deste comando humano.[22]

Esse resultado, alcançado pela vontade humana através do cérebro, do sistema nervoso e da máquina, pode ser denominado “cibernética”.

---

[19]SILVA, Rita de Cássia Lopes da. op. cit., p. 20.
[20]WIENER, Norbert. op. cit., p. 15-27.
[21]FRANÇA, Antonio de S. op. cit., p. 118-135.
[22]SILVA, Rita de Cássia Lopes da. op. cit., p. 21-22.

CAPÍTULO II. A *INTERNET*

1. Conceito

Podemos definir a *internet* como uma rede mundial de usuários que simultaneamente trocam informações. Trata-se da maior e mais célere rede de comunicação do planeta.

Nos Estados Unidos da América, em 1969, no mesmo ano de sua criação, a Suprema Corte definiu a *internet* como:

> The Internet is an international network of interconnected computers. Is the outgrowth of what began in 1969 as a military program called ARPANET, which was designed to enable computers operated by the military, defense contractors, and universities conducting defense related research to communicate with one another by redundant channels even if some portions of the network were damaged in a war. While the ARPANET no longer exists, it provided an example for the development of a number of civilian networks that, eventually linking with one another, now enable tens of millions of people to communicate with one another and to access vast amounts of information from around the world. The Internet is the unique and wholly new medium of worldwide communication.[23]

Segundo a Norma nº 004/95, da Agência Nacional de Telecomunicações (ANATEL), aprovada pela Portaria nº 148, de 31 de maio de 1995, do Ministério das Comunicações, item 3, alínea 'a', Anexo A, a *internet* é "nome genérico que designa o conjunto de redes, os meios de transmissão e comutação, roteadores, equipamentos e protocolos necessários à comunicação entre computadores, bem como o 'software' e os dados contidos nestes computadores". Em nota conjunta divulgada pelo Ministério das Comunicações e Ministério da Ciência e Tecnologia, item 2.1, Anexo B, de junho de 1995, *internet* é "um conjunto de redes interligadas, de abrangência mundial".

Para Patricia Peck Pinheiro[24], a *internet* consiste na ligação de milhares de dispositivos em todo o planeta, interconectados por protocolos IP (internet protocol),

---

[23]THE UCLA ONLINE INSTITUTE FOR CYBERSPACE LAW AND POLICY. Disponível em: <http://gseis.ucla.edu/iclp/internet.html>. Acesso em: 29 abr. 2011.

[24]PINHEIRO, Patricia Peck. *Direito digital*. 4. ed. São Paulo: Saraiva, 2010. p. 59.

utilizando-se de um mesmo padrão de transmissão de dados. Esta comunicação é feita por linha telefônica, fibra óptica, satélite, ondas de rádio ou infravermelho. Já a comunicação do computador com a rede pode ser direta ou por outro computador, conhecido por servidor, próprio ou de terceiros (provedores de acesso).

A navegação é feita por *browser*, tal como MS Internet Explorer, da Microsoft, o Netscape Navigator, da Netscape. *Browser* pode ser definido como programa usado para visualizar páginas disponíveis na rede, que interpreta as informações do *website*, trazendo à tela dos computadores textos, sons e imagens.

Marcos Salt[25] define esta tecnologia informática como a segunda revolução industrial, dizendo-a, inclusive, mais transformadora do que a revolução industrial do século XIX, dado o desenvolvimento de sua tecnologia e a sua enorme influência na vida cotidiana dos habitantes.

Milhões de computadores podem comunicar-se entre si, graças ao sistema global de intercomunicação, denominado *internet*, que permite de qualquer lugar remoto do planeta acessar, através de um *site*, uma informação ou serviço oferecido.[26]

Trata-se de um meio que não conhece distâncias, limites, nem obstáculos linguísticos. Aponta o referido autor a *internet* como um enorme caminho de informação que cria uma nova estrutura social global.

Por meio do computador e de um provedor de acesso, todos passaram a se comunicar dentro de um só espaço. Esse espaço de comunicação é chamado ciberespaço ou espaço cibernético.

Para Opice Blum[27], os programas de computadores possibilitaram o desenvolvimento de inúmeros setores da economia mundial, além de permitir maior conforto e agilidade para o homem, sendo uma das mais relevantes criações no campo científico-tecnológico.

---

[25]SALT, Marcos. Delitos informáticos de carácter econômico. In: MAIER, Julio B. J. (Comp.). *Delitos no convencionales.* Buenos Aires: Editores del Puerto, 1994. p 225 e ss.

[26]ABOSO, Gustavo Eduardo; FLORENCIA ZAPATA, María. *Cibercriminalidad y derecho penal*. Buenos Aires: Editorial B de F, 2006. p. 6.

[27]SETTE, Luiz Augusto Azevedo. Dados sobre a proteção jurídica do software no Brasil. In: BLUM, Renato M. S. Opice et al. (Coord.). *Direito eletrônico*: a internet e os tribunais. Bauru, SP: EDIPRO, 2001. p. 627.

Percebe-se que, em pouquíssimo tempo, a era informática vem mudando nossas vidas e costumes. A cada dia nos tornamos mais e mais dependentes dos sistemas de informação providos pela *internet*.

As nações, distantes por milhares de quilômetros, foram aproximadas pela tela de um computador, celular, *ipad* e outros aparelhos ligados em rede. Através da rede temos uma comunicação simultânea entre países localizados em lados opostos do planeta.

Tem-se com a *internet*, além da comunicação, a possibilidade de enviar comandos possibilitando a realização de atividades, independentemente de distâncias. Pode-se, pela *internet*, de São Paulo comprar uma empresa em Tóquio.

Através dela, em tempo real, transmitem-se imagens que possibilitam o homem visualizar um lugar distante. Através da *internet* o planeta acompanhou a recente tragédia japonesa com *tsunami* causado por tremores de 8.9 graus.

Pela *internet* o homem passou a realizar seus negócios, aumentando em frações inimagináveis seu mercado de trabalho.

Segundo dados da Organização Mundial do Comércio[28], no ano de 1998, as transações comerciais no espaço virtual já tinham atingido 300 bilhões de dólares. "Sistemas informáticos não se deixam limitar por fronteiras territoriais".[29]

Esta máquina, ligada em rede, é hoje responsável principalmente pela nossa segurança, comunicação, alimentação, trabalho, registro de dados, conforto e saúde.

2. Origem

Sobre o surgimento da *internet*, afirma Maria Eugênia Finkelstein que se deu por meio de pesquisas norte-americanas, desenvolvidas em 1969 pela ARPANET. Aponta ainda que apesar de haver comentários de que ela teria sido criada para fins militares, a tese dominante registra seu surgimento através de pesquisa da agência norte-americana ARPA, tendo sua primeira ligação ocorrida entre quatro universidades.

---

[28]WORD TRADE ORGANIZATION. Disponível em: <http://www.wto.org>. Acesso em: 03 fev. 2011.

[29]ALBUQUERQUE, Roberto de Araújo de Chacon de. *A criminalidade informática*. 2003. Tese (Doutorado em Direito Penal) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2003. p. 65.

Foi no ano de 1970 que os estudos a respeito se aprofundaram com a criação de um conjunto de protocolos dando base à *Internet*. Em seguida, centros de pesquisas foram integrados por redes de computadores através da agência ARPA. Em 1986, houve a interligação da NSFNET, da entidade americana NSF, à ARPANET, dando origem às atuais bases da *Internet*.[30]

Outros relatos históricos, a nosso ver mais consistentes, dão conta de que a *internet* surgiu de um programa militar americano chamado ARPANET[31] (Advanced Research Projects Agency Network), mantido pelo Departamento de Defesa do governo norte-americano, na agência de Advanced Research Project Agency (ARPA), hoje denominada DARPA (Defense Advanced Projects Research Agency). Tal programa militar teria como objetivo realizar pesquisas de novas tecnologias, além de encontrar um meio de manter uma comunicação mesmo em caso de ataque inimigo.

Esta rede surgiu nos Estados Unidos da América no período da guerra fria, mais precisamente em 1969[32], por receio de um ataque da União Soviética ao Ocidente, o qual, se ocorresse, poderia deixar as bases militares americanas sem comunicação ou fazer com que as informações lá armazenadas fossem perdidas.[33]

Assim, Paul Baran, da Rand Corporation, criou esta rede de comunicação sem comando central, utilizada pelo sistema telefônico, onde todos se comunicavam simultaneamente. Isto quer dizer que se um dos pontos interligados fosse interrompido, os demais continuariam se comunicando.[34]

Esta comunicação foi instalada na Universidade da Califórnia, de Los Angeles, e interligada a outras três universidades: Universidade de Santa Bárbara, Universidade de Utah e Instituto de Pesquisa de Stanford, surgindo, a partir desta comunicação, a Arpanet. Alguns anos mais tarde, agências governamentais e militares, como a Nasa, foram igualmente interligadas a esta rede.

---

[30]DE LUCCA, Newton; SIMÃO FILHO, Adalberto (Coords.). *Direito & internet*: aspectos jurídicos relevantes. São Paulo: Quartier Latin, 2008. v. 2, p. 407.
[31]LEONARDI, Marcel. *A responsabilidade civil dos provedores de serviços de internet*. São Paulo: Juarez de Oliveira, 2005.
[32]Id. Ibid.
[33]PINHEIRO, Patricia Peck. op. cit., p. 58 e 59.
[34]SILVA, Rita de Cássia Lopes da. op. cit., p. 22.

Até os anos setenta, esta comunicação em rede era dividida entre a Milnet, de utilidade militar e a Arpanet, de utilidade acadêmica. Na década de 80, a Arpanet estabeleceu o padrão IP/TCP, utilizado até os dias de hoje.

O primeiro correio eletrônico, denominado *e-mail* foi enviado nos Estados Unidos, em 1972, tendo no ano seguinte sido enviado para o Reino Unido e Noruega.

A comunicação, primeiramente feita em laboratório, passou a ser feita por empresas especializadas. Em 1985, foram interligados os computadores da National Science Foundation (NSF), surgindo a National Science Foundation Network (NSFNET).

A *internet* de fato passou a existir com a ligação dos *backbones* NSF com a ARPANET. Define-se *backbone* como a espinha dorsal de cabos de telecomunicação de dados entre computadores de grande porte e roteadores que controlam o tráfego na *internet*, possibilitando a visualização e a transferência de dados através de quilômetros de distância.[35]

No ano de 1987 a *internet* passou a ser utilizada para fins comerciais, sendo tal feito considerado por muitos como o grande marco para o desenvolvimento dessa tecnologia.[36]

Esse sistema precursor de comunicação entre redes (ARPANET) deixou de operar em 1990, visto a existência, nos Estados Unidos da América, de novas redes, como a criada pela National Science Foundation, denominada Backbone Defense Research Internet (DRI*).* Em 1991 e 1992 surgiu a Ansnet, passando a ser um dos principais backbones da época.

Também no início da década de noventa foi criado o primeiro *backbone* europeu, denominado Ebone, interligando alguns países daquele continente.

Foi no ano de 1993, com o desenvolvimento da World Wide Web (www) e da autoridade estatutária conferida pela National Science Fundation para comercializar a denominada NSFNET, que a *internet* efetivamente nasceu aos olhos da sociedade. Surgiu, então, o mundo *on line*[37]. Antes disso sua finalidade comercial era proibida.

---

[35]SILVA, Rita de Cássia Lopes da. op. cit., p. 23.
[36]PINHEIRO, Patricia Peck. op. cit., p. 59.
[37]DE LUCCA, Newton; SIMÃO FILHO, Adalberto (Coords.). op. cit., v. 2, p. 407-408.

3. A *internet* no Brasil

A *internet* chegou ao Brasil apenas em 1988, através da Rede Nacional de Pesquisa (RNP) e por iniciativa do Ministério da Ciência e Tecnologia.

No ano seguinte, com o apoio da Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), da Universidade Federal do Rio de Janeiro (UFRJ) e do Laboratório de Computação Científica (LNCC), sob execução e coordenação política e orçamentária do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), foi oficialmente lançada no Brasil.

Apenas em 1992 foi instalada a primeira espinha dorsal conectada à *internet* nas principais universidades e centros de pesquisa do País e em algumas organizações não governamentais.[38]

Foi, no mesmo ano, firmado convênio entre o Instituto Brasileiro de Análises Sociais e Econômicas (IBASE) e a Associação para o Progresso das Comunicações com o escopo de dar às ONGs espaço na rede. Ainda nesse ano o convênio foi alterado para criar, pelo Ministério da Ciência e Tecnologia, a Rede Nacional de Pesquisa.

Mais precisamente em maio de 1995, a operação da Rede no Brasil deixou de atuar nas áreas da educação e pesquisa, para tornar-se acessível comercialmente a qualquer setor da sociedade, com a criação de um provedor de acesso privado.[39]

O Brasil já conta com aproximadamente 36,4 milhões de internautas[40], com previsão de expandir ainda mais este expressivo número, vez que o comércio e os serviços migram a cada dia para este terreno abstrato que é a *internet*, razão pela qual tem demonstrado preocupação no que diz respeito ao regramento jurídico do tema.

O número de *sites* cadastrados aumenta a cada dia. Atualmente existem quase 2,5 milhões de *sites* cadastrados no Brasil.[41] Paralelamente a este crescimento, o Brasil se tornou o líder na América do Sul em ocorrências eletrônicas criminosas.[42]

---

[38]SILVA, Rita de Cássia Lopes da. op. cit., p. 25.
[39]DE LUCCA, Newton; SIMÃO FILHO, Adalberto (Coords.). op. cit., v. 2, p. 408.
[40]ESTATÍSTICAS sobre a Internet no Brasil. Disponível em: <http://www.tobeguarany.com/internet_no_brasil.php>. Acesso em: 14 jan. 2010.
[41]REGISTRO.BR. Estatísticas. Disponível em: <http://www.registro.br/estatisticas.html>. Acesso em: 16 fev. 2011.
[42]SAFER NET. *Brasil é o campeão de crimes eletrônicos na América do Sul*. Disponível em: <http://www.safernet.org.br/site/noticias/brasil-%C3%A9-campe%C3%A3-crimes-eletr%C3%B4nicos-am%C3%A9rica-sul>. Acesso em: 16 fev. 2011.

Abaixo, colaciona-se, apenas para referência, o número de provedores de *internet* nos países que lideram a quantidade do serviço em janeiro de 2009:[43]

Posição	País	Número de servidores Internet
1	Japão	33,333,000
2	Alemanha	16,494,000
3	França	12,556,000
4	Países Baixos	11,170,000
5	China	10,637,000
6	Austrália	9,458,000
7	Brasil	8,265,000
8	México	7,629,000
9	Polônia	5,681,000
10	Reino Unido	5,118,000
11	Taiwan	5,111,000
12	Canadá	4,196,000
13	Itália	4,117,000
14	Estados Unidos	3,950,000
15	Suécia	3,318,000
16	Bélgica	3,195,000
17	Dinamarca	3,114,000
18	Rússia	2,844,000
19	Espanha	2,552,000
20	Áustria	2,427,000
21	Finlândia	2,323,000
22	Hungria	2,313,000
23	Índia	2,306,000
24	Argentina	2,159,000
25	Noruega	2,084,000

[43]Fonte: CIA World Factbook *in* INDEX MUNDI. Comparação entre países. *Número de servidores internet*. Disponível em: <http://www.indexmundi.com/g/r.aspx?v=140&l=pt>. Acesso em: 11 mar. 2011.

4. Seu funcionamento[44]

Para que se possa pesquisar e escrever sobre *internet* e sua relação com o direito é preciso adentrarmos no seu funcionamento.

O governo, em junho de 1995, emitiu Nota Conjunta, itens 2.2 a 2.5 definindo o funcionamento da *internet* nos seguintes termos:

> A Internet é organizada na forma de espinhas dorsais backbones, que são estruturas de rede capazes de manipular grandes volumes de informações, constituídas basicamente por roteadores de tráfego interligados por circuitos de alta velocidade. Interligadas às espinhas dorsais de âmbito nacional, haverá espinhas dorsais de abrangência regional, estadual ou metropolitana, que possibilitarão a interiorização da Internet no País. Conectados às espinhas dorsais, estarão os provedores de acesso ou de informações, que são os efetivos prestadores de serviços aos usuários finais da Internet, que os acessam tipicamente através do serviço telefônico. Poderão existir no País várias espinhas dorsais Internet independentes, de âmbito nacional ou não, sob a responsabilidade de diversas entidades, inclusive sob controle da iniciativa privada.

Explicando passo a passo, a ligação da *internet* se dá por uma linha telefônica, onda de rádio, satélite ou banda larga com cabos de fibra ótica, conectando-se a um provedor de acesso, que por sua vez se conecta a uma rede maior denominada roteador, detentor de grandes volumes de informações, onde usuários poderão se conectar e estabelecer também uma conexão entre si.

Não se trata de uma entidade física ou tangível, mas de uma enorme rede que se conecta a inúmeros grupos de redes menores de computadores conectados entre si. Trata-se de uma rede de redes. Algumas delas estão restritas, têm o acesso limitado a outras redes ou provedores. As redes, de uma forma geral, estão conectadas através de redes que estão, por sua vez, conectadas em outras redes de tal maneira que permitam a cada um dos computadores, de qualquer lugar do mundo, conectar-se com outro computador, desde que conectado àquela rede. Esta rede global de computadores conectados entre si é o que chamamos de *internet*.[45]

---

[44]LEONARDI, Marcel. op. cit.
[45]Id. Ibid.

Para que haja comunicação entre usuários conectados à *internet*, a conexão se dá através de pontos de presença, localizados em determinadas regiões, denominados *Network Access Points* (NAP's), que nada mais são do que equipamentos informáticos que possibilitam a conexão de seus usuários.

Todos os usuários que acessarem este ponto de presença de um provedor, desde que livre o acesso para ele, poderão se comunicar. Estes pontos de presença, por sua vez, através de cabos de fibra ótica, de telefonia ou por satélite, conectam-se a outros pontos de presença, criando assim os pontos de acesso, os quais tornam possível que todos estes pontos conectados ao provedor se conectem entre si, transmitindo dados de uma rede para outra.

Estas redes interligadas a uma limitada região conectam-se com os provedores *backbones*, muitas vezes situados no exterior, definidos, conforme Nota Conjunta, como estruturas de redes capazes de manipular grandes volumes de informações, constituídas basicamente por roteadores de tráfego interligados por circuitos de alta velocidade.

Os roteadores têm papel imprescindível nesta comunicação em rede. São os responsáveis para que as informações cheguem ao destino correto, bem como garantir que elas não cheguem a locais não almejados ou proibidos. Sem eles seria impossível organizar as milhares de comunicações interligadas simultaneamente no planeta.

A linguagem dos dados transmitidos pelo usuário na *internet* é o TCP/IP (Transmission Control Protocol /Internet Protocol), conhecido em nosso vernáculo como Protocolo de Controle de Transmissão/Protocolo de *Internet*.

Estes dados são unificados pelo Protocolo de Controle de Transmissão (TCP) em pequenos pedaços chamados "pacotes". O Protocolo de *Internet* coloca em cada pacote uma determinada quantidade de dados transmitidos por um usuário, as informações para chegarem a seu destino, o endereço de seu remetente e de seu destinatário, o número total de pacotes em que a informação transmitida foi dividida (isto no caso de ter sido dividida em mais de um pacote) e o número daquele pacote específico. Estes dados constantes neste pacote serão enviados pela melhor rota possível.

Sendo os dados transmitidos em número maior que o permitido em um pacote, serão divididos em dois ou mais pacotes que serão enviados para o mesmo destino, porém podem ser enviados por rotas diversas, disponíveis naquele instante.

Em caso de problema técnico em qualquer das rotas que impeça o tráfego do pacote de dados, outras rotas serão imediatamente selecionadas até que tais dados cheguem ao destinatário final.

A respeito, explana Marcel Leonardi que os pacotes de dados possuem os endereços de IP do remetente e do destinatário. O número do IP é o que identifica um determinado computador conectado à *internet* em determinado momento. Este número, atualmente, é dividido em quatro partes com três dígitos cada. Toda vez que um usuário se conecta à rede, seu computador recebe automaticamente de seu provedor de acesso um determinado número de IP que será o único durante aquela conexão. Sem ter conhecimento deste número de IP, um pacote de dados não tem como chegar a seu destino final.[46]

Por conta do excessivo crescimento de usuários, está em desenvolvimento novo protocolo para substituir o IPv4, dividido em quatro partes com três dígitos cada por um IPv6, dividido em seis partes.

Por fim, para que os endereços textuais, também conhecidos como nomes de domínio, almejados pelos usuários, sejam identificados na rede, precisam transformar-se em IP. Este serviço, que consiste na decodificação da sequência numérica em nome, é feito pelos servidores DNS. Caso não conheçam aquele número de IP, buscam em outros DNSs. Não encontrando tal número, uma mensagem de erro ao usuário é enviada.

5. A *internet* e o direito

Desde os primórdios da história, a guerra tem sido, a um só tempo, involução humana e social e também terreno fecundo para desenvolvimento tecnológico. As guerras acabam. As inovações tecnológicas nelas produzidas são desenvolvidas nos anos seguintes.

Com a *internet*, novas condutas passaram a existir e com elas novos litígios. Alguns já regulamentados pelas normas existentes. Outros, não.

Conforme relata o Manual das Nações Unidas[47], o homem nos dias atuais e em um futuro próximo dependerá cada vez mais do computador e de sua ligação em rede para sobreviver.

---

[46]LEONARDI, Marcel. op. cit.
[47]Vide anexo inteiro teor.

Reclama atenção a matéria, não apenas do legislativo, mas de toda a ciência jurídica. Trata-se de realidade cotidiana, imprescindível à humanidade e em constante mutação, que exige premente reflexão.

Se por um lado compete ao legislativo regular o uso, punir o abuso e traçar diretrizes para se alcançar segurança na informática, por outro cabe à sociedade e às entidades governamentais e privadas a efetivação da almejada segurança por meio da prevenção e de programas que visem o adequado uso deste meio de comunicação e trabalho tão importante.

O direito deve acompanhar a evolução humana, mas nem sempre isto é possível. Muitas vezes o direito só é alterado após o surgimento de situações antes não reguladas[48]. No mundo virtual estas mudanças são ainda mais dinâmicas.

5.1. Da autorregulamentação

O primeiro ponto a ser enfrentado neste item é a discussão que paira sobre a necessidade ou não de a *internet* ser regulada pelo direito frente à sua suposta capacidade de se autorregular.

Uns defendem a liberdade total, outros a auto-regulação[49], outros a utilização da legislação existente[50], outros a necessidade de nova e específica legislação[51] e, por fim, há aqueles que sustentam a necessidade de regulação por nações.

Um dos primeiros pontos a ser analisado quando o assunto direciona-se aos crimes informáticos diz respeito à aplicabilidade ou não da legislação vigente. Para uns a legislação existente é suficiente para punir esta nova modalidade delitiva, para outros há necessidade de nova legislação.

---

[48]Cite-se como exemplo as divulgações feitas pelo *site* do Wikleaks, acerca de documentos postados por anônimos, veiculando notícias diversas, e apagão da *internet* provocado pelo governo do Egito na tentativa de conter os protestos contra o presidente Hosni Mubarak.

[49]LAWRENCE, Lessig. *The future of ideas*: the fate of the commons in a connected world. New York: Random House, 2001.

[50]GRECO FILHO, Vicente. Algumas observações sobre o direito penal e a internet. *Boletim IBCCRIM*, São Paulo, ed. especial, ano 8, n. 95, out. 2000.

[51]LORENZETTI, Ricardo. L. *Comercio electrônico.* Buenos Aires: Abeledo Perrot, 2000. p. 227.

Com efeito, a *internet* não é bem jurídico sobre o qual repousa posse, propriedade. Não existe relação de domínio entre uma pessoa e a *internet*. No entanto, não por isso se deva dizer que o ciberespaço é um ambiente não regulável.

A despeito de o espaço cibernético ser um ambiente não físico, deve ser ele passível de ser regido pelo direito, até porque seus resultados são materiais.

O direito não encontra seu fundamento na regulamentação do espaço, objeto ou conduta. Repousa o esteio do direito na necessidade de proteger os valores entendidos como importantes para determinada sociedade.

No século XXI, a nova forma de convivência relacionada a uma cultura de convergência, em que a internet molda uma nova vida, é exemplo de manifestação de um meio ambiente cultural. [52]

Analisando-se pormenorizadamente os institutos gerais da lei penal é possível a verificação das razões que conduziram às alterações legislativas rumo ao progresso científico do direito penal.[53]

Miguel Reale[54], em sua célebre Teoria Tridimensional do Direito ensinou que sobre o valor é que deita a norma. Não há que se regular toda e qualquer conduta, mas sim aquela sobre a qual há juízo axiológico.

Da mesma forma, a exemplo da questionável lei da oferta e da procura, preconizada por Adam Smith como sendo o remédio para os males do mercado, o ciberespaço não pode se autorregular sem a ingerência estatal.[55]

O Estado liberal mostrou-se prevaricador para com os menos favorecidos no passado. Basta lembrar que quando adotada em França, após a revolução, a teoria "laissez faire, laissez passez, le monde va de lui-même", o modelo foi copiado em todo o mundo e não tardou para o capitalismo mostrar que a falta da regulação estatal apenas serviria para tornar latente a desigualdade entre as pessoas. A burguesia enriqueceu-se vertiginosamente e o proletariado amargou inigualável miséria.

---

[52]FIORILLO, Celso Antonio Pacheco. *Curso de direito ambiental brasileiro*. 12. ed. rev., atual. e ampl. São Paulo: Saraiva, 2011. p. 77.

[53]BUENO, P. A. T. A. C. Notícia histórica do direito penal brasileiro. In: BITTAR, Eduardo Carlos Bianca (Org.). *História do direito brasileiro*. São Paulo: Atlas, 2003. v. 1, p. 180.

[54]REALE, Miguel. *Lições preliminares de direito*. São Paulo: Saraiva, 2006.

[55]SMITH, Adam. *A riqueza das nações*: investigação sobre sua natureza e suas causas. Tradução de Luiz João Baraúna. São Paulo: Nova Cultural, 1996. v. 1 e 2.

Mostrar-se-á o Estado igualmente não cumpridor de sua função e dos fundamentos do pacto social se não proteger a sociedade e os seus valores. Nesta esteira é que se defende ser adúltero o direito que fecha os olhos aos reclamos sociais e que espera a autorregulação da realidade social, enquanto esta tem seus valores espancados pelas condutas tidas por autorreguláveis.

Colaborando com o retardamento da adequação legislativa ao tema em análise, por muito tempo persistiu a ideia de que a *internet* se autorregularia. Talvez parte dela de fato possa se autorregular. As condutas proibidas ou obrigatórias, no entanto, certamente, precisam ser regulamentadas.

Para Aznar, criticando aqueles que defendem a autorregulamentação na *Web* sob a justificativa de se compensar deficiências e defeitos apresentados pela regulamentação estatal, a regulamentação autônoma, certamente, não conseguirá suprir o papel do Estado de normatizar as condutas do homem.

Continua expondo o autor que esta mencionada regulamentação deve cumprir seu importante papel complementar ao Direito, em especial, nas áreas pouco regulamentadas por ele, como é o caso do ciberespaço. Pode, ainda, contribuir para melhorar o panorama coletivo da rede, mas não pode, por si só, resolver os conflitos surgidos com ela ou criar a esperança de que sozinha pode solucionar os problemas oriundos dela própria.[56]

Para Maria Eugênia Finkelstein[57], a *internet* exige uma convivência ordenada. Por tratar-se de manifestação de sociedade, necessita do Direito para regulamentá-la. O Direito tem o dever de tentar acompanhar esta revolucionária evolução social, na mesma velocidade deste fabuloso meio de comunicação. Alerta ainda a mencionada autora, da dificuldade em se aplicar o Direito, em face da novidade e dinâmica da *internet*, dizendo que este problema não é restrito à exploração da Rede, mas ao desenvolvimento e aplicação do Direito como um todo, sempre mais lento que o desenvolvimento da sociedade.

Quer-nos parecer que a regulamentação estatal, a ingerência do direito no ciberespaço, assim como em todo o meio de comunicação, conquanto que preservada a

---

[56]AZNAR, H. Medios de comunicación y esfera pública: el papel de la autorregulación. In: BUENDÍA, Manuel. *Deontologia y autorregulación informativa.* México, D.F., 2000. p. 160-162.

[57]FINKELSTEIN, Maria Eugênia. Fraude eletrônica. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto (Coords.). op. cit., v. 2, p. 404-405.

liberdade de expressão, dogma do estado democrático de direito, e nos estritos limites do necessário, faz-se mister.

Porquanto impossível a vida sem o computador e sua interligação, a sociedade tem que se adequar para recebê-lo, ditando, quando necessário, regras aos usuários e sanções a seus infratores.

O Estado, por meio de suas leis e nos termos em que ensinados por Reale[58], protege aquilo que é tido pela maior parte do povo como correto. Ao menos este é o fundamento da democracia representativa.

Em 1980, o Direito da informática foi oficialmente reconhecido pelo Conselho da Comunidade Europeia, devendo adequar-se ao direito tradicional, após reunir todos os aspectos jurídicos da informática.

A nossa Lei 9.800, de 1999, por exemplo, atenta às facilidades propiciadas pelo mundo digital, permitiu e regulamentou o envio de petições aos tribunais por *e-mail*. Na mesma esteira, a Lei 11.419, de 2006, regulamentou a informatização do processo judicial.

Não se deve ver na *internet* a anunciação do fim dos tempos. Tampouco se deve entendê-la como símbolo da modernidade inatingível pelo tradicional direito. Antes, haverá a classe jurídica de identificá-la, entendê-la e regulá-la, como realidade social e, como tal, passível de ser palco de conflitos.

5.2. A *internet* e o direito penal

As diversas áreas do direito por todo o mundo já se mostram permeadas de relações com a *internet*. Já se debruçam sobre o tema. Diversas obras foram escritas e até mesmo algumas leis[59] fazem menção ao mundo digital e seus instrumentos.

---

[58]REALE, Miguel. op. cit.

[59]BRASIL. Lei 11.690 de 10 de junho de 2008. Altera dispositivos do Decreto-Lei nº 3.689, de 3 de outubro de 1941 – Código de Processo Penal, relativos à prova, e dá outras providências. *Diário Oficial da União*, Brasília, DF, 10 jun. 2008 e BRASIL. Lei 12.403 de 4 de maio de 2011. Altera dispositivos do Decreto-Lei nº 3.689, de 3 de outubro de 1941 - Código de Processo Penal, relativos à prisão processual, fiança, liberdade provisória, demais medidas cautelares, e dá outras providências. *Diário Oficial da União,* Brasília, DF, 05 maio 2011.

O artigo 201 do Código de Processo Penal, alterado pela Lei 11.690 de 10 de junho de 2008, previu a possibilidade de por meio eletrônico, e aqui se inclui a *internet*, intimar a vítima no processo penal acerca dos atos processuais relativos ao *status libertatis* do acusado, audiências, sentença e acórdãos. Esta Lei permitiu, ainda, o interrogatório do acusado preso por meio de vídeoconferência (artigo 185, § 2º do Código de Processo Penal).

Seguindo a mesma linha, a Lei 12.403 de 4 de maio de 2011, com *vacatio legis* de 60 dias, que também modificou o Código de Processo Penal, deu redação ao artigo 289, § 1º de forma a permitir ao juízo requisitar a prisão do acusado por qualquer meio de comunicação.

Ainda, contudo, nossa literatura está muito aquém do que é necessário.

Uma vez mais, o direito deve, nas questões mais relevantes, impor suas regras e sanções a seus infratores. Deve o direito penal estar adequado ao mundo digital, tutelando bens e punindo seus infratores.

Encontra a lei penal, assim como todas as demais leis do estado de direito, fundamento na democracia e, por tal razão, impera sobre os que a criaram e também sobre os que com ela não concordam. O seu desrespeito é retribuído com a sanção cominada em seu preceito secundário.

A conduta reprovável pela sociedade, quando devidamente tipificada pelo direito penal como criminosa, resvala na esfera dos direitos protegidos pela norma, desafiando punição estatal. Trata-se de uma resposta legal do Estado à prática criminosa. Mesmo na *internet* a conduta reprovável pela sociedade deve continuar protegida pelo Estado.

Miguel Reale Júnior aponta que a aplicação correta do Direito Penal e de suas sanções constituem mais que um direito, um poder do Estado, que, almejando assegurar a harmonia social, não pode deixar de atuar e deixar ao talante dos particulares sua efetividade. Se assim agisse teríamos uma *capitis diminutio*, com a fragilização da soberania e o surgimento de uma profunda insegurança jurídica para a sociedade, de sorte que a eficácia da norma estaria limitada ao interesse da vítima ou de sua família, gerando

inclusive ao infrator uma insegurança jurídica e ao Estado uma limitação da aplicabilidade da lei.[60]

O Direito Penal, no entanto, por encontrar seus fundamentos legais basicamente no Código Penal, mostra-se por vezes alheio às inovações trazidas à sociedade pelo computador e sua rede de comunicação.

Zamora aponta que desde o ano de 2000 o mundo tomou consciência das diferentes ameaças surgidas para a sociedade com a rede. Com ela surgiu o crime cibernético. Já no ano de 1995 a *internet* era conhecida como um instrumento apto ao favorecimento do crime. Assim, alerta sobre o tratamento que os meios de comunicação em massa estavam dando ao tema *internet*, em especial à liberdade de comunicação e ao acesso universal da informação. Afirma que a liberdade de comunicação serviria, sobretudo, para organizar redes racistas, fascistas e pedófilas. Conclui expondo que o comércio eletrônico seria o reino dos traficantes de órgãos e de lavagem de dinheiro, e que o sigilo das comunicações seria um meio seguro para esconder assassinos a solta.[61]

Como se vê, a ingerência estatal na *internet*, antes de ser uma afronta à liberdade de expressão ao argumento de que a *internet* é apenas mais um meio de comunicação, faz-se imperiosa na medida em que o ciberespaço se tornou terreno fecundo para variados crimes.

Diversamente dos clássicos delitos, na era digital as mudanças são diárias e o direito penal deve, com uma linguagem mais apropriada, sem ofender o princípio da taxatividade ou da anterioridade da lei penal, acompanhar tais mutações.

Não obstante a crescente preocupação no âmbito penal com as condutas criminosas perpetradas pelo computador, tipificando-as e punindo-as, nada se tem discutido acerca da aplicabilidade da lei penal deste ou daquele país. Sem ela, a norma vigente se torna inaplicável. Assim, a preocupação do direito penal não deve se reduzir à tipificação. Tratando-se de condutas que têm em sua essência a internacionalidade, faz-se mister a persecução de regras que determinem a jurisdição sobre as condutas que se pretende punidas.

---

[60]REALE JÚNIOR, Miguel. *Instituições de direito penal*: parte geral. 3. ed. Rio de Janeiro: Forense, 2009. p. 15.

[61]LÓPEZ ZAMORA, Paula. *El ciberespacio y su ordenación*. Madrid: Difusión Jurídica y Temas de Actualidad, 2006. p. 61.

O conflito de leis no espaço, tratado em capítulo específico, por esta razão tem sido dirimido pelas regras e princípios encampados na Parte Geral do Código Penal, e assim o será até que legislação específica venha à luz e de forma concreta enfrente o tema, ou até que se faça uma releitura de tais regras e princípios à luz da nova realidade.

Desta forma, independentemente da posição dos juristas quanto à necessidade de nova legislação acerca do tema, tem-se hoje que as condutas praticadas por meio do computador são criminosas e como tais devem ser punidas. Assim, propõe-se, como se verá em capítulo próprio, uma releitura das regras de aplicação da lei penal no espaço, de forma a nelas encontrar fundamento necessário à repressão.

CAPÍTULO III. OS LIMITES DE VALIDADE DA LEI PENAL NO ESPAÇO

A lei penal é dotada, assim como as demais leis, de validade no tempo e no espaço. Quanto à sua validade no espaço, deve ela observar a soberania de cada Estado sobre seu respectivo território e domínio. Isto porque, como todo Estado possui sua própria sistemática penal, a ausência de delimitação das leis penais poderia ensejar ofensa ao Estado que sofresse a invasão de lei alienígena em seu território.

Como se depreende do até aqui exposto, o princípio da territorialidade é questão discutível a partir do momento em que se tem por bem delineado o lugar do crime, de sorte que se torna impossível qualquer tentativa de buscar a lei penal aplicável quando incerta a soberania estatal.

Assim, tendo-se em vista que o presente trabalho tem por objetivo discutir o lugar do crime naqueles denominados informáticos, convém, ainda que superficialmente, traçar algumas linhas sobre o princípio da territorialidade e sua relação com o lugar do crime.

A aplicação da lei penal no espaço observa alguns princípios que delimitam sua validade e seu conteúdo, além de figurar como fonte de interpretação em caso de conflitos. São, destarte, apontáveis cinco princípios norteadores do tema.

1. Princípio da territorialidade

Entende-se por princípio da territorialidade o fundamento imbuído no sistema penal pelo qual a lei nacional aplicável será sempre a do país no qual o ato ou resultado foi praticado, independentemente da nacionalidade do agente ou da vítima.

Escreve Miguel Reale Júnior que o Estado, detentor do poder-dever de punir, impõe a norma penal por ele editada no seu território, isto quer dizer, na área geográfica em que se assenta o país. Esta noção, se compreendida literal e isoladamente, poderia nos levar a conceituar território como apenas o espaço terrestre. Mas, na verdade, território é toda a

área na qual o Estado exerce soberania, compreendendo a zona de fronteira, marcada por rios e lagos, bem como o mar territorial.[62]

Este princípio é consectário da soberania que tem um Estado face aos demais Estados e em relação às pessoas que se encontram em seu território, sejam elas nacionais ou não. A soberania do Estado brasileiro é o primeiro dos fundamentos da República e consta do artigo 1º, inciso I da sua Constituição.

Divide-se o princípio da territorialidade em ativa, passiva e mista.

A territorialidade ativa preocupa-se com o local em que foi praticada a conduta do agente. Encontrará o Estado, adotada a teoria da territorialidade ativa, fundamento para punir o agente que praticar uma conduta criminosa em seu território.

Se adotada a territorialidade passiva como regente da soberania estatal para fins de aplicação da lei penal, deverá o Estado punir apenas as condutas criminosas que produzam resultado em seu território.

Por fim, a teoria da territorialidade mista torna legítima a aplicação da lei penal tanto a Nação onde o agente pratica a conduta quanto aquela onde o delito surte efeito.

Pela regra da territorialidade mista, a qual é aplicada no Brasil, o país é competente para processar e julgar o autor de qualquer crime praticado, no todo ou em parte, em seu território, da mesma forma como aqueles em que a conduta foi praticada no exterior, mas seu resultado se deu ou deveria se dar em nossas fronteiras.

Esta regra não prevalece, contudo, em havendo disposição em contrário constante de tratados, convenções e regras de direito internacional.

Por comportar exceções relacionadas aos tratados e convenções internacionais, eventualmente uma lei estrangeira pode ser aplicada no Brasil, se assim dispuser o tratado ou convenção contemplada, como, por exemplo, na hipótese dos crimes praticados por agentes diplomáticos, razão pela qual, diz-se que o Brasil adota, como principal regra de vigência da lei penal no espaço, a territorialidade mista temperada.

O temperamento encontrado na teoria adotada visa atenuar aquilo que Bettiol[63] assinalou como um critério muito rígido de solução de aplicabilidade da lei penal no

[62]REALE JÚNIOR, Miguel. op. cit., p. 105.
[63]BETTIOL, Giuseppe. *Direito penal*. Tradução brasileira e notas do Professor Paulo José da Costa Junior e do magistrado Alberto Silva Franco. São Paulo: Ed. Revista dos Tribunais, 1966. v. 1, p. 188.

espaço, criticando o argumento de que seria uma consciência do próprio Estado de sua soberania e de um consequente sentimento de ciúmes para com as ordenações penais estrangeiras.

A tradicional noção de soberania do Estado é bastante para, por si só, limitar a atuação do seu poder político ao espaço físico de seu território.

É a partir desta noção que o artigo 5º do Código Penal Brasileiro estabelece que "aplica-se a lei brasileira, sem prejuízo de convenções, tratados, e regras de direito internacional, ao crime cometido no território nacional".

Cumpre salientar que o conceito jurídico de território ultrapassa os limites meramente geográficos de um Estado, vez que não se restringe ao solo interrompido pelas fronteiras. Em verdade, o território se estende por todo o espaço sobre o qual o Estado exerce sua soberania.

O conceito de território em direito público é mais largo que o conceito de território do direito privado. Para o direito público, o território estende-se por todo o espaço que o Estado exerce sua soberania e sobre o qual faz, assim, valer a vontade jurídica nacional. Ao passo que para o direito privado o termo território está relacionado à posse e ao domínio.

Hungria escreve que a autoridade do Estado sobre o território não se identifica com o direito privado de propriedade – trata-se de uma autoridade exclusivamente política, tal como a exercida sobre as pessoas. É o poder do governo.[64]

Aníbal Bruno observa a este respeito que este princípio "corresponde à noção interna e à delimitação imposta pelo Direito Internacional ao poder de *imperium* de cada Estado".[65]

Em se tratando de direito público, são tidos como território a porção da superfície terrestre e águas que se encontram entre os limites impostos pela natureza e reconhecidos como sendo de domínio do Estado, ou seja, as faixas de águas fronteiriças e os mares territoriais definidos nos termos das regras do direito internacional, o subsolo e o espaço aéreo correspondente ao território e mar territorial, tanto quanto necessário, no entendimento do Estado, para garantir a segurança nacional e tanto quanto possível ao homem penetrar e exercer atividade.

---

[64]HUNGRIA, Nelson. *Comentários ao Código Penal*. Rio de Janeiro: Revista Forense, 1955. p. 154.
[65]BRUNO, Aníbal. *Direito penal*. 3. ed. Rio de Janeiro: Forense, 1967. p. 231.

Quanto aos rios, segundo definição de Noronha, podem ser considerados como nacionais ou internacionais, conforme corram pelo território de apenas um país ou corram pelo território de mais de um país, ou, ainda, dividam os territórios de dois Estados.[66]

Se o rio internacional é sucessivo, isto é, se corta mais de um país, cada Estado exerce sua soberania sobre a parte do rio que lhe corta o território.

São estas, como pode se depreender, as limitações territoriais naturais do poder soberano estatal.

No passado, conforme observa José Frederico Marques[67], foi fixada uma norma costumeira segundo a qual os limites da faixa marítima sobre a qual exercia sua soberania o Estado, coincidia com o poder de alcance de suas armas, com a linha de alcance de um tiro de canhão situado na costa.

Evidentemente, hoje é imprecisa esta definição. No entanto, a partir dela se compreende que o critério norteador do limite do interesse estatal deve ser do tamanho da capacidade que tem de ser ofendido e de se defender.

Mas, como já ressaltado anteriormente, o conceito de território para fins de direito público é mais extenso do que pode propor a natureza.

Compreende-se, como continuidade do território estatal, como espaço geográfico submetido à jurisdição estatal e sob o jugo de suas leis penais, as aeronaves e as embarcações brasileiras, de natureza pública ou a serviço do governo brasileiro, onde quer que se encontrem, bem como as embarcações e aeronaves brasileiras, mercantes ou de propriedade privada, que se achem, respectivamente, no espaço aéreo correspondente ou em alto-mar.

Rene Ariel Dotti define as aeronaves e navios como públicos quando a serviço do Estado, em qualquer lugar, inclusive em território estrangeiro. São privadas quando o interesse passa a ser privado (comércio, turismo, missões científicas etc). O crime cometido no interior destas aeronaves ou navios será julgado pela lei do país a que pertencerem se se encontrarem em território nacional ou em alto-mar ou espaço aéreo respectivo. Se ocorrido em território ou espaço aéreo estrangeiro, a princípio, será esta a

[66]NORONHA, E. Magalhães. *Direito penal.* São Paulo: Saraiva, 1977. p. 96.
[67]MARQUES, José Frederico. *Tratado de direito penal*. Campinas: Bookseller, 1997. p. 292.

legislação aplicada. Aplica-se a lei brasileira aos crimes ocorridos em aeronaves ou embarcações estrangeiras de propriedade privada, dentro do território nacional.[68]

Se praticados crimes a bordo de barcos salva-vidas ou embarcações feitas a partir dos destroços em alto-mar de um navio naufragado ou avião acidentado, por estes serem considerados remanescentes da nave ou aeronave, e como tal extensão do território do país em que estava matriculada, a lei aplicável é a da sua bandeira.[69]

Atento ao fato de que o conceito de território deve ser jurídico e não físico, o Código Penal brasileiro, no parágrafo 1º do artigo 5º encampou mais do que a terra nacional:

> Para os efeitos penais consideram-se como extensão do território nacional as embarcações e aeronaves brasileiras, de natureza pública ou a serviço do governo brasileiro onde quer que se encontrem, bem como as aeronaves e as embarcações brasileiras, mercantes ou de propriedade privada, que se achem respectivamente, no espaço aéreo correspondente ou em alto-mar.

O princípio da territorialidade, segundo Juarez Cirino dos Santos, apresenta três caracteres: "a plenitude, como totalidade de competências sobre questões da vida social; a autonomia, como rejeição de influências externas nas decisões sobre essas questões; e a exclusividade, como monopólio do poder nos limites de seu território".[70]

O princípio da territorialidade, no entanto, não pode existir estanque dos demais princípios, pois, como assevera Mirabete, pode ser corolário de injustiça e levar à impunidade, deixando o Estado obrigado a julgar apenas os crimes ocorridos em seu território, abstendo-se de julgar aqueles ocorridos no estrangeiro.[71]

Ademais, não raro, os interesses estatais vão além de seu território. Ou seja, os bens jurídicos estatais que estão além de suas fronteiras também devem ser acobertados pelo manto de proteção do direito penal, razão pela qual se faz imperiosa a extensão da lei nacional de forma a atingir limites antes não previstos expressamente.

Mirabete compreende, para efeitos penais, o território nacional como o delimitado espaço geográfico, as embarcações e aeronaves nacionais, públicas ou a serviço do estado,

---

[68]DOTTI, René Ariel. *Curso de direito penal*: parte geral. Rio de Janeiro: Forense, 2002. p. 277.
[69]MIRABETE, Julio Fabbrini. *Manual de direito penal*. 22. ed. São Paulo: Atlas, 2005. p. 76.
[70]SANTOS, Juarez Cirino. *Direito penal*. Rio de Janeiro: Forense, 1985. p. 47.
[71]MIRABETE, Julio Fabbrini. op. cit., p. 73.

em qualquer lugar, embarcações e aeronaves brasileiras mercantes ou privadas, que se achem, respectivamente, em alto-mar ou no espaço aéreo correspondente.

Qualquer delito praticado nestes meios de transporte nos locais apresentados, obrigatoriamente, é alcançado pela lei brasileira, exceto aqueles expressos por convenções, tratados e regras de direito internacional.[72]

Concluímos com Paulo José da Costa Junior que "território é todo o espaço, estritamente geográfico ou ampliado mercê de ficção jurídica, sujeito à soberania e à jurisdição do Estado".[73]

2. Princípio da nacionalidade

A territorialidade, o espaço geográfico, a determinação do país em cujas terras houve a prática delitiva não é suficiente critério para identificar a lei aplicável para sua repressão.

Outros princípios, embora não majoritariamente aplicados, são igualmente invocados para dirimir conflitos entre leis penais no espaço. Dentre eles, o princípio da nacionalidade, também denominado princípio da personalidade.

Pelo princípio da nacionalidade ou da personalidade resolve-se a questão suscitada há pouco – a de que o princípio da territorialidade poderia, se bastante em si mesmo, dar azo à impunidade.

Isto porque, por força do princípio da nacionalidade, pode o agente criminoso ser punido segundo as leis de seu país, ainda que tenha praticado o crime além das fronteiras de seu Estado.

Funciona este princípio como se o Estado estivesse a exigir de seu cidadão bons modos em sua terra e também no estrangeiro. A lei nacional acompanha o seu súdito onde quer que este se encontre.

---

[72]MIRABETE, Julio Fabbrini. op. cit., p. 77.
[73]COSTA JR., Paulo José da; COSTA, Fernando José da. *Curso de direito penal*. 12. ed. São Paulo: Saraiva, 2010. p. 85.

Também é atribuível a este princípio o direito que tem o Estado de não extraditar o seu nacional, responsabilizando-o ou não pelos atos por ele praticados.

Sendo certo que a maioria dos países, e aqui se inclui o Brasil[74], não extradita seus cidadãos, seria demasiado injusto que o agente praticasse a conduta no exterior e voltasse para o seu país, dele se valendo como manto para não ser punido.

Por outro lado, as relações entre as nações restariam estremecidas caso o Estado do agente criminoso, além de não extraditá-lo, o acobertasse da justiça do país ofendido. Da mesma forma, um país, diverso daquele onde a conduta e o resultado delitivo sucederam-se, que nega extradição a estrangeiro abala o relacionamento entre estas Nações.[75]

Segundo este princípio da nacionalidade, ainda que praticado o delito no exterior, o agente será punido pelo seu país de origem como forma exemplar, afastando-se a impunidade e acalmando os ânimos do país cujas leis foram ofendidas.

O cidadão é, por força deste princípio, acompanhado pelo Código Penal de seu país.

A ampliação do poder punitivo estatal, em razão do princípio da nacionalidade, tem por consequência a proteção que o Estado dá aos seus cidadãos, na medida em que lhes confere o direito de ser por ele punido em detrimento do *jus puniendi* alienígena, sem, contudo, consentir com a impunidade.

Diante da opção de punir seu cidadão ou de entregá-lo para que o país agredido o puna, o Estado prefere a primeira.[76] Se o Estado não entregar seu cidadão ao país que o reclama pelo crime praticado contra bem protegido por lei estrangeira, obriga-se a reprimi-lo, segundo suas leis, pelo mesmo fato.[77]

Os cidadãos alemães, entre os anos 1939 e 1945, por exemplo, radicados no ex-protetorado boêmio-morávio, eram julgados segundo a lei penal alemã, assim como os

---

[74]Conforme se depreende da Constituição da República, artigo 5º, inciso LI. (BRASIL. Constituição (1988). *Constituição da República Federativa do Brasil, de 5 de outubro de 1988*. 13. ed. São Paulo: Ed. Revista dos Tribunais, 2011).

[75]Neste sentido tivemos recentemente o caso do ex-ativista italiano Cesare Battisti, condenado à prisão perpétua na Itália, por quatro homicídios, no qual, em 31/12/2010, o então presidente da República Federativa do Brasil Luiz Inácio Lula da Silva, com base no parecer da Advocacia-Geral da União, negou pedido de extradição oriundo da Itália concedendo a ele asilo político. Tal decisão estremeceu o relacionamento entre o Brasil e a Itália.

[76]PRADO, Luiz Regis. *Curso de direito penal brasileiro*: parte geral, arts. 1º a 120. 7. ed. São Paulo: Ed. Revista dos Tribunais, 2007. p. 201.

[77]FRAGOSO, Heleno Cláudio. *Lições de direito penal*: parte geral. Ed. rev. e atual. por Fernando Fragoso. Rio de Janeiro: Forense, 2004. p. 132.

italianos radicados na Eslovênia, durante o período compreendido entre os anos 1941 e 1943, eram julgados segundo as disposições da lei penal italiana.[78]

Este princípio é aplicável tanto nas situações em que o agente é o nacional quanto naquelas em que a nacionalidade traz soberania ao país da vítima, denominado princípio da nacionalidade passiva. O Estado protege o seu cidadão, esteja ele em território nacional ou não.

Conclui-se, assim, que o princípio da nacionalidade pode ser dividido em duas espécies, a saber: o da nacionalidade ativa, quando o Estado pune o seu cidadão pela prática de crime cometido no exterior, e o da nacionalidade passiva, quando o Estado pune o agente pela prática de conduta criminosa contra seu cidadão, hipótese em que apenas a nacionalidade da vítima terá importância.[79] Este princípio, visto que subsidiário, aplica-se quando o crime é praticado no exterior e o princípio da territorialidade não é o bastante para alcançá-lo.[80]

Cumpre dizer que se trata de um princípio no Brasil cuja aplicabilidade é condicionada às circunstâncias previstas no artigo 7º, § 2º de nosso Código Penal. Sendo o autor do delito estrangeiro e a vítima brasileira aplicam-se ainda as circunstâncias do § 3º do mesmo dispositivo.

3. Princípio da proteção ou da defesa

O terceiro princípio é o da proteção. Também chamado de princípio da defesa, é o princípio pelo qual a lei do país é aplicada ao fato que atinge interesse nacional, pouco importando o local da conduta, do resultado ou a nacionalidade do agente. Leva-se em consideração a nacionalidade do bem jurídico lesado nos delitos de dano ou exposto a perigo de lesão nos delitos de perigo.

Estipula o artigo 7º, inciso I, do Código Penal, que ficam sujeitos à lei brasileira, embora cometidos no estrangeiro, os autores de crime contra a vida ou a liberdade do

---

[78]BETTIOL, Giuseppe. op. cit., v. 1, p. 188.

[79]Em sentido contrário, René Ariel Dotti afirma que é necessário também que o criminoso seja nacional para que a lei seja aplicada: DOTTI, René Ariel. op. cit.

[80]BITENCOURT, Cezar Roberto. *Tratado de direito penal*: parte geral. 8. ed. São Paulo: Saraiva, 2003. v. 1, p. 115.

Presidente da República, contra o patrimônio ou a fé pública da União, do Distrito Federal, de Estado, de Território, de Município, em empresa pública, de sociedade de economia mista, de autarquia ou fundação instituída pelo Poder Público, contra a administração pública, por quem está a seu serviço, de genocídio, quando o agente for brasileiro ou domiciliado no Brasil.

O § 3º do mesmo artigo também se vale do princípio da personalidade quando diz que a lei brasileira aplica-se também ao crime cometido por estrangeiro contra brasileiro fora do Brasil. Observa-se, contudo, que neste último caso a aplicabilidade fica condicionada às circunstâncias preconizadas pelo próprio artigo.[81]

Para Aníbal Bruno, o determinante para escolha da lei penal é a nacionalidade do titular do bem jurídico ofendido ou ameaçado pelo fato punível, sendo independente a nacionalidade do agente ou o lugar da prática criminal.[82]

Aqui temos a distinção do princípio da personalidade passiva para o da proteção. Este tutela o bem jurídico ofendido ou ameaçado; aquele está diretamente ligado à nacionalidade do sujeito passivo do delito. Estende-se a jurisdição penal estatal para além dos limites territoriais apenas e exclusivamente em razão da nacionalidade do titular do bem jurídico lesado.

Observa-se que não é toda ofensa a bem jurídico que está contemplada neste princípio, pois o Estado, por meio deste permissivo principio lógico protege apenas e tão somente os bens considerados de elevada importância, como a vida e a liberdade do Presidente da República, o crime de genocídio, desde que o agente seja brasileiro e domiciliado no Brasil.

São objetos de tutela apenas os bens ou interesses estatais, coletivos ou comunitários e não de ordem individual.[83]

Também é de se ponderar que em caso de condenação em outro país, o rigor deste princípio é atenuado pelo artigo 8º do Código Penal, que declara que a pena cumprida no

---

[81]DOTTI, René Ariel. op. cit., p. 278.

[82]BRUNO, Aníbal. op. cit., p. 233 *in verbis:* "No princípio real, da defesa, o determinante na escolha da lei penal aplicável é a nacionalidade do titular do bem jurídico ofendido ou ameaçado pelo fato punível, qualquer que seja o lugar em que este se pratique ou a nacionalidade do agente. Com este sistema se protegem, mesmo no estrangeiro, os bens jurídicos do Estado nacional ou de qualquer dos seus súditos."

[83]PRADO, Luiz Regis. op. cit., v. 1, p. 200.

estrangeiro diminui a pena imposta no Brasil, pelo mesmo delito, quando diversas, ou nela é computada quando iguais.[84]

Procura-se, por meio do princípio da proteção, suprir as lacunas deixadas pelos princípios da territorialidade e da personalidade e que, por isso mesmo, deixariam os bens e interesses estatais de maior importância para o Estado, à mercê de condutas delituosas do estrangeiro fora do território nacional.

Fragoso, que denomina este princípio como "princípio da defesa", exemplifica sua aplicabilidade invocando-o como fundamento para o Estado punir o crime de falsificação de moeda perpetrado no estrangeiro.[85]

Talvez seja este o princípio que melhor expresse a soberania estatal ao estender sua jurisdição para delitos praticados fora de seu espaço territorial.

4. Princípio da competência universal

Pelo princípio da competência universal, o estado pode e deve punir o crime, tenha ele sido ou não praticado em seu território e sejam ou não nacionais a vítima ou o agente. Ou seja, pune o delito independentemente da "nacionalidade do agente ou do bem jurídico lesado ou posto em perigo e qualquer que tenha sido o lugar onde tenha sido o fato praticado".[86]

Aplica-se a lei penal a todas as pessoas, onde quer que se encontrem. Seu objetivo é punir um mal a todas as Nações, independentemente do local onde este se deu.

Para Regis Prado, a *iudex deprehensionis* pode ser considerada como um expoente do ideal de justiça com a eliminação da impunidade, mesmo que o crime tenha sido praticado no estrangeiro e contra estrangeiro será julgado pelo país onde o agente se encontre. [87]

---

[84]NORONHA, E. Magalhães. *Direito penal*. São Paulo: Saraiva, 1997. p. 90.
[85]FRAGOSO, Heleno Cláudio. op. cit., p. 132.
[86]Id., loc. cit.
[87]PRADO, Luiz Regis. op. cit., v. 1, p. 201.

Esta teoria, para João Mestieri, se fundamenta na justificativa de que o crime é um mal universal, tendo todos os Estados um interesse em coibir sua prática e proteger os bens jurídicos da lesão provocada pela infração criminal. [88]

Os delitos que são punidos pelo Estado com fundamento neste princípio são os previstos em tratados e convenções subscritas pelo Estado brasileiro e por força dos quais se obrigou a punir. São exemplos o crime de tráfico ilícito de entorpecentes, a pirataria, a destruição ou danificação de cabos submarinos, o tráfico de pessoas, a tortura, entre outros.[89]

O artigo 7º, inciso II, alínea *a*, do Código Penal obriga o Estado brasileiro a punir os agentes pela prática de crimes que, por tratado ou convenção obrigou-se a reprimir, ainda que praticados no exterior, o que respalda ainda mais o princípio da competência universal.

Ariel Dotti nos lembra que este princípio sofreu críticas severas no passado e que ainda hoje encontra ressonância no meio jurídico. Fundam-se tais críticas no fato de que as legislações penais e processuais penais dos diversos Estados possuem inúmeras diferenças; cabe ao juiz aplicar no país onde o criminoso se encontre o direito estrangeiro a ele desconhecido; a colheita da prova sofre dificuldade com burocracias e questões processuais e, por fim, o Estado e a sociedade estarão mais protegidos com a expulsão deste suspeito ou condenado. [90]

Neste mesmo sentido, Fragoso explica que a aplicação deste princípio encontra barreira na diversidade legislativa dos vários países no que diz respeito à matéria penal e, também, por conta das dificuldades decorrentes da quase impossível realização de processos penais em locais distantes do local onde o crime foi praticado.[91]

Pondera o mesmo autor, no entanto, que com a internacionalização dos direitos humanos e o progresso da civilização aumenta a necessidade de se aplicar a lei penal do País onde o criminoso esteja, desconsiderando sua nacionalidade e o local do fato, desde que aquele Estado tenha, por tratado, se obrigado a reprimi-lo. Aduz que as leis penais vão se encaminhando para uma certa uniformidade e a colaboração internacional certamente

---

[88]MESTIERI, João. *Teoria elementar de direito criminal*. Rio de Janeiro: Cadernos Didáticos, 1971. p. 124.
[89]NUCCI, Guilherme de Souza. *Código Penal comentado*. 9. ed. São Paulo: Ed. Revista dos Tribunais, 2008. p. 98.
[90]DOTTI, René Ariel. op. cit., p. 279.
[91]FRAGOSO, Heleno Cláudio. op. cit., p. 133.

acompanha este desenvolvimento das leis contra o crime. Há uma tendência pela formação de um tipo comum de civilização entre as nações modernas, com uma consciência jurídica uniforme, analisando as mesmas necessidades, regras e hábitos da vida social.[92]

É por meio dos tratados e convenções internacionais que a cooperação internacional para o combate aos crimes de repercussão mundial se materializa formalmente.[93]

Aduz Aníbal Bruno, após ponderar que este princípio é também conhecido como "extraterritorialidade absoluta", que se trata do princípio mais amplo e avançado, vez que "apóia a aplicação da lei penal do país onde venha a ser detido o criminoso, seja qual for o lugar em que o crime se pratique ou a nacionalidade do agente ou do titular do bem jurídico violado".[94]

Por este princípio, cada Estado passa a ter uma competência penal universal e sempre será legítima a sua imposição da lei e da ordem com vistas à proteção dos bens jurídicos de interesse nacional e da humanidade como um todo.

A aplicação "extraterritorial das normas penais em caráter absoluto constitui uma das modalidades da cooperação internacional na luta contra a criminalidade"..[95]

Este derradeiro princípio confronta-se diretamente com o princípio da territorialidade, demonstrando uma tendência a, em busca de justiça, aplicar uma jurisdição diversa daquela onde o agente nasceu ou praticou a conduta ou resultado delituoso.

Bettiol afirma que este princípio é reflexo de uma tendência que tem por escopo a criação de um código penal aplicável a todas as nações em resposta à delinqüência, e tem como pressuposto o abandono de legislações penais autônomas. Seria, ainda de acordo com citado autor, uma espécie de sacrifício, pelos Estados, de parte da soberania em matéria legislativa penal.[96]

---

[92]DOTTI, René Ariel. op. cit., p. 279-280.
[93]ROCHA, Fernando A. N. Galvão da. *Direito penal*: curso completo: parte geral. 2. ed. Belo Horizonte: Del Rey, 2007. p. 103.
[94]BRUNO, Aníbal. op. cit., p. 233.
[95]DOTTI, René Ariel. op. cit., p. 280.
[96]BETTIOL, Giuseppe. op. cit., v. 1, p. 188.

5. Princípio da representação ou da bandeira

Como último princípio relacionado à lei penal no espaço, tem-se o princípio da representação ou da bandeira, entendido como o fundamento da aplicação da lei nacional quando o país que deveria punir a conduta delitiva não o faz por qualquer motivo. Sua aplicação fica condicionada a ter o crime sido praticado a bordo de aeronaves ou embarcações nacionais, pois, do contrário, estar-se-ia afrontando a soberania alheia.

Este princípio, utilizável aos casos de não aplicabilidade ao princípio da territorialidade e da extraterritorialida, de tem por finalidade combater a impunidade. A conduta e o resultado ocorridos fora do território nacional, se lá, por qualquer motivo, não forem julgados, mesmo não se enquadrando aos casos de extensão da territorialidade, pelo princípio da representação, serão julgados pelo país representante da embarcação ou aeronave em que a conduta ou o resultado ocorreram.

6. Princípio da extraterritorialidade

Além da territorialidade e de sua extensão, o princípio da extraterritorialidade, sujeita à lei brasileira o agente que pratica crimes no estrangeiro.

As alíneas "a", "b" e "c" do inciso I, do artigo 7º, adotaram o princípio da defesa ou da proteção, levando em conta a nacionalidade do bem jurídico lesado. É o caso, dentre outros, do crime contra o Presidente da República, de lesão ao patrimônio da União, contra agente, em serviço da administração pública.

A alínea "d", do dispositivo em comento, ao tratar do agente de genocídio, adotou o princípio da nacionalidade ou personalidade do agente, sujeitando à lei nacional o agente brasileiro domiciliado no Brasil.

Neste primeiro inciso, esta extraterritorialidade será absoluta. Mesmo que o agente tenha sido absolvido ou condenado no estrangeiro, responderá pela lei brasileira[97].

[97]Código Penal, Art. 7º - Ficam sujeitos à lei brasileira, embora cometidos no estrangeiro: I - os crimes: a) contra a vida ou a liberdade do Presidente da República; b) contra o patrimônio ou a fé pública da União, do Distrito Federal, de Estado, de Território, de Município, de empresa pública, sociedade de economia

O inciso II, do mesmo artigo, trata da extraterritorialidade, sujeitando-se à lei brasileira, aos crimes em que o Brasil, por tratado ou convenção, obrigou-se a reprimir (princípio da justiça penal universal), praticados por brasileiro (princípio da nacionalidade) ou em aeronaves ou embarcações brasileiras, mercantes ou privadas (princípio da bandeira) no estrangeiro, e ali não forem julgados (princípio da representação).

Nestes casos do segundo inciso, só se aplica a lei brasileira, se presentes algumas circunstâncias como a entrada do agente no território nacional, for o fato punível no país em que foi realizado o fato, estar o crime na lista dos casos em que o Brasil autoriza a extradição, não ter sido o agente absolvido, cumprido pena no estrangeiro, nem ter tido sua pena extinta.

Sobre o crime praticado por estrangeiro que se encontra fora da jurisdição brasileira, e cujo país se recusa extraditá-lo, Nucci traz posição inovadora ao defender que mesmo que a nossa lei penal não exija o ingresso do agente em nosso território para processá-lo, não haverá interesse de agir na ação, uma de suas condições. Isto porque, como é cediço, é pressuposto do processo penal válido a citação do acusado e, por óbvio, o Estado que se recusou a processar ou extraditar o seu nacional, pouco provável queira cumprir a carta rogatária para citação. Esta ausência está fundamentada, sobretudo, na utilidade que o processo possa trazer.

Aponta o autor que nos casos de extradição não cabível ou negada não há razão para ser instaurado um processo criminal. Explana que, estando o estrangeiro distante de nosso território, mesmo que iniciado o processo ele deverá ser citado, não havendo extradição possivelmente o país onde ele se encontre também não cumprirá carta rogatória para sua citação. Se cumprida mesmo que o processo continue e ao final seja condenado

---

mista, autarquia ou fundação instituída pelo Poder Público; c) contra a administração pública, por quem está a seu serviço; d) de genocídio, quando o agente for brasileiro ou domiciliado no Brasil; II - os crimes: a) que, por tratado ou convenção, o Brasil se obrigou a reprimir; b) praticados por brasileiro; c) praticados em aeronaves ou embarcações brasileiras, mercantes ou de propriedade privada, quando em território estrangeiro e aí não sejam julgados. § 1º - Nos casos do inciso I, o agente é punido segundo a lei brasileira, ainda que absolvido ou condenado no estrangeiro§ 2º - Nos casos do inciso II, a aplicação da lei brasileira depende do concurso das seguintes condições: a) entrar o agente no território nacional; b) ser o fato punível também no país em que foi praticado; c) estar o crime incluído entre aqueles pelos quais a lei brasileira autoriza a extradição; d) não ter sido o agente absolvido no estrangeiro ou não ter aí cumprido a pena; e) não ter sido o agente perdoado no estrangeiro ou, por outro motivo, não estar extinta a punibilidade, segundo a lei mais favorável. § 3º - A lei brasileira aplica-se também ao crime cometido por estrangeiro contra brasileiro fora do Brasil, se, reunidas as condições previstas no parágrafo anterior: a) não foi pedida ou foi negada a extradição; b) houve requisição do Ministro da Justiça. (BRASIL. *Código Penal.* 13. ed. São Paulo: Ed. Revista dos Tribunais, 2011).

sua aplicabilidade está fadada ao insucesso, devendo aguardar o prazo prescricional. Se citado por edital, da mesma forma o processo acabará em prescrição, embora a lei aponte que tal prazo prescricional deva ficar suspenso, a doutrina não tem admitido que esta situação seja eterna. Pela inexistência de utilidade, o magistrado pode rejeitar a denúncia ou queixa, pela falta de interesse de agir. Não se tem notícia de nenhum processo como este proposto com resultado satisfatório.[98]

O parágrafo 3º do artigo em tela determinou ainda a aplicação da lei brasileira ao crime praticado por estrangeiro contra brasileiro, desde que reunidas as condições apresentadas pelo § 2º, do artigo 7º, do Código Penal e não ter sido pedida ou ter sido negada sua extradição, ou tenha havido requisição do Ministro da Justiça (princípio da nacionalidade passiva).

Sobre a legitimidade da extraterritorialidade, Reale Júnior considera possuir um significado penal e processual penal, já que a prevalência extraterritorial da lei nacional importa persecução do agente perante a Justiça nacional. A disciplina da extraterritorialidade é de caráter misto, ou seja, penal e processual penal, não tendo valor a incidência da lei brasileira se não houver legitimidade para processar o agente no Brasil e aplicar nossa legislação.[99]

[98]NUCCI, Guilherme de Souza. op. cit., p. 97.
[99]REALE JÚNIOR, Miguel. op. cit., p. 111.

CAPÍTULO IV. CRIMES INFORMÁTICOS

1. Conceito

Trouxe a *internet* um novo mundo, denominado digital. Nele as pessoas navegam, se comunicam e de um mundo virtual praticam condutas e consequências em um mundo real. O direito, conforme já escrito no tema "A *internet* e o Direito" deve aparecer para ditar normas e punir seus infratores.

Se não a mais importante interligação entre o direito e a informática, o direito penal figura entre as principais interfaces que podem ocorrer em meio a estas duas áreas do conhecimento humano.

A *internet* não trouxe ao cotidiano apenas benefícios, mas também possibilitou novas ferramentas para práticas criminosas, tanto as tradicionais, já tipificadas no Direito Penal positivo, quanto aquelas que necessitam de nova legislação para, ao punir os infratores, tentar coibi-los.[100]

Escrevem Alexandre Daoun e Renato Opice Blum[101] que o estudo a respeito dos crimes cibernéticos é apaixonante. O infinito do tempo, através do avanço da tecnologia, nos dá uma fonte inesgotável de informações. Quando se fala em crime informático, unindo direito e informática, se fala em um mundo de constante mutabilidade em princípios, conceitos e ideias.

O crime informático, espécie de crime, é conceituado como uma ação típica, antijurídica e culpável, ao qual o termo "informático" consubstancia apenas um *plus.*[102]

Ivette Senise Ferreira reconhece como crime da informática "toda ação típica, antijurídica e culpável cometida contra ou pela utilização de processamento automático de dados ou sua transmissão".[103]

---

[100]DAOUN, Alexandre Jean. Crimes informáticos. In: BLUM, Renato M. S. Opice et al. (Coord.). op. cit., p. 203.
[101]DE LUCCA, Newton; SIMÃO FILHO, Adalberto (Coords.). op. cit., v. 2, p. 129.
[102]DAOUN, Alexandre Jean. op. cit., p. 206.
[103]FERREIRA, Ivette Senise. A criminalidade informática. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto (Coords.). op. cit., v. 2, p. 210.

Acertada a denominação da autora muito semelhante à da OECD e aceita pelo Conselho da Europa e das Comunidades Europeias que define o delito em comento como "qualquer comportamento ilegal, aético ou não autorizado envolvendo processamento automático de dados e/ou transmissão de dados".

O autor Ferreira Lima adota a nomenclatura Crimes de Computador ao argumento de que o computador é a ferramenta básica para a prática delitiva. Assim, também devem ser nomeados os crimes que de qualquer forma têm a utilização do computador para a facilitação do alcance do resultado almejado.[104]

Túlio Vianna prefere a terminologia crimes informáticos, ao argumento de que o adjetivo informático é já o utilizado para denominar a ciência que estuda os dados de um computador, suas formas de transmissão, armazenamento, processamento e interceptação.[105]

São ainda definidos como crimes de informática por serem praticados por meio do uso de computadores.[106]

Entendemos imprecisa a definição "crimes de computador". Nos dias atuais, o delito informático não está mais restrito ao uso de um tradicional computador com seu disco rígido, teclado e visor, mas pode ser praticado por diversos outros aparelhos ligados à *internet* como telefone fixo ou móvel, *ipad*, *laptop*, *notebook*. Mais adequada, portanto, a nomenclatura "crimes informáticos".

Assim, temos que a informática não modificou, conforme salientado acima, o quanto preconizado pela teoria do crime, mas trouxe à baila um poderoso meio de consecução de condutas, delitivas ou não – o meio digital.

Como um influente meio de se levar a ação humana a locais até então não imaginados, o agente delitivo pode ter acesso a bens jurídicos penalmente tutelados que não se encontravam fisicamente à sua disposição.

---

[104]LIMA, Paulo Marco Ferreira. *Crimes de computador e segurança computacional*. Campinas, SP: Millennium Ed., 2005. p. 24.
[105]VIANNA, Túlio Lima. *Fundamentos de direito penal informático.* Rio de Janeiro: Forense, 2003. p. 10.
[106]José Caldas define como "crimes de informática" GOIS JR, José Caldas. *O direito na era das redes*: a liberdade e o delito no ciberespaço. Bauru, SP: EDIPRO, 2001. p. 119.

Mas não é só. Além de um novo meio de consecução de condutas, os meios digitais também se transformaram no próprio bem juridicamente tutelado, merecedores de reprimenda quando lesados.

2. Evolução

Com o surgimento do computador e da *internet,* surgiu o espaço cibernético e com ele uma nova modalidade criminosa que foi denominada por todo o mundo como crime eletrônico, digital, informático, cibernético, *cybercrime*, e-crime ou crime.com.

Neste espaço virtual milhares de computadores de diferentes países do planeta estão interligados, por linha telefônica, satélite, fibra ótica ou banda larga, não existindo nenhum controle externo sobre esta comunicação, desde que não ilícita, atendendo ao quanto preconizado pelo direito privado, de que as condutas não proibidas estão autorizadas.

Com isto, o crescimento de condutas ilícitas, estas sim proibidas no mundo informático, vem alcançando números exorbitantes. Segundo dados do *emarketer* apresentados em 2006, tínhamos no planeta mais de 1 bilhão de usuários de *internet*[107]. No Brasil este número superava os 22 milhões[108].

Em relatório[109] divulgado pelo chefe da União Internacional de Telecomunicações (UIT) Hamadun Touré, em vinte e seis de janeiro de 2011 o planeta terra superou o número de dois bilhões de usuários de *internet*. Este crescimento se deu principalmente ao aumento do número de usuários da *internet* por telefone celular. Em 2000, havia 500 milhões de assinantes de celulares e 250 milhões de usuários de *internet*, no início de 2011 o número destes usuários de telefonia móvel subiu para 5 bilhões.

Segundo relatório publicado pela INDEX MUNDI[110], atualizado até janeiro de 2009, através da CIA. WORLD FACT BOOK, o Brasil passou de vinte e dois milhões de

---

[107]IDG NOW. Disponível em: <http://idgnow.uol.com.br/internet>. Acesso em: 04 jun. 2006.

[108]TELECO. Inteligência em Telecomunicações. Disponível em: <http://www.teleco.com.br/internet.asp>. Acesso em: 04 jun. 2006.

[109]NÚMERO de usuários de internet no mundo alcança os 2 bilhões. Diponível em: <http://g1.globo.com/tecnologia/noticia/2011/01/numero-de-usuarios-de-internet-no-mundo-alcanca-os-2-bilhoes.html>. Acesso em: 25 abr. 2011.

[110]INDEX MUNDI. Comparação entre países. *Número de servidores internet*. Disponível em: <http://www.indexmundi.com/g/r.aspx?v=140&l=pt>. Acesso em: 11 mar. 2011.

usuários em 2009 para cinquenta milhões, ocupando a quinta posição de usuários da *internet*, vindo atrás China, Estados Unidos da América, Japão e Índia, respectivamente, tendo a China a impressionante quantidade de duzentos e cinquenta e três milhões de usuários.

Posição	País	Número de usuários da Internet
1	China	253,000,000
2	Estados Unidos	223,000,000
3	Japão	88,110,000
4	Índia	80,000,000
5	Brasil	50,000,000
6	Alemanha	42,500,000
7	Reino Unido	40,200,000
8	Coreia do Sul	35,590,000
9	Itália	32,000,000
10	Rússia	30,000,000
11	Canadá	28,000,000
12	Irã	23,000,000
13	México	22,812,000
14	Espanha	19,690,000
15	Vietname	17,870,000
16	Paquistão	17,500,000
17	Polônia	16,000,000
18	Malásia	15,868,000
19	Países Baixos	15,000,000
20	Taiwan	14,760,000
21	Tailândia	13,416,000
22	Turquia	13,150,000
23	Indonésia	13,000,000
24	Colômbia	12,100,000
25	Romênia	12,000,000
26	Austrália	11,240,000

27	Nigéria	10,000,000
28	Ucrânia	10,000,000
29	Argentina	9,309,000
30	Egito	8,620,000
31	Peru	7,636,000
32	Marrocos	7,300,000
33	Suécia	7,000,000
34	Arábia Saudita	6,200,000
35	Bielorrússia	6,000,000
36	Venezuela	5,720,000
37	Chile	5,570,000
38	Filipinas	5,300,000
39	Bélgica	5,220,000
40	África do Sul	5,100,000
41	Suíça	4,610,000
42	República Checa	4,400,000
43	Áustria	4,277,000
44	Hungria	4,200,000
45	Hong Kong	3,961,000
46	Noruega	3,800,000
47	Finlândia	3,600,000
48	Portugal	3,549,000
49	Dinamarca	3,500,000
50	Argélia	3,500,000
51	Síria	3,470,000
52	Nova Zelândia	3,360,000
53	Cingapura	3,105,000
54	Quênia	3,000,000
55	Grécia	2,540,000
56	Eslováquia	2,350,000
57	Emirados Árabes Unidos	2,300,000
58	Usbequistão	2,100,000

59	Uganda	2,000,000
60	Israel	2,000,000
61	Croácia	1,995,000
62	Cazaquistão	1,901,000
63	Bulgária	1,899,000
64	Tunísia	1,722,000
65	Irlanda	1,708,000
66	República Dominicana	1,677,000
67	Equador	1,549,000
68	Costa Rica	1,500,000
69	Jamaica	1,500,000
70	Sudão	1,500,000
71	Zimbabué	1,351,000
72	Lituânia	1,333,000
73	Guatemala	1,320,000
74	Eslovênia	1,300,000
75	Letônia	1,177,000
76	Jordânia	1,127,000
77	Bósnia e Herzegovina	1,055,000
78	Azerbaijão	1,036,000
79	Bolívia	1,000,000
80	Haiti	1,000,000
81	Porto Rico	1,000,000
82	Uruguai	968,000
83	Líbano	950,000
84	Kuwait	900,000
85	Senegal	820,000
86	Estônia	780,000
87	Sri Lanca	771,700
88	Quirguizistão	750,000
89	Moldávia	700,000
90	Salvador	700,000

91	Macedônia	685,000
92	Gana	650,000
93	Afeganistão	580,000
94	Panamá	525,200
95	Zâmbia	500,000
96	Bangladeche	500,000
97	Albânia	471,200
98	Trindade e Tobago	430,800
99	Honduras	424,200
100	Tanzânia	400,000
101	Camarões	370,000
102	Geórgia	360,000
103	Catar	351,000
104	Luxemburgo	345,000
105	Omã	340,000
106	Maurícia	340,000
107	Nepal	337,100
108	Mongólia	320,000
109	Togo	320,000
110	Iémen	320,000
111	Macau	300,000
112	Costa do Marfim	300,000
113	Etiópia	291,000
114	Montenegro	280,000
115	Paraguai	280,000
116	Líbia	260,000
117	Barém	250,000
118	Congo-Kinshasa	230,400
119	Islândia	202,300
120	Moçambique	200,000
121	Brunei	199,532
122	Guiana	190,000

123	Armênia	172,800
124	Barbados	160,000
125	Malta	158,000
126	Nicarágua	155,000
127	Benim	150,000
128	Gabão	145,000
129	Malavi	139,500
130	Eritreia	120,000
131	Baamas	120,000
132	Madagáscar	110,000
133	Papua-Nova Guiné	110,000
134	Santa Lúcia	110,000
135	Namíbia	101,000
136	Gâmbia	100,200
137	Angola	100,000
138	Mali	100,000
139	Laos	100,000
140	Ruanda	100,000
141	Somália	98,000
142	Burquina Faso	80,000
143	Nova Caledônia	80,000
144	Botsuana	80,000
145	Fiji	80,000
146	Polinésia Francesa	75,000
147	Congo-Brazzaville	70,000
148	Camboja	70,000
149	Lesoto	70,000
150	Turquemenistão	70,000
151	Guame	65,000
152	Chade	60,000
153	Burúndi	60,000

154	Antígua e Barbuda	60,000
155	Andorra	58,900
156	São Vicente e Granadinas	57,000
157	Iraque	54,000
158	Groenlândia	52,000
159	Guiné	50,000
160	Bermudas	48,000
161	Suriname	44,000
162	Suazilândia	42,000
163	Butão	40,000
164	Birmânia	40,000
165	Níger	40,000
166	Cabo Verde	37,000
167	Guiné-Bissau	37,000
168	Guernsey	36,000
169	Faroé	34,000
170	Maldivas	33,000
171	Belize	32,000
172	Seicheles	32,000
173	Ilhas Virgens Americanas	30,000
174	Mauritânia	30,000
175	Jersey	27,000
176	Dominica	26,500
177	Aruba	24,000
178	Granada	23,000
179	São Tomé e Príncipe	23,000
180	Listenstaine	22,000
181	Ilhas Caimão	22,000
182	Comores	21,000
183	Mônaco	20,000
184	Tajiquistão	19,500

185	Vanuatu	17,000
186	São Marinho	15,400
187	Micronésia	15,000
188	República Centro-Africana	13,000
189	Serra Leoa	13,000
190	Jibuti	11,000
191	Marianas do Norte	10,000
192	São Cristóvão e Neves	10,000
193	Tonga	8,400
194	Samoa	8,000
195	Guiné Equatorial	8,000
196	Ilhas Salomão	8,000
197	Gibraltar	6,200
198	Ilhas Virgens Britânicas	4,000
199	Ilhas Cook	3,600
200	Anguila	3,000
201	Ilhas Marshall	2,200
202	Antilhas Neerlandesas	2,000
203	Quiribáti	2,000
204	Ilhas Falkland	1,900
205	Tuvalu	1,300
206	Timor Leste	1,200
207	Libéria	1,000
208	Niue	900
209	Wallis e Futuna	900
210	Ilha Norfolk	700
211	Ilha do Natal	464
212	Nauru	300
213	Vaticano	93
214	West Bank	0

215	Santa Helena	0
216	Gaza Strip	0
217	França	0
218	Cuba	0

Denota-se um crescimento da quantidade de internautas no planeta, desenvolvendo a cada dia uma interligação cada vez maior entre nossos continentes. Este crescimento traz com ele os conflitos, antes regionais agora mundiais.

Da mesma forma, além dos internautas, os domínios[111] vêm sofrendo um grande crescimento. Segundo gráfico da CETIC, os domínios surgiram em nosso país em janeiro de 1996 e passaram de 851 a, em março de 2011, 2412455. Denota-se neste gráfico apresentado abaixo que, com o passar dos anos, o crescimento anual é cada vez mais acentuado.[112]

	1996	**1997**	**1998**	**1999**	**2000**	**2001**	**2002**	**2003**
Jan	851	7.998	27.592	70.882	163.659	369.857	417.610	425.121
Fev	1.006	8.684	30.268	74.517	184.320	379.470	426.005	438.757
Mar	1.280	9.901	33.696	81.048	209.675	391.592	423.468	450.441
Abr	1.823	10.853	36.362	87.131	231.539	402.844	413.312	464.186
Mai	2.283	11.873	39.746	93.340	254.986	392.303	408.729	479.295
Jun	2.862	13.444	43.461	100.212	274.674	403.511	406.662	490.873
Jul	3.769	15.007	46.512	108.192	292.539	416.277	408.416	507.809
Ago	4.512	16.841	51.328	115.145	310.955	430.227	417.653	509.919
Set	5.169	19.521	55.100	123.955	325.297	442.172	430.927	506.236
Out	5.883	21.508	58.634	132.720	338.517	422.719	434.140	513.045
Nov	6.678	23.495	63.850	142.373	349.750	433.849	443.803	527.664
Dez	7.507	25.802	67.777	151.278	359.670	447.916	413.365	539.274

[111]Domínio: Conjunto de endereços na Internet organizado de forma hierárquica. O domínio superior identifica a área geográfica como ".br ou .edu". Um nome domínio é a versão legível do endereço IP como www.uol.com.br. DICIONÁRIO UOL Tecnologia. Disponível em: <HTTP://tecnologia.uol.com.br/dicionarios>/. Acesso em: 16 abr. 2011.

[112]CETIC.br. *Evolução do números de domínios*. Disponível em: <http://www.cetic.br/dominios>. Acesso em: 25 abr. 2011.

	2004	2005	2006	2007	2008	2009	2010	2011
Jan	558.408	715.152	866.969	1.037.296	1.240.931	1.553.940	1.968.709	2.338.849
Fev	574.758	723.933	880.782	1.052.794	1.251.231	1.571.593	1.990.796	2.367.536
Mar	594.221	738.270	899.044	1.074.052	1.273.830	1.608.351	2.026.237	2.412.455
Abr	611.005	753.110	912.512	1.089.609	1.300.184	1.651.412	2.068.022	
Mai	626.784	767.997	928.149	1.112.567	1.342.327	1.692.145	2.102.667	
Jun	639.686	783.352	944.051	1.135.134	1.374.644	1.725.447	2.138.509	
Jul	657.458	796.837	957.979	1.151.856	1.415.968	1.769.918	2.175.258	
Ago	671.654	810.095	978.129	1.175.688	1.449.059	1.804.602	2.207.687	
Set	682.512	828.508	993.504	1.193.293	1.473.396	1.848.161	2.238.723	
Out	693.385	838.639	1.006.111	1.212.183	1.497.893	1.909.349	2.276.382	
Nov	698.612	850.228	1.021.431	1.227.703	1.527.274	1.934.935	2.295.768	
Dez	708.947	858.596	1.029.103	1.230.907	1.533.642	1.949.461	2.319.188	

O Brasil vem crescendo mundialmente não só quanto ao número de usuários e domínios, mas também em outras áreas ligadas à informática. Neste sentido temos a evolução do número de *hosts*[113] no Brasil, segundo relatório abaixo da CETIC[114], tendo como fonte a Network Wizards – saímos de 800 em janeiro de 1995 para 21.121.168 em janeiro de 2011. Com isto saímos da 26ª posição mundial em quantidade de *hosts* para a quarta posição em 2011.

	Janeiro	Julho
1995	800	11.576
1996	20.113	46.854
1997	77.148	68.685
1998	117.200	163.890
1999	215.086	310.138
2000	446.444	662.910

[113]Host: Computador ligado permanentemente à Rede, que mantém um repositório de serviços para outros computadores na internet. Também é chamado de nó, *in* DICIONÁRIO UOL Tecnologia. Disponível em: <HTTP://tecnologia.uol.com.br/dicionarios>/. Acesso em: 16 abr. 2011.

[114]CETIC.br. *Evolução do número de hosts do Brasil*. Disponível em: <http://cetic.br/hosts/index.htm>. Acesso em: 25 abr. 2011.

2001	876.596	1.025.067
2002	1.644.575	1.988.321
2003	2.237.527	---
2004	3.163.349	3.485.773
2005	3.934.577	4.392.693
2006	5.094.730	6.508.431
2007	7.422.440	8.264.709
2008	10.151.592	9.572.594
2009	14.678.982	15.929.346
2010	17.786.552	19.315.960
2011	21.121.168	---

Sobre esta recente realidade e suas consequentes dificuldades, Maria Eugênia Finkelstein[115] alerta que o início da exploração comercial na *internet*, em 1993, trouxe novas formas de condutas criminosas.

Estas condutas utilizam-se de meios antes desconhecidos, dificultando o rastreamento dos agentes criminosos que se aproveitam da *internet* para alcançar o resultado pretendido. Nesta nova era encontramos os crimes informáticos, delitos praticados por agentes que, muitas vezes, não são sequer identificados.

Nesta era digital, novas ferramentas foram postas à disposição da ciência e do conhecimento, mas também tiveram acesso a elas os criminosos, que as usaram como meio para a prática de delitos até então inexistentes.

Discute-se, com a evolução da informática, se o direito, mais precisamente o penal, já está adequado às novas condutas ilícitas ali praticadas ou se necessita de alterações.

A teoria do direito penal nos mostra, há muito, que a definição daquelas condutas que merecem tipificação respeitam a decisão política de quais bem jurídicos devem ser tutelados, sempre levando em conta ser o direito penal a *ultima ratio.*

O exegeta, então, deve analisar se o bem jurídico lesado pela conduta realizada através dos sistemas eletrônicos já é tutelado pela norma existente, caso em que os

[115]FINKELSTEIN, Maria Eugênia. op. cit., p. 403.

sistemas informáticos configurariam apenas um novo meio de consecução, ou se o próprio bem jurídico é novo ao sistema.

3. Finalidade delitiva

Passados os anos, os crimes informáticos inicialmente praticados com a finalidade de invadir a intimidade de terceiros, quer pessoas físicas quer jurídicas ou de ofender a honra das pessoas, passaram a dividir atenção com os crimes em que o infrator, por meio do computador, em qualquer lugar do mundo, lesa qualquer bem jurídico, inclusive a própria vida.

Hoje a finalidade é, prioritariamente, financeira, tendo como grande incentivo às práticas delitivas a fragilidade dos sistemas informáticos e a limitada e algumas vezes inapropriada legislação a respeito.

No entanto, os crimes informáticos não se resumem a crimes financeiros. A *internet* é também utilizada por pessoas das mais diversas culturas e psicopatias. Nos dias atuais, pratica-se nela com frequência quase todos os crimes praticados antes da era informática.

Alguns infratores encontraram na *internet* um espaço apto a praticar a pornografia infantil, seja trocando imagens e vídeos contendo crianças nuas, seja aliciando-as para a prostituição.

Os especialistas, no início, tinham como finalidade delitiva, na maioria dos casos, a vaidade. Invadir um sistema informático de grande segurança era como uma espécie de troféu, mostrando a terceiros suas habilidades.

Hoje os especialistas invadem sistemas informáticos proibidos, em grande escala, tentando obter uma vantagem econômica com tal informação, quer negociando com a própria vítima invadida, quer por terceiros que com aquela invasão obtém vantagens até ali inalcançáveis.

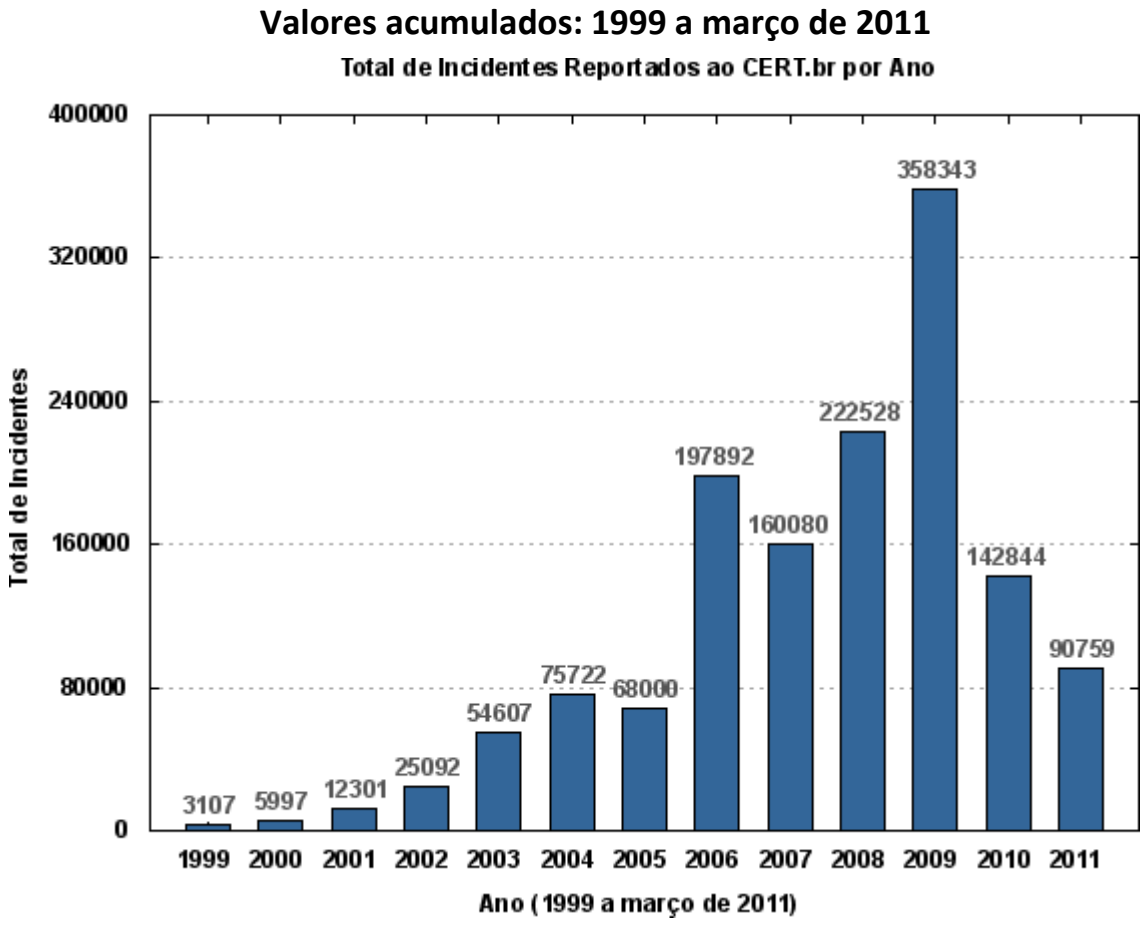
Temos que os crimes cibernéticos não estão mais restritos ao alcance dos *trackers* – podem ser praticados por qualquer pessoa, mesmo que não se trate de grande conhecedora de informática. Com o fácil acesso e manuseio da informática, qualquer pessoa, através dela, é capaz de, em fração de segundos, utilizando um aparelho conectado na rede, enviar

e-mails a terceiros ofendendo a honra de outrem, praticando, pela informática, crime contra a honra.

4. Seu crescimento

Desde seu surgimento a *internet* vem ganhando espaço em nossas ocupações habituais e profissionais. Acompanhando esta evolução está a criminalidade por meio dela e contra ela praticada.

A CERT[116] (Computer Emergency Response Team) apresenta relatório dos ataques na *internet*, reportados a ela, de 1999 até o primeiro trimestre de 2011. Este número certamente bem menor que o real, salta de 3107 ataques no ano de 1999 para 90759, só no primeiro semestre de 2011:



[116]ESTATÍSTICAS dos Incidentes Reportados ao CERT.br. Disponível em: <http://www.cert.br/stats/incidentes>. Acesso em: 25 abr. 2011.

Segundo relatório da OECD[117] (Organisation for Economic Co-operation and Development) chamado "Norway Information Security", os crimes cibernéticos têm aumentado nos últimos anos, tornando-se uma ameaça à sociedade.

Este mesmo relatório aponta os quatro principais fatores deste crescimento: a sofisticação das ferramentas de ataque; as novas tecnologias trazendo novas vulnerabilidades; as infraestruturas importantes tornadas dependentes da segurança dos sistemas de informação e da rede e, por fim, o aumento considerável do objetivo do crime cibernético.

De acordo com o último relatório feito pela Symantec, o 14º sobre ameaças de segurança na *internet*, em 2008 foram detectados mais de 1,6 milhões de novos códigos maliciosos.[118]

A quantidade de códigos maliciosos detectados apenas em 2008 corresponde a mais de 60% do total de códigos identificados em todos os 13 relatórios anteriores. Ainda de acordo com a Symantec, a identificação destes códigos maliciosos permitiu, naquele ano, bloquear aproximadamente 245 milhões de ataques por mês em todo o mundo.

Neste respeitado relatório a *web* continua sendo, no ano de 2008, a maior fonte de novas infecções. Informa ainda que, a cada dia, os criminosos digitais utilizam-se dos *kits* customizados, denominados "toolkits", com a finalidade de criar e disseminar novos códigos maliciosos. Detectou-se ainda que, noventa por cento destas ameaças visavam subtrair informações confidenciais dos usuários, visando registrar o que está sendo digitado no teclado (keytroke-logging). Destes noventa por cento, setenta e seis representavam ameaças visando a obtenção de dados confidenciais, superiores aos setenta e dois por cento registrados no ano de 2007.[119]

A respeito, Ivette Senise Ferreira[120] explana que a crescente informatização das inúmeras atividades desenvolvidas na sociedade veio a colocar instrumentos, até então inexistentes, nas mãos dos criminosos, cujo alcance ainda não foi avaliado com precisão.

---

[117]OECD. Disponível em: <http://www.oecd.org/home/0,3305,en_2649_201185_1_1_1_1_1,00.html>. Acesso em: 06 jan. 2010.

[118]SYMANTEC. Relatório da Symantec sobre ameaças de segurança na internet detecta que atividade maliciosa continua a crescer em velocidade recorde. Disponível em: <http://www.symantec.com/pt/br/about/news/release/article.jsp?prid=20090414_01>. Acesso em: 06 jan. 2010.

[119]Id. Ibid.

[120]FERREIRA, Ivette Senise. op. cit., p. 207.

Isto se deve ao surgimento diário de novas modalidades de lesões aos mais variados bens e interesses que cabe ao Estado tutelar. Com isto surge uma criminalidade específica da informática, com tendência a aumentar este novo campo quantitativamente e qualitativamente, além de aperfeiçoar seus métodos de execução.

Pouco mais de cinquenta por cento dos crimes ocorridos na *internet* estavam ligados a fraudes bancárias, segundo dados colhidos no site da CERT, no terceiro trimestre de 2005.[121]

O Manual das Nações Unidas, preocupado com este novo campo para a prática delitiva, mormente pela dependência humana desta tecnologia, aponta que

> The burgeoning of the world of information technologies has, however, a negative side: it has opened the door to antisocial and criminal behavior in ways that would never have previously been possible. Computer systems offer some new and highly sophisticated opportunities for law-breaking, and they create the potential to commit traditional types of crimes in non-traditional ways. In addition to suffering the economic consequences of computer crime, society relies on computerized systems for almost everything in life, from air, train and bus traffic control to medical service coordination and national security. Even a small glitch in the operation of these systems can put human lives in danger. Society's dependence on computer systems, therefore, has a profound human dimension. The rapid transnational expansion of large-scale computer networks and the ability to access many systems through regular telephone lines increases the vulnerability of these systems and the opportunity for misuse or criminal activity. The consequences of computer crime may have serious economic costs as well as serious costs in terms of human security

O citado relatório apurou ainda que o Brasil ocupa, na América Latina, o primeiro lugar em termos de atividade maliciosa, o que corresponde a 34% de toda a atividade assim entendida na região.

Tanto os crimes comuns praticados por meio de um computador, em rede, denominados crimes informáticos impróprios, quanto os praticados contra o computador ou dados abertos por ele ou nele contidos, conhecidos como próprios, têm aumentado vertiginosamente nos últimos tempos.

---

[121]ESTATÍSTICAS dos Incidentes Reportados ao CERT.br. Disponível em: <http://www.cert.br/stats/incidentes>. Acesso em: 25 abr. 2011.

No ano de 2008, a América Latina já era responsável por doze por cento dos *spams* detectados em nível mundial. O Brasil, Argentina, Colômbia, Chile e México são os países que mais se destacam na detecção destes *spams*.[122]

Segundo informativo da Secretaria da Fazenda de São Paulo, já em 2005, a lucratividade virtual superou a do narcotráfico. As drogas ilícitas movimentaram cem bilhões de dólares enquanto que as fraudes *on-line* totalizaram prejuízos da ordem de cento e cinco bilhões de dólares. O informativo CAT 19 nº 63, publicado pela mesma Secretaria da Fazenda, registrou que a pirataria acompanha os mesmos números, estes já superiores ao do narcotráfico. O comércio ilegal vem se expandindo na *internet*. Alertou mencionado informativo da inexistência de panorama otimista no tocante à utilização de transações eletrônicas e da impotência do Estado face a este crime. [123]

5. Medidas preventivas

Um dos grandes passos a serem dados contra a criminalidade informática é a prevenção. Determinadas medidas, se adotadas pelos usuários da rede, podem impedir que a criminalidade alcance seu resultado. Tão relevante quanto a adoção destas medidas está a sua própria divulgação e sem ela o usuário não saberá como se proteger deste mundo ainda desconhecido.

A ONU, em relatório elaborado em Genebra, pela ITU (União Internacional para Telecomunicações), em dezembro de 2006, alertou sobre o crescente furto qualificado de dados na *Internet*. Enfatizou que se trata de uma crise mundial e que o roubo de senhas e identidades na *web* vem crescendo em ritmo acelerado, podendo colocar em crise os negócios realizados em operações eletrônicas do e-GOV[124].

---

[122]SYMANTEC. Relatório da Symantec sobre ameaças de segurança na internet detecta que atividade maliciosa continua a crescer em velocidade recorde, cit.

[123]SANTOS, Coriolano Aurélio Almeida Camargo. Atual cenário dos crimes cibernéticos no Brasil. *OAB/São Paulo*. Disponível em: <http://www2.oabsp.org.br/asp/comissoes/sociedade_informacao/artigos/crimes_ciberneticos.pdf>. Acesso em: 08 jan. 2010.

[124]SAFER NET. Disponível em: <http://www.denunciar.org.br/twiki/bin/view/SaferNet/WebHome>. Acesso em: 08 jan. 2010.

Em 2008, foi publicado pela Symantec[125] relatório sobre ameaças de segurança na *internet*. Nele uma relação de vários códigos maliciosos foi responsável pelo bloqueio de 245 milhões de ataques por mês na *internet* em todo o planeta terra.

Neste ponto nosso país saiu na frente, pois no início de 2005, o Instituto Nacional de Criminalística da Polícia Federal em Brasília já despontava perante a comunidade científica internacional como um dos mais modernos e completos do mundo (INC), apto a coibir as ações criminosas praticadas na *web*[126]. De iniciativa privada temos a criação da SaferNet Brasil, organização não governamental, que através da Central Nacional de Denúncias de Crimes Cibernéticos, em parceria com o Ministério Público Federal, oferece à sociedade brasileira e à comunidade internacional um serviço anônimo de recebimento, processamento, encaminhamento e acompanhamento *on-line* de denúncias sobre qualquer crime ou violação aos Direitos Humanos praticado através da *internet*[127].

Visando orientar o usuário, foi criada a Cartilha de Segurança da *Internet*, com recomendações e conselhos de como o usuário pode aumentar a sua segurança, disponibilizada pelo centro de estudos, com respostas e tratamentos de incidentes de segurança no Brasil[128].

Orlando Ruiz, perito criminal da Superintendência da Polícia Técnico-Científica de São Paulo, visando o combate à criminalidade, aponta necessidade de uma maior integração entre governo, usuários e a iniciativa privada.[129]

Ainda neste sentido, o Ministério Público Federal Paulista publicou, em abril de 2006, o Manual Prático de Investigações de Crimes Cibernéticos. Neste Manual, um grupo de Procuradores da República do Estado de São Paulo desenvolveu uma cartilha trazendo ao leitor informações sobre o funcionamento da *internet*, crimes cibernéticos e sua investigação, *websites*, *e-mails*, *softwares*, salas de bate papo (*chat*), *Orkut*, competência jurisdicional, responsabilidade dos provedores, jurisprudência, modelos de peças

[125]SYMANTEC. Relatório da Symantec sobre ameaças de segurança na internet detecta que atividade maliciosa continua a crescer em velocidade recorde, cit.
[126]SAFER NET. Disponível em: <http://www.denunciar.org.br/twiki/bin/view/SaferNet/WebHome>. Acesso em: 08 jan. 2010.
[127]Id. Ibid.
[128]CERT.br. *Cartilha de Segurança para a Internet*. Disponível em: <http:/cartilha.cert.br>. Acesso em: 26 abr. 2011.
[129]SAFER NET. Disponível em: <http://www.denunciar.org.br/twiki/bin/view/SaferNet/WebHome>. Acesso em: 08 jan. 2010.

processuais, endereços úteis, acordos celebrados pela Procuradoria em matéria de *internet* e a Convenção sobre cibercriminalidade.

No Brasil denota-se um avanço no combate à criminalidade informática. Foram criadas delegacias e núcleos de investigações especializados, tais como: DIG-DEIC – 4ª Delegacia de Repressão a Crimes de Informática em São Paulo, SP, DERCIFE (Delegacia Especializada de Repressão a Crimes contra Informática e Fraudes Eletrônicas), em Belo Horizonte MG; DRCI – Delegacia de Repressão aos Crimes de Informática, no Rio de Janeiro, RJ.[130]

No âmbito da Polícia Federal, a perícia de informática iniciou-se em primeiro de novembro de 1995. Em 1996 foi criada a Unidade de Perícia de Informática da Polícia Federal. Esta Unidade, no ano de 2003, recebeu a denominação atual de SEPFIN (Serviço de Perícia em Informática). A prevenção, aliada à legislação mundial em consonância com a nova realidade do mundo virtual, é uma das mais eficazes maneiras de se evitar o crime informático.

6. Classificação

A doutrina, para melhor analisar o crime informático, vem dividindo-o em próprio ou impróprio e puro ou impuro.

Cumpre ressaltar que antes de pensar em denominações acerca dos crimes praticados por intermédio ou contra o computador ou qualquer aparelho conectado à *internet*, qualquer denominação será espécie de um grupo maior que a contemplará, o qual será denominado "crime".

Diante do princípio da reserva legal, a conduta reprovável não será crime se assim não dispuser a lei.

Desta forma, é de se retomar o que já foi dito alhures, a saber: muitas condutas praticadas contra o computador e por meio do computador são fraudulentas e atentam com vigor contra a ordem jurídica, mas devem, até que se tipifiquem criminalmente, ser

[130]SAFER NET. Disponível em: <http://www.denunciar.org.br/twiki/bin/view/SaferNet/WebHome>. Acesso em: 08 jan. 2010.

reprovadas por meio da tutela civil dos direitos, pois inaplicável a analogia penal *in malam partem.*

Partimos do pressuposto de que as definições doutrinárias que se apresentam, os conflitos de leis que se procura dirimir e todas as questões tratadas neste trabalho pressupõem ilícitas no âmbito criminal as condutas comentadas.

Preferimos, para as nomenclaturas acima tratadas, a distinção "crimes informáticos próprios e impróprios". Próprios porque criados e praticados, exclusivamente, pelo computador e impróprios porque o computador é um meio utilizado para a prática delitiva. A nomenclatura puro dá uma conotação equivocada de licitude.

A incipiente doutrina concernente a este tipo de delito tem classificado como "crime de informática puro" a conduta que é praticada por meio e contra o sistema de informática. Quanto às condutas praticadas por meio de um computador, mas contra bem jurídico tutelado em lei e não compreendido entre os bens tidos como informáticos, tem denominado "crimes de informática mistos ou impuros". Funcionaria a *internet*, neste último tipo, apenas como um novo *modus operandi* para os crimes "tradicionais".[131]

Para Rita de Cássia Lopes da Silva, seriam crimes informáticos puros todas as condutas delitivas que surgiram com o uso da informática, pois teriam eles o sistema informático como meio e fim da conduta. Já os crimes informáticos impuros, ainda segundo a autora, seriam os tipos penais que, embora não dependam do sistema informático para serem cometidos, dela se servem como meio de execução. Tem, esta última espécie de crime informático, sua tipificação já claramente definida na legislação penal existente.[132]

Como ensina Ivette Senise Ferreira[133], há várias classificações quanto aos crimes informáticos, sendo muito adotada aquela que divide os atos ilícitos dirigidos contra um sistema de informática, podendo ser o computador ou seus dados e programas e os atos cometidos por intermédio de um sistema da informática, que alguns autores denominam crimes informáticos impróprios.

---

[131]DAOUN, Alexandre Jean. op. cit., p. 207.
[132]SILVA, Rita de Cássia Lopes da. op. cit., p. 60.
[133]FERREIRA, Ivette Senise. op. cit., p. 214-215.

Em outras palavras, Daoun afirma que a conceituação pode ser orientada pela análise da aplicação e interpretação dos verbetes "contra" e "pela".[134]

A importância da distinção entre os tipos de delitos advém da necessidade de se visualizar se a conduta tida por ilícita é ou não criminosa, bem como possibilitar a discussão acerca das que não são, a fim de tipificá-las e puni-las.

Repudiável, no entanto, a inflação legislativa. Não se defende a "criação" de leis de emergência que apenas acalmam ânimos e reclamos. Por outro lado, não se pode deixar de lado a necessidade de proteger direitos relacionados aos sistemas de informação e banco de dados.

A rigor, a simples conceituação "crime informático puro" ou "crime informático impuro" já pressupõe criminosa a conduta. No entanto, a esta classificação mais importa identificar o adjetivo do que a nomeação do substantivo. Isto porque, como exposto, entendida como criminosa a conduta que fere direito informático (puro, portanto) haverá a possibilidade de legislar e torná-la criminosa.

Conclui Daoun restar claro que, "em se falando de crimes informáticos de natureza mista, onde a *internet* é uma nova ferramenta para a prática do crime, não há que se cogitar em definir novos tipos penais".[135]

Ocorre que não comungamos da opinião de que os crimes informáticos impróprios ou mistos têm a *internet* apenas como via eleita para a prática delituosa e portanto nem sempre merecendo modificação legislativa.

Na verdade, a semelhança existente entre o delito comum e o mesmo delito praticado por um computador (informático impróprio) está tão somente no bem jurídico tutelado. Uma injúria, quando praticada oralmente, da mesma forma como aquela praticada por meio do computador, sempre ofenderá a honra subjetiva da vítima.

Além das semelhanças, existem as distinções. Um delito quando praticado por um computador torna sua apuração muito mais difícil, sem contar questões como a que norteou a escolha do tema deste trabalho ligada ao lugar do crime, mormente quando apresenta conduta e resultado em países distintos. Sem esta definição não se tem, com exatidão, a nação apta a aplicar a legislação própria ou alienígena.

---

[134]DAOUN, Alexandre Jean. op. cit., p. 206.
[135]Id. Ibid., p. 207.

Por essas razões, entendemos que o crime comum, se praticado por meio de um computador, por certo não carece de legislação autônoma, mas questões como a coleta de prova, cooperação internacional, sanção, não há dúvidas, devem ser revistas. Esta última, certamente, majorando-a.

Paralelamente a esta classificação, é de se ter em consideração que quando se fala em crimes praticados contra o computador por meio do computador, não se está a falar da máquina. Em verdade, danos à máquina serão possíveis também por meio de agressão mecânica.

O dano causado ao disco rígido de um computador por meio da disseminação de um vírus, por exemplo, configura, em última análise, um dano ao banco de dados do computador. Há, na hipótese, uma destruição dos arquivos, das informações contidas na máquina que o alojava e não só do objeto denominado disco rígido.

Questiona-se a possibilidade de entender criminosa a conduta que leva à destruição os bancos de dados contidos no computador, das informações nele armazenadas. Pela legislação vigente estaríamos diante de um delito de dano ou de conduta atípica?

Sandra Gouvêa explica que

> qualquer dado inserido em um computador é representado por um ou mais bits. Um texto, por exemplo, é digitalizado no teclado e os dados, armazenados na memória. O espaço ocupado pela memória é formado por bits, isto é, cada um dos caracteres representa um bit que foi arquivado na memória da máquina. Estes dados, agrupados de forma a constituir uma idéia, são, então, o que se chama de informação. A informação é um bem de inestimável valor para as sociedades modernas. Mas a visualização da informação nos computadores é feita, aparentemente, em um suporte não material. Surge daí a dúvida: as informações digitalizadas e armazenadas em computadores, formando arquivos, banco de dados etc, podem ser consideradas documento, para fins de proteção jurídica do capítulo do Código Penal que dispõe sobre 'A Falsidade Documental'?[136]

Como já dissemos em outra oportunidade, o mundo informático é novo e, portanto, passível de inúmeras indefinições, dentre elas, a ausência de normas regulamentadoras. Um tema prático em discussão diz respeito aos dados armazenados na memória de um computador.

---

[136]GOUVÊA, Sandra. *O direito na era digital.* Rio de Janeiro: Mauad, 1997.

O Superior Tribunal de Justiça, em maio de 2009, já chegou a afirmar que os dados contidos no computador podem ser considerados documentos para os fins penais[137].

Acertada nos parece a decisão, pois o valor do banco de dados, assim como o dos documentos em geral, está exatamente nas informações nele contidas. Assim, sua violação ou destruição estará afetando diretamente estas informações.

A informação tem valor inestimável. Seu valor, não raro, supera o do ambiente em que está armazenada. Todavia, não é de se equiparar a informação ao bem tangível, observa Daoun.[138]

O arquivo danificado pelo agente criminoso, a informação contida no computador por ele deletada ou deturpada são bens passíveis de proteção pelo Direito, eis que, embora virtual, afiguram-se tão reais no dia a dia que mais do que merecer, necessitam de proteção jurídica específica.

Aplicando a legislação em vigor, condenar-se-á o agente que violar tais direitos. Far-se-á, no entanto, na esfera civil, com fulcro nos artigos 186 e 927 do Código Civil, obrigando-lhe a reparar os danos causados. Ao Direito Penal só resta a figura do dano, certamente ineficaz e inapropriado se analisarmos os diferentes prejuízos causados com a destruição de dados arquivados dentro de um computador.

---

[137]*HABEAS CORPUS*. PENAL E PROCESSUAL PENAL. CRIME DE FALSIDADE IDEOLÓGICA. ALEGAÇÃO DE ATIPICIDADE DA CONDUTA, EM RAZÃO DA SUPERVENIENTE TIPIFICAÇÃO DO DELITO PREVISTO NO ART. 313-A DO CÓDIGO PENAL. INOCORRÊNCIA. 1. Vislumbrando que as instâncias ordinárias, após procederem à ampla análise dos elementos fáticos e probatórios constantes nos autos, reconheceram que a conduta praticada pelo ora Paciente se amoldava perfeitamente ao crime tipificado no art. 299, parágrafo único, do Código Penal, não se faz possível a modificação de tal entendimento por esta Corte, diante da inevitável necessidade do reexame da matéria fático-probatória, que, como é sabido, afigura-se inviável na via estreita do *habeas corpus*. 2. Ademais, o fato de ter sido posteriormente editada a Lei n.º 9.983/2000, inserindo no Código Penal o art. 313-A, não tem o condão de afastar a condenação imposta ao Paciente. Com efeito, o simples fato de sobrevir Lei nova tipificando uma conduta de forma mais especificada, como no caso em tela, onde trouxe para um tipo próprio a prática de crime cometido por funcionário autorizado que inserir dados falsos em sistemas informatizados ou bancos de dados da Administração Pública, não significa dizer que a realização de tais condutas, praticadas anteriormente à Lei n.º 9.983/2000, fossem atípicas, já que, à época eram perfeitamente alcançadas pelo disposto no art. 299, parágrafo único, do Código Penal. 3. Aliás, o legislador, ao criar o novo tipo penal previsto no art. 313-A do Código Penal, teve como intuito apenar de forma mais elevada a conduta de inserção de dados falsos em sistemas informatizados ou bancos de dados da Administração Pública, praticada tão somente pelos funcionários autorizados. Deixou de fora do referido tipo penal, portanto, o funcionário não autorizado a cuidar dos sistemas informatizados ou banco de dados da Administração Pública, aplicando-se, assim, a esses, o disposto no art. 299, parágrafo único, do Código Penal. 4. Ordem denegada. (STJ. HC 100062 / SP, Rel. Ministra Laurita Vaz – Quinta Turma. J. em 25.05.2009).

[138]DAOUN, Alexandre Jean. op. cit., p. 208.

O legislador pátrio, de forma limitada, mostrou-se conhecedor da imperiosa reclama. Tipificou algumas condutas praticadas pelo computador contra os dados e informações contidos no sistema informatizado da Administração Pública.

Comete crime desta espécie, conforme disposto no artigo 313 - A do Código Penal, quem nos sistemas informatizados da Admistração Pública insere ou facilita a inserção de dados falsos, altera ou exclui indevidamente dados corretos com o fim de obter vantagem indevida ou causa dano.

O artigo seguinte do mesmo diploma legal tipifica a conduta do funcionário que modifica ou altera sistema de informações ou programa de informática sem autorização. Diversamente do dispositivo anterior, o agente não age com o dolo específico de obter vantagem indevida ou de causar um dano. Se ocorrido o dano, uma das circunstâncias que aumentam a pena este não poderá ter sido alcançado dolosamente. Ainda se configura o delito ora analisado se o funcionário altera dados, substituindo os incorretos por corretos de um sistema de informática, se não autorizado para tanto.

Tais condutas, incriminadas pela Lei 9.983/2000, não podem pretender exaurir todas as ofensas praticáveis por meio do computador contra seu sistema e banco de dados, mas certamente ao trazer pena de reclusão de dois a doze anos e multa no artigo 313 - A do Código Penal avançou quanto à sanção do crime de dano comum que pune seu infrator com detenção de um a seis meses ou multa ou, na modalidade qualificada, detenção de seis meses a três anos e multa.

Como se depreende sem esforço de leitura dos artigos penais retro mencionados, visou o legislador proteger exclusivamente o sistema de informação da Administração Pública. No entanto, não é este o único sistema de informática que merece proteção estatal. Tanto assim que a Lei 9.609/1998 considera crime violar direitos de autor de programa de computador.

A propósito, tem-se aqui um apropriado exemplo de inflação legislativa. Com efeito, os direitos de autor de programa de computador seriam muito bem tutelados pela Lei de Direitos Autorais que, inclusive, lhe é contemporânea (Lei 9610/1998).

Feitas estas considerações, é de se ter em mente que

> o veículo que transporta a informação está dissociado de seu conteúdo, observa-se que pode a informação referir-se ao patrimônio, à honra, a um arquivo literário refletindo um direito do autor. Considerando que a afetação a estes bens juridicamente tutelados se encontra em um sistema informático, a realização de condutas ilícitas contra eles far-se-á, necessariamente, por meio do meio informático.[139]

Nos crimes informáticos puros, como o dano a dado ou programa de computador, a ação do agente se volta contra o conteúdo da máquina, alterando-lhe, destruindo ou inutilizando determinado programa ou dado por meio da introdução de vírus e afins.

Não raro, a ação do agente criminoso tem por escopo um fim determinado, como, *v.g.* a espionagem industrial ou invasão e violação de privatividade, ocasião em que deverá ser absorvida a primeira pela segunda em razão do dolo específico do agente, além da homenagem ao princípio da consunção.

6.1. Os crimes informáticos próprios

Nos dias atuais o computador tornou-se peça indispensável à sobrevivência da humanidade. Em qualquer situação o computador tem seu papel de imprescindibilidade desde a segurança de um usuário à própria segurança de uma Nação.

Os crimes informáticos ameaçam esta relação existente entre o homem e o computador, surgida a partir da revolução informática do século XX.

Nos crimes informáticos próprios a informática serve como meio e fim almejado pelo agente. Neste prisma, se não criarmos legislação específica, pelo princípio da anterioridade da lei penal, não haverá como punir o responsável pelas condutas ilícitas praticadas pelo computador.

A respeito, Rita de Cassia Lopes[140] alerta que nos dias atuais várias ações são praticadas com o uso do computador e a dúvida surge no instante de se saber se essas ações estão ou não tipificadas na legislação penal, quando prejudiciais ao convívio social.

---

[139]SILVA, Rita de Cássia Lopes da. op. cit., p. 95.
[140]Id. Ibid., p. 49-50.

Aduz ainda a autora que, em respeito ao princípio constitucional da legalidade, ações mesmo que prejudiciais não poderão ser punidas se não previstas previamente em lei.

Assim, para enfrentar a questão da tipicidade ou atipicidade das condutas praticadas na informática é necessário definir se determinados bens informáticos se encontram na categoria dos bens já tutelados pela norma penal para, posteriormente, verificar se podem ser tutelados por normas já existentes ou se necessitam de novas normas.

Dos crimes informáticos próprios, ofensivos contra o computador ou dados nele contidos ou por ele fabricado, podem-se destacar aqueles que atentam contra a inviolabilidade dos dados, das telecomunicações, do *hardware*, do *software*, das correspondências eletrônicas conhecidas como *e-mail*, do bom funcionamento dos sistemas operados por computador, da segurança nacional, dentre tantos outros.

A proliferação de vírus na *internet* é, cada dia, mais comum. No instante em que se cria um anti-vírus, os *hackers*, pessoas com *expertise* em computação, já criaram novos vírus acarretando novos ilícitos, que muitas vezes geram prejuízos irreparáveis e incalculáveis. Aqui não se trata de um crime comum de dano, mas muitas vezes traz ainda risco à segurança nacional, à atividade de uma empresa, ao transporte aéreo, dentre outros.

Não comungamos em parte com posicionamento pela atipicidade; há situações em que mesmo se tratando de crimes informáticos próprios o direito penal já tipifica aquela conduta.

O ponto que merece reflexão está ligado à correta adequação da figura típica existente com o mundo informático. Se um agente envia um vírus em um computador destruindo os sistemas, os dados e as informações podemos estar diante de um crime de dano, de concorrência desleal etc.

Temos com a era digital um novo meio utilizado para se alcançar o resultado, um aparelho ligado em rede, não sendo este o ponto da discórdia, mas a lesão aqui verificada não está exclusivamente ligada ao patrimônio computador, mas a todo o conteúdo nele existente com dados, informações, *software* e os dados dos recursos disponíveis, bens muitas vezes imateriais e intangíveis.

A informação[141] no mundo globalizado passou a ser um dos bens mais valiosos da humanidade, quer pelo valor patrimonial, quer pelo valor intelectual. Quando de um banco de dados ela é subtraída, copiada, divulgada ou destruída, temos possíveis bens lesados tais como patrimônio, intimidade, honra, imagem, propriedade imaterial, segurança nacional. Estariam eles adequados à figura da informação? A princípio pensamos que não.

Este é um dos casos em que se sustenta pela necessidade de o direito penal se adequar à nova realidade.[142]

Alguns vírus ganharam notoriedade pela sua alta proliferação, como o vírus Madonna, que ao final de um *strip-tease* da cantora avisava que o disco rígido do computador estava sendo apagado.

O vírus Melissa[143] foi o primeiro capaz de se multiplicar na *internet*, em grande escala, causando prejuízo estimado de oitenta milhões de dólares americanos, só no ano de 1999[144]. Este vírus infectava os computadores fazendo-os disparar grande quantidade de *e-mails*, causando congestionamento na rede.

Temos a *data diddling*, consubstanciada na alteração dos comandos existentes por outros com o fim de permitir o acesso ao banco de dados, registros e codificação.

Superzapping, que paralisa a memória do processador central, vetando a utilização das atividades com o acesso ao banco de dados e memória.

O *trojan horse* inclui, em programa existente, outras instruções que passam a coexistir com o programa já existente.[145].

É certo que não é só a ausência de legislação adequada a única causadora do aumento da criminalidade informática; temos ainda a falta de investimentos na segurança digital e o número reduzido de pessoas que utilizam o computador e a *internet*

---

[141]O Código de Defesa do Consumidor, Lei 8.078 de 1990, em seus artigos 72 e 73, respectivamente, criminaliza a ação de impedir ou dificultar o acesso do consumidor às informações em cadastros, bancos de dados, fichas e registros de pessoas e da conduta omissiva de não corrigir imediatamente informação sobre consumidor constante de cadastro, banco de dados, fichas ou registros que sabe ou deveria saber ser incorreta. BRASIL. Lei 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. *Diário Oficial da União*, Brasília, DF, 12 set. 1990.

[142]SILVA, Rita de Cássia Lopes da. op. cit., p. 65.

[143]DE LUCCA, Newton; SIMÃO FILHO, Adalberto (Coords.). op. cit., v. 2, p. 218.

[144]INELLAS, Gabriel Cesar Zaccaria de. *Crimes na internet.* 2. ed. São Paulo: Juarez de Oliveira, 2009. p. 16.

[145]SZNICK, Valdir. *Novos Crimes e novas penas no direito penal*. São Paulo: Livr. e Ed. Universitária de Direito, 1992. p. 6-8.

corretamente. Todavia, uma legislação inadequada e inaplicável certamente estão entre os principais motivos que justificam este exacerbado aumento da criminalidade informática.

A sociedade tenta se defender. São inúmeros os alertas, normalmente enviados por *e-mails*, de vírus ou golpes de crimes cibernéticos. Em atenção às diretrizes da Convenção de Budapeste, falta legislação a respeito, muitas vezes limitada ainda pela pouca atenção que se dá ao tema.

Neste diapasão, há quem sustente que qualquer lesão a estes bens informáticos como pichação de uma *homepage* é ainda atípica; trata-se de crime informático próprio ou puro, que necessita de legislação específica. Neste sentido, sustenta-se ainda pela atipicidade das condutas de vandalismo na rede, dano em arquivos provocado por vírus, pirataria de *software*, violação de *e-mail*.[146]

Outro ponto que merece reflexão está ligado ao conteúdo deste bem e a finalidade delitiva. A destruição de informações contidas em um banco de dados, visando prejudicar um concorrente, deixa de ser crime de dano para crime contra propriedade industrial.

6.2. Os crimes informáticos impróprios

Tais crimes são aqueles comuns praticados por intermédio de um computador. Anteriormente já existiam e eram praticados por meio diverso do computador. Com o surgimento do computador e sua ligação em rede, os criminosos passaram a ter mais um meio para operar.

Nesta espécie delitiva a informática serve apenas como meio e não como o fim almejado, este, inclusive, já era, anteriormente, tutelado pelo direito penal.

Quanto aos crimes comuns, praticados através de computador ou um aparelho ligado na *internet* como um *ipad* ou um telefone móvel, denominados crimes informáticos impróprios, melhor solução, conforme outrora já explanado, seria que também tivessem alterações legislativas, como punição superior da mesma forma como ocorre nos crimes

[146]CASTRO, Carla Rodrigues Araújo de. *Crimes de informática e seus aspectos processuais*. Rio de Janeiro: Lumen Juris, 2001. p. 11-12.

contra o patrimônio praticados por funcionário público. Criar legislação específica é aumentar, desnecessariamente, legislação existente.

Os crimes contra a honra são uma das espécies delituosas mais frequentes praticadas pelo computador. A exemplo do artigo 180 do Código Penal português, que pune o crime de difamação e é aplicável a essas condutas também quando praticadas pela *internet*, nosso Código Penal bem dá conta de punir tais crimes independentemente do *modus operandi.*

Nesta modalidade, inclusive, nossa legislação aumenta a sanção em um terço quando praticada por meio que facilite sua divulgação.

Ainda dentre os crimes informáticos impróprios destacam-se os chamados *phishing scams*, onde o infrator envia a usuários de serviços bancários *e-mails* com mensagens falsas, visando capturar informações pessoais daquele destinatário para com elas obter vantagem patrimonial.

Os infratores, por ainda limitado conhecimento informático por parte da sociedade (vítimas das condutas delituosas) e das Autoridades (responsáveis pela apuração e punição aos responsáveis pelo cometimento das infrações), atrelados a uma precária tecnologia apta a investigar, ganharam amplo mercado ao praticarem, por intermédio de um computador, antigas modalidades criminosas, aqui denominadas crimes de informática impróprios.

Um criminoso poderá, no mundo virtual, subtrair milhões de reais de uma instituição financeira sem sair de sua casa, sem usar uma arma, sem praticar violência contra terceiro, sem enfrentar *vis-a-vis* a vítima e ser preso em flagrante ou perder a própria vida.

São motivos mais que suficientes para fomentar uma nova geração de criminosos, diversa daquela já existente, que certamente também tentará se aproveitar das oportunidades do novo e inexplorado mundo informático.

As assertivas por meio da *internet* propaladas, pela sua dinamicidade a depender de seu conteúdo podem ofender, em muito, a esfera de direitos subjetivos da pessoa.

Sites de relacionamentos trazem estampados em suas páginas milhares de depoimentos, comunidades e testemunhos injuriantes, difamatórios, caluniosos e, por vezes, discriminatórios. Estas ofensas propaladas na w*eb*, mesmo que dirimidas,

dificilmente repararão estragos já causados. Milhares de pessoas que hoje leram matéria injuriante, amanhã, certamente, não serão as mesmas que lerão matéria reparatória.

Uma falsa informação enviada hoje na rede, capaz de ser divulgada a milhões de endereços eletrônicos, amanhã dificilmente será excluída integralmente da rede, se for esta a decisão judicial.

Com notável freqüência, o Judiciário é invocado para dirimir conflitos cíveis originados no âmbito do *site* de relacionamentos "Orkut".[147]

A privatividade é colocada em xeque todo o tempo por meio da *internet*. Paulo José da Costa Júnior, no ano de 1969, sem falar neste meio de comunicação moderno, chamava atenção ao fato de que a preciosidade do conceito "vida privada" parece estar sofrendo progressiva deformação em várias camadas da população. Na sociedade moderna, a existência de intimidade, privatividade, contemplação e interiorização é posta em cheque, numa escala de assédio cada vez maior, sem que reações proporcionais possam ser notadas.[148]

Sobre a transmissão de material obsceno, os Estados Unidos, em 1996, sancionou lei responsabilizando criminalmente infratores que transmitissem *on-line* material obsceno para menores de idade.

Não é este trabalho o campo para discussão acerca dos limites que, transpostos, mudariam a liberdade de expressão em conduta criminosa. Mas não é de se ignorar a possibilidade de, por meio da *internet*, praticar condutas que ignorem as barreiras impostas pelo direito em favor da intimidade, hipótese em que se consuma um crime e porque tal, devem ser punidas. Este sim, campo fecundo para discussões e objeto do nosso trabalho.

Também é criminoso o provento auferido mediante fraude perpetrada pela *internet*. Incide no artigo 171 do Código Penal o agente que engana o internauta para dele obter qualquer vantagem, causando-lhe prejuízo ou prejudicando terceiro.

O crime de pornografia infantil na rede, comumente denominado de pedofilia, tem aumentado sensivelmente nos últimos anos. Seu combate tem envolvido diversas polícias do mundo todo e também várias organizações não governamentais.

---

[147]STJ, REsp 1070183 / MG, Relatora Ministra Nancy Andrighi, julgado em 18/09/2008. SUPERIOR TRIBUNAL DE JUSTIÇA. Disponível em: <http://www.stj.jus.br>. Acesso em: 15 mar. 2011.

[148]COSTA JR., Paulo José da. *Tutela penal da intimidade*. São Paulo: Ed. Revista dos Tribunais, 1969. p. 17.

Enquanto existente a conduta, punível esta será com fulcro no Estatuto da Criança e do Adolescente, sendo certo que a *internet* configurará apenas o *modus operandi* do criminoso e, por isso mesmo, despiciendo seria legislar sobre o assunto de forma específica.

Vários outros crimes podem ser cometidos através da utilização do computador sem que seja necessária legislação específica para coibi-los

Pode-se, através da *internet*, entrar de forma criminosa no sistema informático de um hospital para, querendo-se assassinar um paciente, alterar-lhe na ficha médica o tipo ou a dosagem do remédio ou mesmo desligar-lhe o aparelho que lhe garante a vida.

Não obstante a gravidade da conduta, desnecessário seria legislar sobre o assunto e, por conseguinte o Projeto de Lei apresentado sob o nº. 76/2000. Este projeto de Lei, arquivado em 2003, trazia modalidade criminosa consistente em utilizar a informática para acionar bomba ou mecanismo que o valha para atentar contra a vida e integridade física das pessoas. No entanto, o Código Penal, em seu artigo 121, traz modalidade criminosa de homicídio e o qualifica quando executado com o auxílio de explosivo. Seria, em última análise, tornar tipo penal autônomo aquilo que é hoje qualificadora.

O crime de homicídio, contido no artigo 121 do Código Penal, é punido já pelo direito. Novo tipo penal acarretaria, dessarte, um *bis in idem.*

Temos ainda os crimes informáticos mistos. Nestes, a norma penal tutela dois ou mais bens jurídicos. São os denominados crimes complexos, tendo em uma mesma conduta a prática de um crime informático próprio e um ou mais crimes informáticos impróprios. Como exemplo, temos o artigo 72 do Código Eleitoral, que criminaliza a conduta, com pena de cinco a dez anos de reclusão, ao agente que obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, com o objetivo de alterar a apuração ou a contagem de votos.

Não se está a negar a necessidade de legislação específica para os crimes informáticos, mas sim a chamar a atenção que não se pode criar leis penais que protejam bens já protegidos por leis da mesma natureza ou pelo Código Penal.

Salienta Ricardo M. Mata y Marin que o direito penal

> representa el medio jurídico más gravoso para los bienes e intereses de las personas por lo que únicamente debe ser empleado en los casos de ataques a los bienes mas importantes de las personas e y de la comunidad y cuando no existan otros medios jurídicos que pudieren solucionar satisfactoriamente este tipo de situaciones.[149]

O tema aqui discutido não diz respeito propriamente à aplicabilidade ou não do direito penal, sustentada pela teoria do direito penal mínimo, mas da necessidade ou não de se criar legislação penal específica para proteger os bens ofendidos pelo delito informático.

Antonio Fernandes Scarance lembrou-se de matéria veiculada na Folha de São Paulo em 1999, a qual noticiou que a Polícia do Mato Grosso do Sul prendeu, em flagrante, várias pessoas que utilizavam a *internet* para veicular *shows* eróticos ao vivo. Houve apreensão dos equipamentos de informática que foram montados para transmitir os *shows*. O fato foi enquadrado no artigo 234 do Código Penal que criminaliza as condutas consistentes em "fazer, importar, exportar, adquirir ou ter sob sua guarda para fim de comércio, de distribuição ou de exposição pública, escrito, desenho, pintura, estampa ou qualquer objeto erótico".[150]

Denota-se perfeita adequação do tipo ao fato, sendo possível punir condutas que se entendam criminosas valendo-se, para tanto, de uma norma talvez não específica, mas suficiente para não ofender o princípio da reserva legal.[151]

Reitere-se, contudo, que não se defende aqui a aplicação por analogia de uma lei penal a condutas não tipificadas, mas sim que a conduta entendida por criminosa seja, sempre que possível, punida pelo direito penal já existente, em detrimento de nova tipificação.

---

[149]MATA Y MARTÍN. Ricardo. *Temas de direito da informática e da internet*. Porto, Portugal: Coimbra Ed., 2004. p. 201.

[150]FERNANDES, Antonio Scarance. Crimes praticados pelo computador: dificuldade na apuração dos fatos. *Revista de Ciências Criminais*, São Paulo, ano 3, p. 20, 1999.

[151]Sem ofensa ao princípio *nulla crime sine lege previa*, é possível flexibilizar na norma incriminadora, a exemplo do artigo 241 do Estatuto da Criança e do Adolescente. O dispositivo citado estampa diversas condutas praticáveis em qualquer meio de comunicação e, após reza "(...) inclusive por sistema de informática ou telemático (...)". O novo *modus operandi* garantido pelo legislador desde 1990, alterado em novembro de 2008, quando a *internet* estava muito longe do alcance de grande parte da população e, consequentemente dos pedófilos é um exemplo da moderna técnica legislativa amoldada à atualidade, mais precisamente antecipando a ela, sem a necessidade de criar novo dispositivo penal.

Isto porque, mais do que provocar desnecessário aumento de leis, pode o excesso de tipificação redundar, aí sim, em conflito aparente de normas ou na aplicação do direito penal por analogia. Caso se tente legislar um tipo penal para cada conduta praticável em um mundo que tem a mutação por sua principal característica (assim o é o espaço cibernético), correr-se-á o risco de tornar obsoleto o tipo penal da noite para o dia e, por conseguinte, colocar em risco, pelo princípio da reserva legal, sua própria aplicabilidade.

Neste sentido, em artigo sobre direito penal informático, José de Faria Costa[152] analisa a questão da necessidade ou não de se criar uma norma específica para tutelar os bens ofendidos por meio da informática.

Traz como exemplo delitos informáticos lusitanos, tratados pela Lei 109, de 17 de agosto de 1991. São eles: falsidade informática (artigo 4º), dano relativo a dados ou programas informáticos (artigo 5º), sabotagem informática (artigo 6º), acesso ilegítimo (artigo 7º), interceptação ilegítima (artigo 8º) e reprodução ilegítima de programa protegido (artigo 9º).

Faria da Costa explana que de todos estes delitos informáticos apenas a reprodução ilegítima de programa protegido traz um novo bem jurídico. Nos demais delitos o bem jurídico continua sendo o mesmo, o patrimônio, o normal fluxo de informações, da veracidade dos documentos, dentre outros.

Sobre a reprodução ilegítima, o autor sustenta que o que de fato se almeja tutelar não é propriamente o fluxo informacional automatizado, mas os direitos patrimoniais de seus detentores, estes surgidos antes do próprio fluxo informacional.

Conclui seu artigo sustentando que a única mudança surgida nos crimes informáticos é o meio pelo qual se opera a conduta, não havendo motivo para a criação de uma nova disciplina jurídico-penal, quando muito de uma área específica normativa de incriminação.

Vicente Greco Filho[153], nesta mesma esteira, não adula nova legislação para tratar dos meios eletrônicos. Alerta que a *internet* é mais uma criação humana e como tal deve ser tratada pelo Direito, especialmente pelo Direito Penal.

---

[152]COSTA, José de Faria. Algumas reflexões sobre o estatuto dogmático do chamado "direito penal informático". *Revista Jurídica da Universidade Moderna*, v. 1, p. 47-63, 1998.
[153]GRECO FILHO, Vicente. op. cit.

Critica aqueles que sustentam que a ordem jurídica desconhece ou não está apta a disciplinar a nova criação. Deve-se evoluir, sem precipitações. A informática, a *internet* ou a peixeira são apenas instrumentos utilizados para a prática lesiva, e o direito penal, em regra, já está aparelhado na missão de coibir condutas lesivas. Seria um grave e perigoso erro de política penal querer definir crimes específicos para estas situações.

Exemplifica o autor demonstrando que a intimidade deve ser tutelada de forma geral e não específica. Aponta que a mesma pode ser lesionada não só pela informática, mas por outros meios, como a gravação ambiental ou uma foto de um *paparazze*.

Conclui que o agente que, indevidamente, tira cópia de documentos ou acessa uma caderneta de telefones pratica a mesma conduta reprovável que o *hacker* que acessa indevidamente um banco de dados de um computador. Sustenta, com razão, que tanto os documentos quanto a caderneta são igualmente possuidores de banco de dados.

Para Góis Júnior[154], parte da legislação está, com algumas alterações, apta à era informática, mas parte ainda necessita ser legislada. É o caso do furto de programas de computador e outros bens na rede.

Para o autor, tais bens, na maioria dos países, são considerados imateriais, portanto não passíveis de serem adequados à conduta tipificada pelo furto, restrito à subtração de bens materiais.

Situações como esta precisam, com urgência, de uma definição. Superando a definição da materialidade ou imaterialidade dos bens existentes na rede, aí sim o direito penal deverá ser ajustado a ela, alterando legislação existente ou criando legislação nova.

Se há hoje lei penal não específica que, adequadamente, permita a punição, não há de se invocar o legislativo para tipificar condutas praticadas pela *internet*, mesmo porque, legislar em área do direito em que o princípio da taxatividade impera de tal forma – como o é no direito penal – acerca de assunto mutável por natureza, é correr-se o risco de, em pouco tempo, ter-se por atípica grande parte do que foi legislado.

Ademais, o termo empregado pelo legislador na redação do tipo é o grande responsável pela sempre atual leitura que se consegue fazer do crime que vai ali tipificado.

---

[154]GOIS JR, José Caldas. op. cit., p. 120.

Maior deve ser a preocupação da comunidade jurídica penal acerca de qual o país competente para punir o crime praticado por meio do computador do que sobre a necessidade ou não de criar um "código penal informático".

6.3. Dos crimes informáticos frente ao direito, a liberdade de informação, de expressão e de comunicação

Este tema já é considerado um dos mais emblemáticos da era digital. Qual o exato momento em que a conduta sai da legalidade, respaldada pelo direito a livre expressão, informação ou comunicação e entra na ilicitude, quer pela ofensa à honra objetiva ou subjetiva, quer pela ofensa à intimidade, entre outras?

Enfrentando o tema, a Corte australiana, em dezembro de 2002, decidiu no caso Dow Jones[155] que a liberdade de expressão era mais ampla que a honra objetiva de um magnata do minério chamado Joseph Gutnick, difamado por um jornal na *internet* pela prática de lavagem de dinheiro.

O tema enfrentado pela Corte Australiana tem como centro a discussão de um tema que não é novo em nosso sistema jurídico, qual seja, o confronto entre os direitos e respectivas esferas de proteção.

Assim, o conflito entre a liberdade de informação sempre teve pontos de tensão com o direito à intimidade, sendo que ambos são protegidos em nossos ordenamento. Até mesmo antes do advento da *internet* e dos sistemas de armazenamento de dados, as invasões à intimidade já eram sentidas, muitas vezes sob o manto do direito à informação/expressão/comunicação. Basta que liguemos a televisão para que nos confrontemos com notícias e reportagens que devassam a vida de diversas pessoas, bem como apresentam informações que, a princípio, estariam armazenadas em bases de dados privados ou acobertadas por sigilo.

O vazamento de informações também é bastante sentido em nosso sistema jurídico, mormente no direito criminal, com o vazamento de informações processuais e a ampla

[155]ABOSO, Gustavo Eduardo; FLORENCIA ZAPATA, María. op. cit., p. 32-33.

cobertura de operações policiais, o que faz com que dados e imagens dos envolvidos sejam amplamente divulgadas.

Tais condutas, quando excessivas, em nossa opinião, não podem ser acobertadas pelos direitos à informação, expressão ou comunicação. Deve haver um temperamento aplicado ao caso concreto.

Os direitos de informar, expressar e comunicar devem ser respeitados, mas sempre se zelando pela intimidade dos envolvidos, bastando que se faça um sopesamento entre a necessidade da exposição de algumas imagens ou informações para que sejam cumpridos os primeiros direitos citados.

Assim, basta a indagação: Para que se informe algum fato é necessário que se divulgue imagens do agente em ocasiões privadas? Para que se noticie algum evento é necessário que o sigilo telefônico dos envolvidos seja levado à imprensa? Para que alguém se expresse em uma rede social é necessário que seja atacada a honra de pessoa citada na mencionada manifestação?

As questões acima levantadas, de forma exemplificativa, trazem diretrizes de como devem ser enfrentados estes conflitos entre direitos.

Muito nos preocupa nesta nova era a tendência de priorizar a informação, expressão e comunicação em detrimento da intimidade, honra e sigilo das comunicações. Ambas as vertentes são imprescindíveis em nossa vida ligada ao mundo digital. Sem a comunicação ou a informação dificilmente conseguiríamos conectar-nos com o mundo, todavia sua imprescindível necessidade não pode ser posta como justificativa para desrespeitar direitos tão importantes como o da honra, intimidade e sigilo das comunicações.

7. Os crimes informáticos permanentes

A classificação dos delitos é por demais antiga na doutrina brasileira, sendo uma das classificações aquela que separa os delitos entre os instantâneos, permanentes e instantâneos de efeitos permanentes.

No que diz respeito aos crimes permanentes, temos que são aqueles em que sua consumação se perpetua no tempo, isto é, a conduta delitiva passa a se dilatar de forma que enquanto não interrompido o ato delitivo a consumação se prolonga no tempo.

Tal classificação delitiva também pode ser aplicada aos delitos informáticos, sendo este o que utiliza o sistema como meio de consecução do delito ou quando o crime é praticado contra o próprio sistema.

Keytroke-logging: É um programa de computador que monitora as teclas usadas na digitação. Na maioria das vezes, ele vem com um cavalo de tróia e é utilizado para se descobrir *login* e senha de *e-mails* e até mesmo de contas bancárias.

Teremos um crime informático permanente quando o agente instala um *keytroke-logging* em um computador para monitorar a digitalização das teclas e descobrir informações daquele usuário tais como contas bancárias, senhas e com elas passa a subtrair dinheiro da conta bancária daquele usuário. Todavia, se instalado o *keytroke-logging,* e o agente não danificar a máquina, nem divulgar ou obter vantagem através das informações colhidas no âmbito penal a conduta será atípica, a violação à intimidade não é criminalizada em nossa ordenação.

Neste caso, ou em qualquer delito informático em que haja permanência, acreditamos que seja perfeitamente possível a aplicação do preconizado pela doutrina aos crimes permanentes não classificados como informáticos sendo normalmente iniciado por uma primeira fase de natureza comissiva e as demais de natureza omissiva.

8. Espécies de infrações penais informáticas

Sem desviar do tema deste trabalho, algumas anotações sobre as espécies delitivas frente a era digital precisam ser apresentadas. Não só pelo surgimento dos crimes informáticos próprios, mas também pela necessária adequação de nossa legislação aos crimes informáticos impróprios.

8.1. Dos crimes contra a pessoa

Vários são os crimes informáticos capazes de atingir o homem, quer na sua integridade física, mental, quer na sua própria vida. Quanto mais nos tornamos dependentes da informática, mais estamos sujeitos, através dela, a violações por condutas ilícitas.

8.1.1. Do homicídio

Há poucas décadas não imaginávamos ser possível praticar um homicídio à distância através de um aparelho comunicado a outro. Hoje, através de um computador ligado em rede, isto não só é possível como passou a ser provável.

Com a informatização, a cada dia mais presente em nosso cotidiano, vários serviços passaram a ser executados por ela. A informática, em um hospital, como exemplo, é responsável pelo preenchimento da ficha dos pacientes, dos pagamentos e cobranças, dos procedimentos a serem adotados aos pacientes e, em muitos casos, pelo próprio comando de aparelhos ligados ao paciente para monitorar sua respiração, batimento cardíaco ou aplicar medicamentos.

Desta forma, pode-se afirmar que é possível, através da *internet*, uma pessoa com exímio conhecimento informático, entrar no *site* de um hospital e, com senhas de acesso ou quebrando barreiras de segurança eletrônica, muitas vezes precárias, determinar, de qualquer lugar do planeta, o desligamento de uma máquina ou a alteração de um medicamento, levando o paciente a óbito.

Com o avanço da medicina e da informática surgiu a Telemedicina, tecnologia que permite, através da *internet*, a realização de exames, consultas e intervenções cirúrgicas à distância. A interceptação e a alteração desta comunicação de dados pode também lesionar ou até matar o paciente.

Não podemos nos esquecer que os atentados terroristas contra os Estados Unidos da América, ocorridos em onze de setembro de 2001, mostraram ao mundo do que a *internet* é capaz. Foi através dela que os terroristas, em grande parte, se comunicaram de países distintos, organizaram os ataques, obtiveram informações, compraram passagens etc.

Muitas vezes, mesmo que a informática não tenha diretamente sido utilizada na conduta nem no resultado, como no caso do atentado ao World Trade Center, sem ela dificilmente estes crimes seriam consumados.

Sobre a tipicidade ou não das condutas acima, praticadas através ou com a ajuda de computadores ligados em rede, o resultado lesão corporal leva à figura do delito contra a integridade física. A morte leva à figura do homicídio e assim por diante. Não há conduta atípica, tendo aqui a diferença encontrada apenas no meio pelo qual estas condutas

chegaram a seu resultado, um aparelho conectado à rede. São os chamados crimes informáticos impróprios.

Nos crimes contra a vida, tramitou no Congresso projeto de lei 76/2000 que, em seu artigo 1º, parágrafo 4º, tipificava o uso de informática contra a vida e integridade física das pessoas. Neste projeto, arquivado em 2003, por ter sido substituído pelo PLC 89/2003, o qual não trata mais desta questão, há um claro conflito de normas.

Tem-se que, na ânsia de legislar sobre questões ligadas ao mundo virtual, não criar legislações já existentes, causando com isto um resultado inverso do pretendido, uma inaplicabilidade de norma ao caso concreto até que se decida qual norma deve ser aplicada.

Foi muito divulgado um caso de um médico chamado Jack Kevorkian[156], vulgo doutor morte, que, através da *internet*, orientava pessoas a se suicidar. Após muita discussão social, o Poder Judiciário condenou-o à pena de 25 anos de prisão pela prática de homicídio, eis que um de seus pacientes não possuía condições de administrar as drogas que o levariam a óbito, o que foi feito pelo citado médico.

8.1.2. Dos crimes contra a honra (*cyberstalking*) e a liberdade moral

Temos nossa honra como um dos bens mais indispensáveis a nossa confortável sobrevivência. Ela divide-se em objetiva e subjetiva. A primeira representada pela nossa reputação perante terceiros. A segunda se relacionada ao nosso decoro e dignidade.

Através de qualquer aparelho ligado em rede o usuário é capaz de enviar para milhões de outros usuários, desde que públicos, qualquer imagem ou escrito. Com isto este documento enviado eletronicamente poderá ofender a honra de terceiros ou ameaçá-los em fração de segundos.

Preocupados com a proliferação deste delito, agora facilmente praticado através da *internet*, os Estados Unidos vêm estudando esta modalidade delitiva definindo-a como *cyberstalking*.[157] Muitos Estados americanos, inclusive, já alteraram sua legislação para

[156]JACK Kevorkian. Disponível em: <http://pt.wikipedia.org/wiki/Jack_Kevorkian>. Acesso em: 10 mar. 2011.
[157]The law vs. Online Stalking. NetGuideMagazine. MADCAPPS. Disponível em: <http://www.madcapps.com>. Acesso em: 15 mar. 2011.

adequar-se a esta modalidade delitiva.[158] Dentre tais alterações está a possibilidade de suspensão do acesso à *internet* por parte do acusado, podendo acarretar em prisão seu descumprimento.

O primeiro caso de prisão no Brasil pela prática de *cyberstalking* ocorreu em agosto de 1997[159]. Um analista de sistemas de São Paulo, casado, pai de duas filhas, com 38 anos de idade, foi preso ao ameaçar uma apresentadora da TV Cultura, Maria Cristina Poli. Dizia-se louco pela jornalista e em exatas 15 linhas descrevia cenas de sexo que iria protagonizar com a vítima.

A autoria foi descoberta após o provedor de serviços rastrear e identificar seu usuário, que tinha em seu disco rígido outras 430 mensagens com o mesmo teor.

Surgiram, com a *internet*, *sites* de comunicação e relacionamento, como o *e-mail*, o *chat*, o *youtube*, *facebook*, *skype*, *twitter*, por meio dos quais milhares de pessoas se comunicam, trazendo e colhendo informações sobre qualquer tema.

Todavia, este novo meio de comunicação abriu caminho à prática de condutas ilícitas como aquelas ofensivas à honra. Para aumentar ainda mais este número de acessos e consequentemente de divulgação de ofensa surgiram os *news groups* ou *chats* onde grupos de usuários conectados por assuntos, sexo, idade, religião, dentre outros temas, se comunicam.

Nestes *sites* de bate-papo, como comumente são conhecidos, é muito comum a divulgação de ameaças e ofensas à honra de pessoas. Os grandes alvos são pessoas famosas, ex-companheiros ou desafetos. Tem-se sites em que o próprio título e motivo de sua criação já são ofensivos a terceiros como "eu odeio Sandy e Júnior" ou "Eu odeio a Telefônica" [160] .

Nossa legislação, nos crimes contra a honra, anteriormente a este incalculável número de pessoas que terão ciência das ofensas, estipulou um aumento de pena em um terço para os casos em que tenha sido a ofensa praticada na presença de várias pessoas ou por meio que facilite sua divulgação.

---

[158]GOIS JR, José Caldas. op. cit., p. 147.
[159]SIMAS FILHO, Mario. A face bandida. *Isto É*, São Paulo, n. 1496, p. 50, 13 jun. 1998.
[160]Eu odeio Sandy e Jr. em CJB.NET. Disponível em: <http://www.euodeiosandy.cjb.net>. Acesso em: 26 jun. 2010 e Eu odeio a Telefônica em ARTEWEB. Disponível em: <http://www.arteweb.com.br/telefonica>. Acesso em: 26 jun. 2010.

Reside nesta causa de aumento um dos pontos em que se faz necessária revisão legislativa. Sua proliferação, através da rede, em fração de segundos pode ser divulgada a milhões de pessoas e mesmo que seja futuramente determinada sua exclusão, permanecerá arquivada em muitos *sites* e dados de usuários desconhecedores de tal decisão ou arredios a ela. Isto torna esta ofensa instantânea com efeitos permanentes.

Assim, não obstante se trate de um crime formal, merecida revisão se faz necessária, para adaptar-se a esta nova realidade do mundo virtual. Melhor adequado à era digital se o aumento de pena tivesse relação direta com o número de pessoas que acessassem tal ofensa na *web*.

A respeito, tivemos na última Copa do Mundo a frase "Cala boca Galvão"[161], posta no *twitter*, em alusão a um famoso locutor esportivo. Tal mensagem que foi lida e divulgada por milhões de pessoas em diversos países, tendo o envolvido optado por levar tal ofensa na brincadeira, talvez por receito de, se tomadas medidas judiciais cabíveis, sofrer novo ataque na rede.

8.1.3. *Cyberbullying*

Entre os males que atingem a população brasileira, sobretudo os mais jovens, está o fenômeno denominado "Bullying", sendo esta a denominação universal para um conjunto de atividades agressivas, repetitivas e sem motivação aparente perpetradas por um aluno, ou grupo deles, contra outro indivíduo, causando a este sofrimento e humilhação.[162]

Tais atitudes são praticadas pelos denominados 'bullies' e consistem, no mais das vezes, na prática de insultos, ataques físicos, depreciações e isolamento das vítimas, entre outras atitudes que impingem sofrimentos e humilhações às vítimas.

O problema aqui examinado é de repercussão mundial, merecendo diversos estudos, mesmo porque revela um comportamento distorcido por parte daqueles que infringem os males, bem como provocam às vítimas severas sequelas psicológicas.

---

[161]O GLOBO. Disponível em: <http://oglobo.globo.com/pais/noblat/posts/2010/06/11/sucesso-mundial-cala-boca-galvao-299364.asp>. Acesso em: 15 mar. 2011.

[162]DIGA não ao Bullying. Disponível em: <http://www.diganaoaobullying.com.br/bullying.htm>. Acesso em: 10 mar. 2011.

Além das sequelas acima citadas, é de se notar que quando o "bullying" é praticado no âmbito escolar, nota-se nas vítimas de tais condutas uma sensível queda no rendimento escolar, assim como receio de até mesmo frequentarem a escola, temerosas de qualquer ato contra si.

Diante dos malefícios que tais condutas provocam a todos os envolvidos, estudiosos, educadores, famílias e sociedade têm se mobilizado em ações de esclarecimento para que seja evitado tal tipo de violência, encontradiço, sobretudo, no ambiente escolar.

Como conduta encontrada no mundo fenomênico, deve ser feita, respeitado o princípio da tipicidade, a respectiva adequação típica, de modo que condutas que lesem bem jurídicos penalmente tutelados não fiquem à margem das respectivas punições.

Destarte, temos que são claros os prejuízos a bens jurídicos penalmente tutelados, como a saúde, a honra, a integridade física e mental das vítimas, dependendo da modalidade de "bullying". Nesta mesma esteira, pode haver a tipificação das condutas em crimes como ameaça, contra a honra e lesões corporais.

Cotejando as argumentações acima com a delinquência informática, temos que o "bullying" também pode ser praticado tendo como mecanismos os meios eletrônicos, como a proliferação de mensagens de *e-mails* ou até comentários desabonadores em redes sociais, sendo que para ambos os casos, em nosso entender, estaria caracterizado delito informático impróprio, já preconizado em nossas legislações, sendo o meio eletrônico utilizado como o meio para a consecução da conduta.

8.1.4. Terrorismo

Várias modalidades delitivas com a era digital ganharam um maior campo de atuação. O terrorismo é um deles, agora denominado terrorismo virtual ou ciberterrorismo.

As motivações continuam as mesmas, mas os meios estão sendo mudados. O terrorista que ontem usava gás *sarin* e granadas explosivas, hoje, com a mesma ou ainda maior nocividade, ataca usando um computador ligado em rede.[163]

[163]GOIS JR, José Caldas. op. cit., p. 163-164.

A *internet* passou a ser um dos locais mais aptos aos terroristas para o planejamento e execução de seus atos. Através dela, a comunicação entre os terroristas localizados a milhares de quilômetros de distância, muitas vezes em nações distintas, passou a ser instantânea e camuflada. Dificilmente eles navegam na rede com seus verdadeiros dados pessoais ou termos não codificados.

Não é de hoje que a comunidade internacional se preocupa com o terrorismo, tanto que já em 1937 a Liga das Nações Unidas elaborou a Convenção para Prevenção e a Punição ao Terrorismo, diploma que foi seguido por tantos outros também suscitando o tema.

Nossa legislação criminaliza a conduta praticada pelo terrorista no artigo 20 da lei 7170/1983, todavia por falha legislativa não definiu tal dispositivo como crime de terrorismo, o que traz discussões sobre sua aplicabilidade.

Não há como negar que a *internet* é usada para trocar informações em velocidade real, além de facilitar o trabalho daqueles que arregimentam terroristas e para a propagação de mensagens conclamando os que pretendem adotar atos de terrorismo.

O mundo se apercebeu do alcance maléfico da *internet* no planejamento dos ataques terroristas de 11 de setembro de 2001, às torres gêmeas, em Nova Iorque, Estados Unidos. Por meio dela, os comandantes se comunicaram com os comandados de dentro dos Estados Unidos da América e determinaram o dia, local e horário para a prática terrorista que levou à morte centenas de americanos e estrangeiros.

Também podemos citar o ataque terrorista ocorrido em 11 de março de 2004, oportunidade em que bombas colocadas nos sistemas de transportes de Madri ocasionaram a morte de 191 pessoas, bem como deixaram mais de 2.000 feridos.

No dia 24 de janeiro de 2011 houve um ataque terrorista na Rússia, ocasião em que um homem bomba detonou o artefato que trazia consigo na área de desembarque do aeroporto de Domodedova, deixando dezenas de mortes e feridos.

Merece ainda registro o ataque terrorista ocorrido em Londres, em julho de 2005, ocasião em que ocorreram explosões de quatro bombas, três no metrô e uma em um ônibus, ocasionando a morte de dezenas de pessoas e algumas centenas de feridos.

Pode-se dizer, com grande margem de segurança, que em todos os ataques, inevitavelmente, houve o uso da *internet*, no planejamento, na troca de informações entre comandantes e comandados e nas ordens de execução.

8.1.5. Dos crimes contra a intimidade

Nossa legislação ainda não criminaliza quem ofende a intimidade, apesar de nossa Constituição Federal, em seu artigo 5º, inciso X, garantir a inviolabilidade da intimidade e da vida privada.

Com o surgimento da *internet* e o uso mais frequente do computador, surge um volume incalculável de armazenamento de dados, contendo informações das mais variadas, dentre elas, aquelas de teor sigiloso.

Os sistemas informáticos vêm, a cada dia, ampliando sua rede e seu cruzamento de informações com outros sistemas. Isto acelera e facilita a navegação. Trata-se de uma tendência que só irá aumentar com o passar dos anos. Em pouco tempo teremos usuários de todo o planeta terra plugados *on-line* – é a chamada globalização.

Pela *internet* realizamos transações comerciais. Para tanto, informamos dados como cartão de crédito, código de segurança, endereços e identificações pessoais, que merecem sigilo.

Com o registro de dados na rede, constata-se uma redução em parte da vida privada, que com o passar do tempo tende a aumentar. Basta acessar sítios de pesquisa como o Google ou Yahoo e clicar um nome de pessoa relativamente conhecida para, em fração de segundos, obter informações sobre sua vida profissional, pessoal, currículo etc. Com uma busca mais criteriosa se obtém, inclusive, informações que a própria pessoa desconhece que estão acessíveis e que, em alguns casos, discorda de tal divulgação.

Contrariando este sigilo de informações, existe uma corrente defensora de, pelo princípio da liberdade de informação na *internet*, deixar livre as informações divulgadas na rede. Trata-se do *Wikileaks* que recentemente pôs em evidência esta questão.

De um lado, Julian Assange, fundador, principal responsável e editor do *Wikileaks*, *site* pertencente a uma organização transnacional de mesmo nome, sem fins lucrativos, com sede na Suécia, divulgou na rede dados sigilosos do governo americano.

Tais dados, acessados por milhares de pessoas em todo o planeta, colocaram o governo americano em constrangedora situação perante países estrangeiros, pois continham informações internas sobre países e seus importantes personagens, muitas delas ofensivas ou mal colocadas.

De outro lado, o governo mais importante e influente do planeta tentou preservar suas informações sigilosas frente a uma corrente amplamente favorável à divulgação de toda e qualquer informação na rede.

Tomou diversas medidas, tais como solicitar às empresas de cartão de crédito Visa e Mastercard que parassem de operar com mencionado *site*, o que foi feito. Em protesto, especialistas em informática, denominados *hackers* enviaram vírus a estas empresas causando-lhes transtornos e milhões de dólares em prejuízos.

Esta situação demonstra uma nova era digital, onde os usuários da *internet* passam a ter um papel se não de comando ao menos de participação nas decisões sobre a rede. Percebe-se que se trata de um mundo diverso do mundo real, passível de adequações jurídicas com o fito de extrair dele apenas o que se tem de positivo.

Visando tutelar ainda mais a intimidade, mormente na era digital, deve o Brasil, assim como fez a França ao garantir o direito de amar e de morrer em paz,[164] criminalizar a conduta que a ofende, quer através da informática quer de qualquer outro meio. Tal medida, certamente, viria ao encontro das tentativas de barrar o acesso irrestrito de pessoas físicas e jurídicas na rede.

8.2. Dos crimes contra o patrimônio

Talvez seja este, ao lado da honra, o bem mais lesado com o surgimento da informática.

Com a *internet* as pessoas que antes não tinham coragem de subtrair o patrimônio alheio, com a oportunidade de, sem sair da frente de um computador ou de correr o risco de ser surpreendida no instante da obtenção da vantagem, passaram a praticar este delito,

[164]COSTA JR., Paulo José da. *O direito de estar só*. 4. ed. São Paulo: Ed. Revista dos Tribunais, 2007. p. 117.

quer motivadas pelo interesse econômico, quer motivadas pela vaidade atrelada à superação de barreiras de segurança informática ou ainda pela improvável possibilidade de serem presas em flagrante ou até condenadas.

Debora Nigri[165] sustenta que nosso Código Penal de 1940 não está adequado aos delitos informáticos. Afirma que antes de se impingir os delitos de estelionato, apropriação indébita, furto ou invasão ao domicílio àquele que acessa o extrato bancário de terceiros ou subtrai seus bens deve-se estabelecer qual o bem tutelado quanto à informação do sistema informático, considerado um bem intangível e merecedor de tratamento autônomo por ser tão valioso quanto um bem corpóreo.

Em sentido contrário, Gagliardi[166] defende que o computador, nos crimes de fraude por manipulação, apenas executa o ato comandado pelo homem, sendo portanto apenas um *longa manus* do criminoso.

Diz ainda que o computador seria uma espécie de preposto ou empregado da vítima, sendo enganado pelo criminoso que se fazia passar pela vítima ao utilizar seu *password*. Assim, se subtraído qualquer valor sem a participação da vítima, por ato unilateral do infrator, teríamos o furto qualificado pela fraude, pela ausência de participação da vítima.

Com o crescimento do comércio eletrônico, milhares de pessoas vêm a cada dia realizando mais operações comerciais. Este novo mercado vem abrindo um campo para os criminosos, através da *internet,* obter alguma vantagem ilícita.

8.2.1. Do furto

Da mesma forma, o crime de furto encontrou campo fecundo na *internet*. É crime de furto a conduta do agente consistente em subtrair numerário da conta bancária alheia.

No crime informático impróprio, a subtração ocorre no instante que o numerário "eletronicamente" sai da conta bancária da vítima, materializando o provento econômico do agente.

---

[165]NIGRI, Debora Fisch. Crime e informática: um novo fenômeno jurídico. *Revista Trimestral de Jurisprudência dos Estados*, 100/40-48, ano 16, maio 1992, p. 47 *in* SILVA, Rita de Cássia Lopes da. op. cit., p. 96.

[166]GAGLIARDI, Pedro Luiz Ricardo. *Crimes cometidos com o uso de computador*. São Paulo, 1999. (Doutorado em Direito Penal) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 1999.

Góis Júnior, contrariando nosso posicionamento, sustenta que a subtração de bens existentes da *internet* como programas de computador, por serem imateriais, conforme entendimento da maioria dos países, não configurariam nosso crime de furto que exige em sua conduta típica a subtração de bem material alheio.[167]

8.2.2. Do furto de bagatela

Furto de bagatela é definido como aquele em que, pelo ínfimo valor patrimonial do bem subtraído para aquela determinada vítima, não há ofensa ao bem tutelado, razão pela qual o direito penal não deve ser aplicado.

Para Nucci, "O direito penal não se ocupa de insignificâncias (aquilo que a própria sociedade concebe ser de somenos importância), deixando de considerar fato típico a subtração de pequeninas coisas de valor nitidamente irrelevante".[168]

Neste sentido, na *internet* surgiu uma espécie de delitiva denominada "furto salame".[169] Consiste na subtração, mediante transferência bancária levada a cabo pela *internet*, de centavos de reais; todavia, como subtraídos de milhares de correntistas, alcançaria valores bem elevados. Porque irrisória a quantia, muitas vítimas não se apercebem do furto e não reclamam o estorno da operação ilícita, permitindo a alta lucratividade destes agentes.

Este tema certamente mereceria atenção especial de nosso legislador, evitando-se com isto que nossos julgadores sejam obrigados a interpretar e aplicar ou não a norma existente frente ao direito penal mínimo.

---

[167]GOIS JR, José Caldas. op. cit., p. 120.
[168]NUCCI, Guilherme de Souza. op. cit., p. 719.
[169]A expressão utilizada por Alexandre Jean Daoun *in* BUSCALEGIS. Disponível em: <http://www.buscalegis.ufsc.br/revistas/index.php/buscalegis/article/viewFile/10722/10287>. Acesso em: 14 jan. 2010.

8.2.3. Do furto de uso

Questões interessantes ainda não julgadas pelas Cortes superiores passam a existir com o mundo virtual. A respeito, temos o furto de uso, praticado em um computador. Provavelmente, por interpretação analógica, se apliquem os mesmos critérios do furto de uso comum ou seja, conduta atípica.

Outra solução para sua incriminação seria pelo furto de energia, o que, como posicionado pela mesma autora[170], se demonstra excessivo, já que a energia subtraída foi irrisória.

Para o furto de uso do computador, muitas vezes repetido, melhor solução seria um tratamento especial, em legislação específica.[171]

8.2.4. Do estelionato

O estelionatário encontrou na *internet* um campo fértil para a prática delitiva. Através dela ele pode obter vantagens ilícitas sem o risco de mostrar seu rosto, sua identidade ou de ser preso em flagrante, aplicando apenas suas habilidades, agora também informáticas.

No estelionato a vítima sofre um prejuízo patrimonial ao ser ludibriada pelo infrator. Na *internet*, mundo ainda desconhecido para a maioria dos usuários, o infrator encontrou mais instrumentos capazes de enganar a vítima, obtendo com isto sua vantagem indevida mais facilmente.

O estelionatário sabe que o internauta é identificável através do rastreamento da rede, todavia há mecanismos de ocultar tal identificação. Como exemplo, temos a denominada conexão anônima; nela, o provedor, com o falso *slogan* de democratizar a *internet*, promete não identificar o internauta. No Brasil, o IG (www.ig.com.br) surgiu com tal propaganda e nos primeiros quinze dias de sua criação captou mais de 14 mil usuários.

---

[170]FERREIRA, Ivette Senise. op. cit., p. 216.
[171]Id., loc. cit.

Visando ainda a obtenção de vantagem patrimonial, através da *internet* surgiu o *phishing scam;* nele o internauta envia *e-mails* contendo mensagens falsas com o escopo de capturar dados pessoais e financeiros dos destinatários.

A vítima, no instante em que clica a mensagem fraudulenta, inicia a instalação de um programa malicioso, seguida de uma mensagem de erro. Em seguida são abertas páginas falsas de formulários para a coleta de informações da vítima. No próximo passo, quando o usuário acessar os *sites* bancários, estes serão substituídos para *sites* redirecionados, onde o infrator conhecedor dos dados e senhas pessoais do usuário poderá de qualquer lugar ligado à *internet*, acessar sua conta bancária e efetuar operações financeiras como se fosse o usuário. Se, exemplificando, utilizasse um usuário falso ou de outrem ou acessasse a rede através dos denominados sítios de acesso anônimo, as chances de ser identificado seriam mínimas.

Da mesma forma, criminosos, com o fim de obter os dados da conta corrente e das senhas dos usuários, criam uma *homepage* falsa como se fosse a *homepage* de uma instituição financeira – quando o acionista acessa a *homepage* do banco na verdade estará acessando uma *homepage* falsa, idêntica a de sua instituição financeira. Nela ele digita seus dados pessoais e senhas imaginando estar realizando uma operação financeira, mas de fato está entregando aos criminosos todos os seus dados necessários para realizarem operações financeiras em sua conta como se ele fosse. No final, quando clica *enter* para comandar sua operação dá um erro de conexão.[172]

Nova modalidade de execução do crime de estelionato foi identificada recentemente pela Polícia Federal em São Paulo. Na operação batizada de "tentáculos", deflagrada com o auxílio da Caixa Econômica Federal, a Polícia prendeu onze pessoas que, por meio de máquinas de cartão de crédito e débito adulteradas, instaladas em estabelecimentos comerciais, por vezes com a leniência do próprio comerciante, obtinham a senha de cartões de crédito e débito dos clientes. Estes, ao digitarem a senha nas mencionadas máquinas de pagamento, enviavam-na, sem que soubessem, a um *lap top* conectado à rede de *internet* por meio da tecnologia *wireless*, em poder dos criminosos. Em poder das senhas, os estelionatários efetuavam saques em caixas eletrônicos e compras de joias, as quais eram vendidas a receptadores.[173]

---

[172]INELLAS, Gabriel Cesar Zaccaria de. op. cit., p. 18.
[173]FOLHA.COM. Disponível em: <http://www1.folha.uol.com.br/cotidiano>. Acesso em: 19 abr. 2011.

Portanto, um *tracker* pode, em poucas horas, subtrair altos valores da conta de correntistas sem sair de sua casa. Se for atento quanto à transferência destes valores para a conta de um laranja que – passando-se por ele, rapidamente saca o dinheiro e utiliza-se da conta falsa de um internauta – dificilmente será descoberto.

8.3. Dos crimes sexuais

Alguns crimes sexuais não serão consumados via *internet*, como é o caso do estupro. Todavia, outros delitos como a pornografia infantil ganharam com a *internet* um amplo espaço para a prática criminosa.

8.3.1. Da pornografia infantil

A *internet* é um espaço virtual onde o internauta navega livremente, tendo a livre escolha de, normalmente por tema, pesquisá-lo e até comercializá-lo.

Dentre os assuntos mais pesquisados na *internet* pelos internautas está a pornografia. O homem criou na *internet* redes de filtros visando a restrição destes sítios para menores de idade com avisos de "proibido para menores de dezoito anos", "só entre se for maior de dezoito anos", mas esta constatação da correta informação fornecida pelo usuário ainda é precária. Ignorando ou falseando a verdade nestes filtros, qualquer criança ou adolescente que almeja navegar em *sites* pornográficos facilmente alcança seu intento.

Basta escrever em um *site* de pesquisa "mulher pelada" e lincar imagens que, em segundos, você terá várias imagens de mulher nua, sem qualquer dificuldade.

Neste espaço virtual, onde o tema pornográfico é amplamente divulgado, alguns internautas, muitas vezes pela facilidade, procuram acessar imagens pornográficas envolvendo crianças ou adolescentes.

Assim, muitas pessoas em busca de lucro ou para satisfazer sua vaidade ou libido divulgam fotografias ou vídeos de menores de idade na rede, praticando o ilícito penal contido no artigo 241 do Estatuto da Criança e do Adolescente.

O número de casos envolvendo este ilícito, alterado e adaptado à era digital em 2008, é muito elevado. Tanto que há relatos de que mensalmente são criados mil novos *sites* de pedofilia.[174]

Um dos motivos que levam os infratores a praticar sem maiores preocupações tais ilícitos está na própria dificuldade em se apurar e punir os infratores. A própria autoria, em vários casos sem perícia, não consegue ser alcançada.[175]

Sobre a própria tipicidade da norma não se tem uma definição precisa de nu artístico, pornografia e sexo explícito. Estes temas inclusive, com a evolução social, vivem em constante mutação. Portanto, o que hoje é considerado como conduta reprovável amanhã pode ser aceito em nossa sociedade ou ainda o que para um determinado Estado é pornografia, para outro é arte.

Sobre o *locus delicti*, se um agente em um *site* localizado em país estrangeiro divulga imagens pornográficas de menores de idade na *internet* em vários países, dentre eles o Brasil, qual seria o país apto a apurar e punir o infrator? Se outros sítios disponibilizassem as mesmas imagens responderiam pelo mesmo crime? E se se tratassem de *sites* de hospedagem gratuita como o hpG mantido pelo IG, que armazena milhares de páginas recebidas diariamente e a princípio desconhece o conteúdo do que ali está mantido? Se tais *sites* estivessem localizados em outros países, qual ou quais países teriam soberania para apurar os fatos?

Este envolvimento de várias nações na prática delitiva informática, mais comum do que parece, motivou a escolha deste trabalho. Se não for enfrentado mundialmente, de nada

---

[174]DIGA não à Erotização Infantil. Pedofilia na internet: números no Brasil são assustadores. Disponível em: <http://diganaoaerotizacaoinfantil.wordpress.com/2007/08/11/pedofilia-na-internet-numeros-no-brasil-sao-assustadores/>. Acesso em: 10 mar. 2011.

[175]EMENTA: "Crime de Computador": publicação de cena de sexo infanto-juvenil (E.C.A., art. 241), mediante inserção em rede BBS/Internet de computadores, atribuída a menores: tipicidade: prova pericial necessária à demonstração da autoria: HC deferido em parte. 1. O tipo cogitado – na modalidade de "publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente" – ao contrário do que sucede por exemplo aos da Lei de Imprensa, no tocante ao processo da publicação incriminada é uma norma aberta: basta-lhe à realização do núcleo da ação punível a idoneidade técnica do veículo utilizado à difusão da imagem para número indeterminado de pessoas, que parece indiscutível na inserção de fotos obscenas em rede BBS/Internet de computador. 2. Não se trata no caso, pois, de colmatar lacuna da lei incriminadora por analogia: uma vez que se compreenda na decisão típica da conduta criminada, o meio técnico empregado para realizá-la pode até ser de invenção posterior à edição da lei penal: a invenção da pólvora não reclamou redefinição do homicídio para tornar explícito que nela se compreendia a morte dada a outrem mediante arma de fogo. 3. Se a solução da controvérsia de fato sobre a autoria da inserção incriminada pende de informações técnicas de telemática que ainda pairam acima do conhecimento do homem comum, impõe-se a realização de prova pericial. (STF. HC 76689/PB. Rel. Min. Sepúlveda Pertence. j. em 22.09.98).

adianta definir os crimes informáticos, suas sanções, investir em técnicas aptas a encontrar os agentes, divulgar medidas preventivas, dentre outras.

8.4. Dos crimes contra a propriedade intelectual

Um crime informático muito praticado é a chamada pirataria cibernética, nela *trackers* ou meros internautas copiam programas, músicas, vídeos sem o consentimento do autor, ofendendo seu direito de proprietário.

8.4.1. Da violação ao direito autoral

Em abril de 1994, nos Estados Unidos, um operador de sistema da BBS Cynosure foi condenado à pena de 37 meses de prisão pela Corte Federal de Massachusets, por permitir a transferência de programas de computador protegidos pela *copyright* no valor de mais de um milhão de dólares.[176] [177]

Fora dos Estados Unidos este tipo de programa pode ser acessado através da BBS e posteriormente disponibilizado na *internet*.

A questão principal discutida no caso acima está relacionada à responsabilidade criminal pela cópia daquele que fornece acesso a material protegido por *copyright*, permitindo inclusive sua cópia (download).

8.4.1.1. Do MP3

Outro tema de grande discussão no mundo virtual está na gravação de MP3, tido pelo *site* de estatística www.searchterms.com como o assunto mais procurado na *internet*, superando o tema sexo, antigo campeão dos internautas.

---

[176] GOIS JR, José Caldas. op. cit., p. 155.

[177] BBS WIKI. Disponível em: <http://bbs.wikia.com/wiki/1994&ei=7gm7Tf79Mobd0QGCt_nfBQ&sa=X&oi=translate&ct=result&resnum=1&ved=0CCMQ7gEwAA&prev=/search%3Fq%3DBBS%2BCynosure%2B1994%26hl%3Dpt-BR%26rlz%3D1I7ADRA_pt-PT%26prmd%3Divnsb>.

Em síntese, esta tecnologia denominada MP3 permite a gravação de centenas de músicas com a mesma qualidade da gravação feita em um CD. Como o processo de gravação é digital pode ser feito quantas vezes for preciso, sempre com a mesma qualidade. Tal gravação poderá ainda ser enviada eletronicamente para qualquer internauta que receberá aquela quantidade de músicas a seu dispor com a mesma qualidade de quem enviou.

Esta difusão aumenta esta clandestina gravação de músicas violando os direitos autorais, gerando com isto enorme prejuízo aos autores, cantores, gravadoras e todos aqueles envolvidos com o mercado da música.

Existem *sites* especializados nesta troca de arquivos de músicas pela *internet* como o Napster. A justiça americana em 2000[178] entendeu que este *site* tinha condição de permitir que os usuários acessassem músicas sem a possibilidade de copiá-las e não o fez, portanto era responsável pelas mesmas e pela violação dos direitos autorais.

Para os advogados das gravadoras, a Nepster permitia a cópia de aproximadamente 14 mil canções por minuto.

8.4.1.2. Violação do direito do autor de programa de computador

A violação do direito autoral está tipificada no artigo 184 do Código Penal. Porém, quando o objeto de proteção é a propriedade intelectual de programa de computador, o legislador efetivou a criminalização através de lei específica, a saber: lei 9.609/1998.

A tipificação de delitos contra a propriedade imaterial tem esteio constitucional, eis que o artigo 216 da Constituição Federal preconiza a proteção aos bens de natureza imaterial, assim como procedido no artigo 5º, inciso XXVII do mesmo diploma legislativo.

O artigo 184 do Código Penal tem o escopo de proteger os direitos de autor, sendo o sujeito passivo o autor, conforme definição dada pelo artigo 11 da lei 9.610/1998. Neste artigo são tutelados, além dos direitos de autor, também aqueles que lhe são conexos.

[178] AGÊNCIA O ESTADO. Disponível em: <http://www.oestado.com.br>. Acesso em: 27 jun. 2000.

A leitura do propalado artigo nos demonstra que se trata de norma penal em branco, necessitando o exegeta da leitura da própria lei 9.610/98, a qual traz diversas definições complementadoras.

Estão abarcados no direito do autor tutelado pelo código penal o direito moral do autor, qual seja, o de reivindicar a autoria de sua obra; de ter seu nome, pseudônimo ou sinal identificado como do autor; o de integridade, para que não possa ser alterada; o de modificá-la, entre outros. Também é tutelado o direito patrimonial do autor, nos termos do artigo 28 da lei 9.610/98, como o de usar, fruir e dispor de sua obra, bem com autorizar sua utilização.

Os parágrafos do artigo 184 do Código penal trazem as formas qualificadas em relação ao 'caput', com pena majorada para reclusão de 2 a 4 anos, e multa.

Revela-se por demais importante a proteção dada pelo Código Penal, mesmo porque, com o advento das novas tecnologias, facilitou-se a violação aos direitos do autor através de sistemas informáticos.

Em tempos passados, para se copiar um livro o sujeito deveria reprografar a obra em sua totalidade ou, ainda, copiá-la. Atualmente, uma vez em arquivo digital, qualquer obra pode ser distribuída a um número de destinos sem limitação por um simples correio eletrônico.

Tal perigo correm a maioria das espécies de obras, como, por exemplo, uma obra literária que pode ser digitalizada e enviada a diversas pessoas indiscriminadamente, sem que seja observado qualquer direito ao autor. Podemos dizer, seguramente, que o advento da informática contribuiu para que fosse facilitada a violação aos direitos do autor, bem como a imediata propagação da obra.

No que diz respeito aos programas de computador, estes receberam especial atenção com o advento da lei 9.609, de 19 de fevereiro de 1998 que, já em seu artigo primeiro, delimita seu objeto de proteção, oferecendo ao intérprete a definição do que seria um programa de computador.

Devemos salientar que a propalada legislação não fala somente em delitos, pelo contrário, traz dispositivos pertinentes à proteção dos direitos de autor, sobre o registro, garantias aos usuários dos programas de computador, contratos de licença de uso,

comercialização, transferência de tecnologia e, em seu penúltimo capítulo, traz as infrações e penalidades, isto já no capítulo V.

Para o perfeito entendimento do quanto expendido sobre as questões penais, indispensável o cotejo entre a lei 9.610/98 e todos os dispositivos da lei 9.609/98.

Quanto ao delito previsto no "caput" do artigo 12 da lei 9.609, que tipifica a violação dos direitos de autor de programa de computador, temos a pena de detenção de seis meses a dois anos ou multa. Cabível, por ser delito de menor potencial ofensivo, o instituto da transação penal.

O parágrafo primeiro do mencionado artigo traz forma qualificada, sendo impingida pena de reclusão de um a quatro anos cumulada com pena de multa. Tal dispositivo legal traz a violação para fins de comércio sem autorização expressa do autor, ou de quem o represente.

O parágrafo segundo, que indica como pena aquela prescrita para o parágrafo anterior, tipifica a venda, exposição à venda, introdução no país, aquisição, ocultação ou manutenção em depósito, para que seja destinado ao comércio, via original ou cópia de programa de computador produzido com violação ao direito autoral.

O que se nota da leitura dos artigos supra é que as formas qualificadas visam impedir e punir a utilização comercial, em todas as suas facetas, daquilo que advém da violação ao direito autoral de programa de computador.

Ainda no estudo do artigo 12, temos que o parágrafo terceiro indica que os delitos previstos no artigo 12 são de ação penal privada, exceto nos casos previstos nos incisos I e II do mencionado parágrafo.

8.4.2. Concorrência desleal

Em todo o mundo, com a crescente disputa de mercado e de concorrência, pessoas optam por criminosamente obter vantagem frente a seu concorrente.

Com a *internet* esta modalidade criminosa adquiriu novos meios de ser alcançada. Através da rede ficou mais fácil obter de um concorrente informações sigilosas contidas em seus arquivos eletrônicos.

Muitas vezes, casos que, num primeiro plano, assemelham-se ao crime de dano, na verdade, pela finalidade específica, trata-se de crimes da lei de propriedade industrial. Seria o caso do envio de um vírus que destrua os dados do disco rígido de um concorrente visando excluí-lo do mercado.

8.5. Alguns crimes informáticos em face da administração pública

Na análise dos delitos informáticos, temos, ainda, que dar atenção aos delitos que, por meio de sistemas, podem trazer prejuízos à administração pública, tanto os praticados por particulares ou pelos próprios funcionários públicos, sempre com atenção à possibilidade de coautoria, nos termos do artigo 30 do Código Penal.

Primeiramente, merece registro o delito acomodado no artigo 153, § 1º - A do Código Penal que nos traz a divulgação de informações sigilosas ou reservadas, contidas ou não nos sistemas de informação ou banco de dados da Administração Pública.

Tal informação será sigilosa ou reservada se assim definida por lei e pode estar contida ou não em sistemas de informação ou banco de dados da administração pública, tutelando-se, assim, a inviolabilidade da informação e a necessidade de que a administração resguarde o sigilo dos seus dados.

A ação privada para o citado delito será de ação penal pública condicionada, exceto se da conduta decorrer prejuízo à administração, caso em que a ação penal será pública incondicionada. Ainda, pela pena de detenção de um a quatro anos, cumulada com multa, cabe a suspensão condicional do processo, nos termos do artigo 89 da lei 9.099/95.

O delito acima examinado foi acrescentado ao código penal pela lei 9.983/2000, eis que nosso legislador sentiu a necessidade de que o delito de divulgação de segredo, já previsto em nosso ordenamento, tivesse também a previsão de que a conduta fosse efetivada com o acesso a bancos de dados ou sistemas eletrônicos, inclusive aqueles pertencentes à administração pública.

Temos que nos dias atuais os grandes bancos de informação encontram-se em sistemas informáticos, inclusive os bancos de dados físicos estão sendo transportados para

os meios digitais, os quais evitam perdas de dados, têm mais fácil manuseio e também são de melhor armazenagem, motivo que justifica a inclusão de mencionado dispositivo .

Prosseguindo o estudo no código penal, temos o delito insculpido no artigo 313 - A do estatuto citado. Tal capitulação incrimina a inserção de dados falsos em sistema de informação ou facilitação para que terceiro assim o faça. Também merece punição a alteração ou exclusão indevida de dados corretos nos sistemas informáticos ou banco de dados da administração pública, para que seja obtida vantagem indevida para o próprio funcionário ou para outrem, ou, ainda, com o objetivo de causar dano.

Tal preceito também foi incluído no código penal pela lei 9.983/2000, tendo em vista a necessidade de que seja resguardada a confiabilidade dos dados contidos nos sistemas de informação ou bancos de dados da administração pública.

Neste caso, os núcleos típicos são inserir, facilitar a inserção, alterar ou excluir. Nos primeiros dois preceitos ocorre a inserção de dados falsos. Nos dois últimos, ocorrem a alteração ou exclusão de dados corretos. Em qualquer das condutas a base de dados ou sistema informatizado pertence à administração pública.

O final da capitulação exige o fim de obter vantagem indevida para si ou para outrem, ou a intenção de causar dano.

O preceito em análise nos dá a pena de reclusão de dois a doze anos, cumulada com pena de multa.

Prosseguindo, temos a tipificação encetada pelo artigo 313 B do Código Penal, que incrimina a modificação ou alteração, feita por funcionário, de sistema de informações ou programa de informática, sem a autorização ou solicitação da autoridade competente.

A capitulação visa a proteção dos sistemas de informação ou programas de informática utilizados pela administração pública, os quais só podem ter nova formatação ou diferente da original quando autorizados ou solicitados pela autoridade competente.

A pena impingida é de detenção de três meses a dois anos, cumulativamente com a pena de multa. O parágrafo único traz causa de aumento de pena, de um terço até a metade, nos casos em que a alteração ou modificação trouxer algum dano para a administração ou para o administrado.

Neste dispositivo, o agente responderá pelo crime mesmo que a modificação ou alteração esteja correta, desde que lhe falte autorização para tanto. Se a inserção de dados resultar em dano, se praticado dolosamente, responderá pelo artigo 313 A; se culposamente, responderá pelo artigo 313 B, parágrafo único.

A análise efetuada no Código Penal encontra também o artigo 325, em seu § 1º, incisos I e II, também acrescentado pela lei 9.983.

O tipo traz o delito de violação de sigilo funcional e, em seu "caput", incrimina aquele que revela fato de que tem ciência em razão do cargo e que deva permanecer em segredo, ou facilitar-lhe a divulgação.

O parágrafo primeiro discorre que incide nas mesmas penas aquele que: i) permite ou facilita, com atribuição, fornecimento ou empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informação ou bancos de dados da administração pública; ii) utiliza-se, indevidamente, do acesso restrito.

No primeiro caso, o agente permite ou facilita que terceiro não autorizado tenha acesso a sistemas de informação ou banco de dados da administração pública através do fornecimento ou empréstimo de senha, ou qualquer outra forma.

Na segunda disposição legal, o agente se utiliza de acesso restrito, de forma indevida.

O preceito secundário veiculado para tal espécie delitiva é a pena de reclusão de dois a seis anos, e multa.

O dispositivo estudado mais uma vez mostra o zelo que se deve ter com o sigilo e a preservação dos bancos de dados e sistemas de informação da administração pública, sendo vedado o simples acesso de quem não tenha autorização para tanto.

8.6. Alguns crimes informáticos em leis extravagantes

Explorando a legislação criminal encontradiça fora do código penal brasileiro, também vislumbramos delitos que tenham relação com a informática, sendo que de alguns deles nos ocuparemos agora.

A lei 8.137, de 27 de dezembro de 1990, definiu os crimes contra a ordem tributária, econômica e contra as relações de consumo. Tal diploma, já em seus primeiros artigos, passa a tipificar os delitos contra a ordem tributária.

O artigo segundo da mencionada lei, em seu inciso V, informa ser crime contra a ordem tributária a utilização ou divulgação de programa de processamento de dados que permita ao sujeito passivo da obrigação tributária possuir informação contábil diversa daquela que é, por lei, fornecida à fazenda pública.

O mencionado inciso visa vedar a utilização ou divulgação de programa de processamento de dados que tenha o escopo de fraudar a fiscalização tributária por produzir informe contábil em desacordo com o que informado às autoridades competentes.

As condutas vedadas no mencionado dispositivo legal são a utilização ou divulgação de qualquer meio informático que vise burlar a fiscalização fazendária.

O preceito primário proclama uma pena de detenção de seis meses a dois anos, cumulada com pena de multa. Desta forma, cabível a transação e a suspensão condicional do processo.

Por fim, temos a análise da lei 9.504 de 30 de setembro de 1997, a qual estabelece normas para as eleições. A propalada legislação, em seu artigo 72, tipifica condutas que atentem contra o bom andamento do sistema eleitoral em desfavor da administração pública.

O primeiro inciso do citado artigo capitula a conduta daqueles que acessam o sistema de tratamento automático de dados utilizados pela justiça eleitoral, com o fim de alterar a apuração ou a contagem de votos.

O segundo inciso dá as condutas de desenvolver ou alterar comando, instrução, ou programa de computador capaz de destruir, apagar, eliminar, alterar, gravar ou transmitir dado, instrução ou programa ou provocar qualquer outro resultado diverso do esperado em sistema de tratamento automático de dados usados pelo serviço eleitoral.

Este inciso busca evitar qualquer tipo de alteração em programa utilizado pelo serviço eleitoral, bem como resultado diverso daquele para o qual foi criado determinado programa.

O terceiro inciso tipifica a conduta daquele que, propositadamente, causa dano físico ao equipamento usado na votação ou na totalização de votos ou a suas partes.

Este último inciso tipifica a conduta não daqueles que têm qualquer interferência no conteúdo ou programação informática dos equipamentos relacionados à justiça eleitoral, mas sim do agente que provocar, de forma proposital, danos físicos aos equipamentos, ou parte deles, utilizados na votação ou totalização de votos.

Para qualquer um dos incisos, é registrada pena de reclusão de cinco a dez anos, bem maior do que a pena de 6 meses a 3 anos de detenção aplicada ao crime de dano contra patrimônio público.

É de se registrar que a legislação que cuida das eleições andou bem nas analisadas tipificações, eis que busca resguardar a própria credibilidade das eleições, assunto de interesse não só da administração pública, mas de todo o país.

Em tempos passados, as votações eram realizadas com a utilização das cédulas de votação, que depois de depositadas nas urnas eram submetidas às longas apurações, as quais demoravam dias e se submetiam à contagem manual.

A justiça eleitoral brasileira na era digital teve evolução notável com a adoção da urna eletrônica, na qual o eleitor registra seu voto que é, posteriormente, repassado de forma eletrônica à justiça eleitoral para totalização. O sistema é totalmente eletrônico e o resultado das eleições é proclamado, no mais das vezes, no mesmo dia em que realizada a votação.

Assim, com a completa informatização do processo eleitoral brasileiro, o sistema jurídico agiu bem zelando por sua integridade e consequente credibilidade, adequando as normas penais à era informática.

CAPÍTULO V. SUJEITOS DO CRIME

Tão importante quanto a materialidade delitiva é o agente responsável por ela. De nada adianta comprovar a materialidade e a antijuridicidade se não encontrar seu autor.

Diversamente do crime comum, no informático, além das diferenças quanto ao *modus operandi*, princípio da territorialidade e do lugar do crime, temos significativas transformações quanto ao agente.

1. Sujeito ativo

Os sujeitos do crime, na era digital, sofreram mudanças na sua personalidade, forma de agir, idade etc. Passamos a ter que os analisar sob o prisma do sujeito real e do sujeito virtual para melhor conceituá-los.

1.1. Conceito

Sujeito ativo do crime informático, da mesma forma como conceituado no crime comum é aquela pessoa que pratica a conduta típica. Se ilícita e culpável, será responsabilizado pelo crime.

Em abril de 2010, foi constatado que, entre os brasileiros com idade superior a 12 anos, pelo menos 54% costuma acessar a *internet* (81,3 milhões de pessoas)[179]. Temos na era digital um número muito elevado de adolescentes utilizando-se do mundo eletrônico e, consequentemente, praticando condutas criminosas. Não obstante para o direito penal sejam inimputáveis, são passíveis de receberem Medidas Sócio-Educativas.[180]

---

[179]ESTATÍSTICAS sobre a Internet no Brasil. Disponível em: <http://www.tobeguarany.com/internet_no_brasil.php>. Acesso em: 14 jan. 2010.

[180]Art. 112. Verificada a prática de ato infracional, a autoridade competente poderá aplicar ao adolescente as seguintes medidas: I - advertência; II - obrigação de reparar o dano; III - prestação de serviços à comunidade; IV - liberdade assistida; V - inserção em regime de semi-liberdade; VI - internação em estabelecimento educacional; VII - qualquer uma das previstas no art. 101, I a VI. (BRASIL. Lei 8.069 de 13 julho de 1990. Dispões sobre o Estatuto da Criança e do Adolescente, e dá outras providências. *Diário Oficial da União*, Brasília, DF, 16 jul. 1990; ret. 27 set. 1990).

Momento apropriado para refletir a respeito da maioridade penal, mormente nos delitos informáticos.

1.2. Características do agente

Temos que os crimes informáticos não são praticados por leigos. O agente possui características diversas daquele criminoso comum. Em grande escala é inteligente, culto, alfabetizado, sem ou com reduzidos antecedentes criminais.

A primeira delas está ligada a um bom conhecimento em informática, pois sem ele dificilmente o agente conseguiria obter êxito em sua conduta, invadindo sistemas, adulterando ou destruindo dados. Através deste conhecimento, conforme falamos em capítulo próprio, o delinquente informático dificulta sua localização. Utiliza-se, dentre outros, de subterfúgios como provedores alienígenas, identificadores (IPs) falsos, locais públicos de acesso à *internet* conhecidos como *lan houses*, alterações de IP na mudança de provedores.

Não é demais afirmar, parafraseando a definição que Paulo José da Costa Junior dá ao estelionatário, que o criminoso que atua por meio do computador é o prestidigitador do direito penal, o intelectual do crime, tamanho o "engenho e arte" de que se mostra possuidor.

A cada dia os mecanismos de proteção a esses ataques e a identificação de seus infratores estão mais avançados, obrigando o agente a estar sempre em processo de evolução e a conhecer cada vez mais o mundo informático, a fim de obter êxito na sua conduta e no seu anonimato.

Ao quebrar uma barreira de proteção digital, aquele programa torna-se vulnerável e obsoleto. Rapidamente o mercado informático exige a criação de um novo protegendo a mencionada vulnerabilidade. Este é um dos motivos que transformou o mundo digital em um dos mais dinâmicos com que o homem já se deparou.

O criminoso informático, ao superar os bloqueios contra condutas proibidas, certamente terá um reduzido tempo de exploração para aquela conduta, até que novos

mecanismos impeçam sua prática. No instante em que novos mecanismos são criados, terá o criminoso que buscar novos caminhos para continuar a delinquir.

Em sua grande maioria os *crackers* conhecem duas ou mais línguas, geralmente a inglesa. Com isto conseguem navegar na *internet* em qualquer lugar do planeta com maior desenvoltura, ampliando suas possibilidades de cometimento de crime. Quanto mais línguas conhecer mais acessível a prática criminosa.

No início da era digital, tinha-se o infrator informático como uma pessoa incapaz de praticar um crime violento. Com o tempo este pensamento foi alterado, e hoje, através da *internet*, é possível assassinar pessoas ao enviar e comandar o disparo de um míssil ou de uma bomba.

Em 1983, o filme *War Games* contou a história de um *hacker* que invadiu os computadores do Departamento de Defesa dos Estados Unidos e tentou disparar um míssil contra a Rússia. Serviu como um marco ao estímulo de jovens que tentavam invadir o sistema informático do Pentágono, chegando a, pelo menos, duas tentativas de invasões diárias.[181]

Ainda quanto à sua personalidade, o agente do crime eletrônico dificilmente o praticaria se tivesse que agir em condições outras que não através da utilização de um aparelho ligado em rede. Por isto que se pode afirmar que a informática abriu um campo ao antigo e ao novo infrator.

1.3. Sua identificação

Pelo novo *modus operandi,* o crime informático é sempre praticado por meio de um computador ou aparelho ligado em rede. Isto torna ainda mais difícil a identificação do infrator. Estamos diante de um sujeito virtual comandado por um sujeito real.

Maciel Colli[182] classifica as pessoas por sua identidade visual caracterizada, dentre outras, por sua altura, cor, peso, voz, cabelo e pela sua identidade legal, caracterizada por

[181]SILVA, Rita de Cássia Lopes da. op. cit., p. 80.
[182]COLLI, Maciel. *Ciências penais:* perspectivas e tendências da contemporaneidade. A problemática detrás da responsabilização penal (objetiva) pela prática de um cibercrime. Curitiba: Juruá, 2011. p. 238-239.

números como certidão de nascimento, carteira de identidade. A primeira trata-se de uma identificação qualitativa, a segunda numérica. Estamos diante de um sujeito real.

Na informática, a identidade do agente possui tanto o aspecto qualitativo quanto o numérico. Temos nela três significativas distinções: a) na rede deve haver identidade qualitativa como o *host* e numérica como o IP; b) o agente será sempre identificado por seu aspecto qualitativo, e numérico e c) sempre terá um endereço numérico, mesmo que a ele relacionado por um curto período de tempo. Na informática nos defrontamos com o sujeito virtual.

Continua o autor, sob o enfoque do sujeito na era informática, a definir o endereço do IP como a identidade de um computador na rede. Como exemplo podemos ter em uma rede de *internet* sem fio (wlan) um *host* A, com um endereço de IP, um *host* B, com um endereço de IP e um roteador, com um endereço de IP. Cada uma destas máquinas possuidora de um IP terá a ela associada um novo identificador denominado *MAC*. Este endereço *MAC* possui um número exclusivo que identifica a interface de rede responsável pela comunicação de uma máquina com a outra. Cada interface possui um número de endereço *MAC*.

Quando um *host* A envia uma comunicação para um *host* B existe um protocolo responsável por esta realização de endereço IP com o endereço *MAC*, denominado *ARP* (Address Resolution Protocol). Desta forma quando um *host* A envia uma comunicação ao *host* B denominada *ARP Request packet*, se respondida teremos uma *ARP Reply packet*.

Os provedores de *internet* são os detentores dos endereços IPs que, quando solicitados por seus clientes, os emprestam naquele momento de conexão na *internet*. Este endereço de IP está relacionado àquele usuário, naquele determinado período de conexão à rede; se, posteriormente, for novamente utilizá-la, um novo número de IP será a ele fornecido.

Assim, se não tivermos identificado o período em que a conduta foi praticada, mesmo que identifiquemos o IP e o provedor de acesso, não identificaremos o usuário final, já que em fração de minutos poderemos ter naquele mesmo IP mais de um usuário.

Concluindo a identificação da comunicação em rede, temos um computador identificado por um endereço IP exclusivo, fornecido por um provedor que, ao comunicar-

se com outros computadores e sistemas desta mesma rede, terá um endereço *MAC* desta interface de rede, que se correlacioná com o endereço IP através do protocolo *ARP*.

Denota-se que na informática sempre teremos a identificação do sujeito através de seu endereço IP. Para identificarmos o agente temos que, primeiro, identificar a correlação do endereço IP com a máquina naquele exato espaço de tempo e, em seguida, encontrar a correlação entre a máquina e o verdadeiro sujeito que a opera naquele determinado espaço de tempo.

Para tanto, inicialmente, deve-se identificar o número de IP. Superada esta etapa, busca-se o provedor detentor daquele endereço IP. Neste momento identifica-se o período em que este IP praticou a conduta para daí o provedor conseguir identificar o usuário que, naquele determinado período, utilizou-se daquele endereço IP. Através do usuário busca-se a identificação da pessoa que contratou aquele serviço de acesso à *internet*.

Aparentemente, desde que identificado o IP, o exato momento em que a conduta foi praticada e o provedor de acesso, denota-se fácil a identificação do agente. Na verdade, só aparenta fácil a mencionada identificação. A informática possui muitos procedimentos complexos e falhos que necessitam, com urgência, de reparação e, mesmo quando reparadas, novos caminhos surgirão burlando as regras. Antes da era digital não havíamos nos defrontado com tamanha dificuldade. Deve o direito, na medida do possível, se adequar a esta realidade.

Vejamos um caso prático trazido por Colli[183], a fim de identificar uma pessoa que praticou uma conduta através da *internet*. Se superada a identificação do IP, de seu provedor e da conta do usuário não necessariamente identificamos a pessoa que praticou aquela conduta.

Se buscarmos a pessoa responsável por determinada navegação na *internet*, realizada através de uma rede de *internet* sem fio (wlan), para a prática delituosa, através do roteador *wireless*, se superadas as etapas anteriores, identificaremos o IP do roteador *wireless*.

Portanto, no instante em que o provedor fornecer a identidade IP do usuário, esta será daquele roteador *wireless* que contratou aquela prestação de serviço de acesso à *internet* e não do verdadeiro usuário que se utilizou dela para a prática criminosa.

---

[183]COLLI, Maciel. op. cit., p. 240-241.

Para identificar o mencionado usuário é necessário verificar se este roteador *wireless* possui *data logging*. Existindo, o que ainda é incomum, consegue-se identificar o endereço MAC do suposto usuário e com ele correlacionar o endereço IP com a máquina utilizada pelo usuário.

Todavia, é muito comum os criminosos utilizarem um programa que falsifica o MAC, denominado *MAC spoofing*, desaparecendo com uma das únicas possibilidades de se identificar a máquina responsável por determinada navegação e seu autor. Aos conhecedores de informática que dela se utilizam para a prática criminosa, certamente tal camuflagem é de grande utilidade.

Por fim, ainda sobre a dificuldade de se identificar o sujeito do crime, mesmo que superadas todas as etapas acima apresentadas, encontrando a máquina responsável por aquela navegação na *internet*, não se pode, com certeza, assegurar que seu proprietário foi de fato a pessoa que realizou aquela conduta.

Muitos são os casos de pessoas que dividem a utilização de um computador ou emprestam para terceiros, que emprestam para outros, sem a menor cerimônia ou cautela. Mesmo dentro de uma residência, o computador, registrado em nome de um proprietário, na maioria das vezes é utilizado por toda a família, parentes e amigos. Quem poderá garantir, com precisão, que o autor daquela conduta é o proprietário daquele computador?

Concluindo diretamente pela responsabilidade do proprietário do computador estaríamos abarcando a responsabilidade objetiva, inaplicável ao direito penal.

Não há meio capaz de afirmar com precisão se o indivíduo é realmente quem se diz ser. Não se tem notícia da exigência de registrar-se para navegar na *internet*. Inexiste controle que assegure que uma mensagem identificada de um procedente seja de fato dele. Uma mensagem pode ser alterada simulando que procede de uma pessoa ou *site* diverso daquele que de fato a originou, sem que sua procedência seja descoberta. Não se pode na *internet* sequer identificar com precisão o emitente, já que os nomes de domínios são adotados livremente, como também não se pode identificar de forma imediata em que país se encontra o emitente, dificultando ainda mais a identificação física do agente.[184]

[184]LÓPEZ ZAMORA, Paula. op. cit., p. 92.

Colli[185], pronunciando-se a respeito, sustenta que uma forma de se evitar este problema seria a prisão em flagrante. De fato, nos casos de prisão em flagrante, o mencionado problema desapareceria, todavia sabemos que os casos de flagrante são mínimos. Teríamos que ter um policial próximo a cada computador ligado em rede, o que seria praticamente impossível, levando-se em conta que usuários podem se encontrar em locais não públicos, como a própria residência, impedindo o acesso de um policial, que até aquele momento teria dificuldade em adentrar aquela residência e poder constatar a flagrância delitiva.

Urge, portanto, a criação de mecanismo identificador universal de todos os usuários. Esta identificação poderia ser a biométrica, com leitor existente em cada máquina apta a navegar na *internet*. Só então, e desde que criada legislação em todo o planeta, impedindo o acesso à *internet* sem a mencionada identificação, teremos, até que os criminosos especialistas encontrem uma forma de burlar tal mecanismo, solucionado o problema da identificação. Isto se de fato todas as nações, através de lei, obrigassem aos provedores de acesso a só fornecerem o direito à navegação mediante a mencionada identificação.

1.4. *Hacker* e *Tracker*

Conforme já escrito acima, aquele que aproveita seu grande conhecimento em informática para por meio dela obter vantagem indevida possui traços de maior intelectualidade, normalmente não possui antecedentes criminais, trata-se de grande conhecedor também em assuntos gerais, dificilmente praticaria a conduta senão através de um computador, não possui traços de pessoa violenta, na maioria das vezes fala ao menos duas línguas.

Sobre o *hacker* e o *tracker*, podemos defini-los como grandes conhecedores de informática, capazes de criar programas, montar e desmontar computadores, navegar na *internet* e adentrar e sair de programas sem serem percebidos.

---

[185]COLLI, Maciel. op. cit., p. 242-244.

O termo *hacker* criado no *Massachusetts Institute of Technology* foi definido aos estudantes de computação que viravam as noites pesquisando nos laboratórios. São os denominados especialistas em computador[186]. Considera-se a tradução mais adequada a este termo a de fuçador.[187]

Os *hackers*[188] utilizam seus conhecimentos informáticos para a prática de condutas em grande parte não criminosas, invadem sistemas informáticos para provar que são frágeis ou mesmo para se promover, alimentar o ego.

São pessoas que dominam mais de um idioma, buscam a fama, ainda que a relacione ao seu pseudônimo. Por vezes, observa Roberto de Araújo Chacon de Albuquerque, tais *hackers* tornam-se consultores em segurança de redes.[189]

Rita da Silva[190] distingue hacker em ético e não ético, este último denominado *cracker*. O primeiro utiliza seus exímios conhecimentos em informática para solucionar problemas criados pelos *crackers*. São capazes de entrar, corrigir e sair de um sistema sem deixar nenhum rastro, na maioria das vezes instalam uma porta de exclusividade para garantir seu acesso e sua autoria quanto ao procedimento por ele realizado.

O *cracker* é, da mesma forma, grande conhecedor em informática, mas utiliza seus conhecimentos para a prática de condutas ilícitas. É o *hacker* malicioso ou não ético.

Para Alexandre e Opice Blum[191], o nome *hacker* acabou sofrendo desvio conceitual na medida em que foi sendo pela mídia divulgado como um indivíduo que pratica crimes virtuais. Aduzem ainda os autores citados que o termo *cracker* é mais comumente utilizado para designar o *hacker* malicioso, dotado de mente criminosa.

---

[186]SILVA, Rita de Cássia Lopes da. op. cit., p. 77.

[187]MARZOCHI, Marcelo de Luca. *Direito.br*: aspectos jurídicos da internet no Brasil. São Paulo: LTr, 2000.

[188]Alexandre Daoun divide os *hackers* em *hacker*, no sentido estrito do termo, como sendo uma pessoa que explora os detalhes mais íntimos dos programas de computador. É uma pessoa com grande capacidade técnica sobre os sistemas de informática e que não pratica crime, apenas é um pesquisador. Por outro lado, define como *cracker* o *hacker* malicioso, ou seja, o indivíduo que possui o conhecimento que tem de informática para praticar crimes. Cecílio Terceiro, por sua vez, esclarece que "genericamente ***HACKER*** é uma denominação para alguém que possui uma grande habilidade em computação. ***CRACKER, BLACK-HAT*** ou ***script kiddie*** neste ambiente denomina aqueles ***hackers*** que têm como hobby atacar computadores. Portanto a palavra *hacker* é gênero e o ***cracker*** é espécie". (TERCEIRO, Cecílio da Fonseca Vieira Ramalho. *O problema na tipificação penal dos crimes virtuais*. Disponível em: <http://www.ibccrim.org.br>. Acesso em: 15 jun. 2002).

[189]ALBUQUERQUE, Roberto de Araújo de Chacon de. op. cit., p. 4.

[190]SILVA, Rita de Cássia Lopes da. op. cit., p. 78.

[191]DAOUN, Alexandre Jean; BLUM, Renato M. S. Opice. *Cybercrimes.* In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto (Coords.). *Direito & internet*: aspectos jurídicos relevantes. São Paulo: Quartier Latin, 2008. p. 122.

Tem-se ainda no mundo digital aqueles denominados *lamers* que se consideram grandes conhecedores, mas na verdade não passam de principiantes; o *wannabe* também principiante que navega com prudência; o *larva* que está se transformando em *hacker*, já conseguindo desenvolver um próprio programa; *phreaker* que associa a computação com a telefonia; o *cardens* um *tracker* especialista em fraudes com cartões de crédito e por fim o *guru* tido como o grande *hacker*.[192]

Neste diapasão, tem-se que o *cracker* é um conhecedor de informática que a utiliza para a pratica delitiva, mas nem todo crime informático será por um *cracker* praticado. Podemos ter um leigo em informática praticante deste crime.

Temos ainda pessoas que definem o infrator de informática como o *hacker*[193], mas nos dias atuais tal definição passou a ser considerada inadequada, pois ele pode praticar um crime informático como qualquer pessoa que, através de um computador, pratique um delito, mas não se pode associar o infrator do crime informático ao *hacker*, pessoa de grande conhecimento informático.

2. Sujeito passivo

No mundo informático nota-se uma crescente mudança da figura do sujeito passivo. Nos cibercrimes, pelo poder aquisitivo, a pessoa jurídica passou a ser o grande alvo dos criminosos. Através da *internet* esta ficou muito mais acessível ao infrator.

Sempre se falou da cifra oculta da criminalidade, também denominada cifra negra definida como aquela não informada às Autoridades. Sergio Salomão Shecaira escreve que a cada crime informado aos Órgãos Públicos, estima-se que outros dois deixam de sê-lo. No entanto estas cifras diziam respeito, na maioria das vezes, a crimes de violência doméstica e sexuais.[194]

---

[192]SILVA, Rita de Cássia Lopes da. op. cit., p. 78.

[193]Para Paulo M. Ferreira Lima, "os *hackers* são, em regra, invasores dos sistemas eletrônico que, por espírito de emulação, estariam desafiando seus próprios conhecimentos técnicos e a segurança de sistemas informatizados de grandes companhias e organizações governamentais. LIMA, Paulo Marco Ferreira. op. cit., p. 72.

[194]SHECAIRA, Sergio Salomão. *Criminologia.* 2. ed. rev., atual. e ampl. São Paulo: Ed. Revista dos Tribunais, 2008. p. 336.

Paulo Lima salienta que quando as vítimas são grandes empresas, normalmente não fazem as devidas comunicações à polícia, com vistas a evitar publicidade negativa. Não obstante a omissão em prestar as comunicações, acredita-se, continua o autor, que as instituições financeiras são as maiores vítimas dos cibercrimes.[195]

No final da década de noventa, de acordo com pesquisa feita pelo *Computer Security Institute* e pelo *Federal Bureau of Investigation* (FBI), 64% das empresas já tinham sofrido algum tipo de ataque virtual[196].

Para a Price Waterhouse, em período semelhante, 73% das empresas já teriam passado por algum problema na segurança informática.[197]

Em um dos poucos casos divulgados, no final da década de noventa, dois russos, a partir de São Petersburgo, invadiram o sistema informático do Citibank e desviaram para suas próprias contas bancárias o valor de US$ 10.700.000. Em 1997 avaliou-se que o prejuízo médio de um crime informático foi de US$ 567.000, enquanto o prejuízo médio de um roubo a uma agência bancária foi de US$7.500.[198]

Vê-se, assim, que não obstante os crimes cibernéticos sejam em sua maioria aptos a vitimar pessoa física ou jurídica, inclusive o Estado, como observado alhures, tem-se que as pessoas jurídicas são as principais ofendidas por tal espécie delituosa. Além de figurar no cibercrime como a principal vítima, sua posição nesta seara se mostra merecedora de muita atenção, como se verá adiante.

2.1. O infrator como herói – denúncia *versus* exposição da vítima

Tem-se ainda na informática um sentimento de insegurança porquanto não se enxerga a forma como seus comandos são enviados, tampouco o outro lado da rede. Este receio se acentua no comércio eletrônico. Muitas pessoas ainda têm receio de comprar produtos e operar movimentações financeiras na *internet* por medo de serem vítimas de crimes informáticos.

---

[195]LIMA, Paulo Marco Ferreira. op. cit., p. 66.
[196]ALBUQUERQUE, Roberto de Araújo de Chacon de. op. cit., p. 5.
[197]Id. Ibid., p. 70.
[198]Id., loc. cit.

No instante em que o mercado noticia que um serviço virtual de um grande banco ou departamento comercial foi vítima de uma conduta criminosa, em regra o prejuízo sofrido com a prática criminosa será bem menor do que aquele alcançado com a perda, pois haverá também crise de credibilidade daquele serviço e de futuras transações *on line*.

Foi publicado no jornal Folha de São Paulo, de 27 de abril de 2011, matéria informando que um invasor de rede quebrou a segurança informática da Sony e obteve dados pessoais como nome, endereço, endereço eletrônico, data de nascimento, senha e *login* dos jogadores *on-line* da PlayStation Network, que está fora de ar desde o dia 21 de abril de 2011. Ainda sob investigação a possibilidade de este invasor ter obtido também os dados dos cartões de crédito destes usuários[199].

O temor da perda de confiabilidade deste serviço faz com que muitas vítimas optem por, anonimamente, negociar com o criminoso oferecendo um valor econômico para cessar a invasão e, se possível, criar um mecanismo que as protejam daquele ataque.

Não são poucos os casos que tais sujeitos passivos contratam este infrator para trabalhar com eles com o objetivo de criar mecanismos capazes de proteger seus sistemas de violações informáticas.

Sandro D'Amato Nogueira recorda o caso emblemático no qual o criminoso virtual foi condenado pelo Juízo de Direito da Lapa, em São Paulo, a prestar serviço junto à Academia de Polícia, ministrando aulas de informática aos novos policiais civis, tamanho o seu conhecimento em sistemas de computadores.[200]

Para estas empresas, o acordo cessa imediatamente aquela vulnerabilidade, além de não permitir que se torne pública esta vulnerabilidade da segurança de seu sistema informático, o que, conforme já dito, em regra, levaria a um prejuízo muito maior do que aquele causado pelo infrator.

Tal postura é um estímulo à prática criminosa. Há uma espécie de competição entre os *trackers* para invadir os grandes e mais bem protegidos sistemas informáticos do planeta. Para eles o resultado delitivo pode gerar um prêmio econômico ou um bom emprego em vez de um processo criminal. O direito não pode permanecer inerte a esta

---

[199]INVASOR de rede obteve dados pessoais de usuários, diz Sony. Disponível em: <http://www1.folha.uol.com.br/tec/907412-invasor-de-rede-obteve-dados-pessoais-de-usuarios-diz-sony.shtml>. Acesso em: 27 abr. 2011.

[200]NOGUEIRA, Sandro D`Amato. *Crimes de informática.* Lema/SP: BH Ed., 2008. p. 31.

situação. Por mais que tal alternativa traga um ganho econômico à vítima, sua postura incentiva o infrator, além de permitir que haja impunidade do criminoso informático.

Da mesma forma como se criou o crime de receptação para desestimular o crime antecedente (contra o patrimônio), o direito penal deve coibir esta prática punindo aqueles que, além de não noticiar os delitos informáticos de ação penal pública incondicionada às autoridades, celebram com os infratores um acordo almejando o anonimato daquele acontecimento.

A sociedade, nos tempos atuais, na qual se constata uma enorme habilidade do infrator – parafraseando Paulo José da Costa Júnior – pelo crescimento do cometimento de crime com o emprego da violência, passa a nutrir certa indulgência e quiçá uma simpatia, uma admiração para com a figura do criminoso cibernético, principalmente aqueles que quebram barreiras de segurança como o sistema de defesa aérea americana ou de um banco de investimentos.[201]

O Professor José Renato Nalini também alerta que os criminosos modernos disseminam não apenas o mal concreto, mas também a idéia de que são Robin Hood modernos lutando contra o Estado opressor. Dessa forma, recrutam a nova geração para luta que, não raro, ganha apoio da opinião pública.[202]

Com o passar dos anos a informática vai se transformando em uma ferramenta cada vez mais indispensável às atividades humanas, mormente no *e*-comércio. O que antigamente através da *internet* era exceção, como pegar um extrato bancário, pagar uma conta, comprar um produto, está se tornando regra.

Neste sentido, temos a própria declaração de Imposto de Renda que, a partir deste ano, só pode ser apresentada à Receita Federal através da *internet*[203]. Existem empresas como a Submarino[204] que só comercializam seus produtos por meio da *internet*. Sem ela o consumidor não consegue obter tal comercialização. Isto cria ao criminoso um ambiente promissor, mormente quando se tem notícia de que a vítima prefere, pelos motivos já expostos, premiá-lo pelo ataque do que processá-lo.

---

[201]COSTA JR., Paulo José da. *Código Penal comentado.* 9. ed. rev. e atual. São Paulo: DPJ Ed., 2007. p. 536.
[202]NALINI, José Renato. *Justiça.* São Paulo: Ed. Canção Nova, 2008. p. 125.
[203]IDG NOW. Disponível em: <http://idgnow.uol.com.br/internet/2010/02/11/em-2011-declaracao-do-imposto-de-renda-sera-feita-apenas-pela-internet/>. Acesso em: 27 abr. 2011.
[204]SUBMARINO. Disponível em: <http://submarino.com.br>. Acesso em: 27 abr. 2011.

CAPÍTULO VI. LEIS, PROJETOS E CONVENÇÕES SOBRE OS CRIMES INFORMÁTICOS

Pode-se afirmar que a informática é um dos temas de mais intensa mutação. Urge, ao abordar a questão da aplicabilidade da lei penal nos delitos informáticos, analisar os projetos e as leis a respeito.

O direito comparado, muitas vezes, deve ser analisado com ressalva, pois traz normas adequadas a determinada região, com seus hábitos e costumes, que, certamente, são diversos dos de outra região. No entanto, quanto ao tema central deste trabalho, *locus delicti* no mundo virtual, dada sua internacionalização, a legislação estrangeira, além de superar estas ressalvas, passa a ser indispensável.

1. Leis no Brasil

No Brasil não há uma lei especial que trate dos crimes cibernéticos. Quatro leis, como mencionado alhures, incriminam condutas relacionadas à informática. São elas:

a) Lei nº 9.296, de 24 de junho de 1996: regulamenta a interceptação de comunicações telefônicas, criminalizando a conduta consistente em realizar interceptação de comunicações telefônicas, de informática ou telemática ou quebra de segredo de justiça com pena de dois a quatro anos e multa.

b) Lei n° 9.609, de 19 de fevereiro de 1.998: dispõe sobre a propriedade intelectual de programa de computador e sua comercialização. Criminaliza a conduta consistente em violar direito do autor de programa de computador, atribuindo-lhe pena de seis meses a dois anos de detenção ou multa, e de um a quatro anos de reclusão e multa se a finalidade for comercial.

c) Lei nº 9.983, de 14 de julho de 2000: Legislação que altera dispositivos do Código Penal. Dentre aqueles ligados à informática, a norma criou o parágrafo 1º A, do artigo 153, criminalizando a divulgação de informações sigilosas ou reservadas, contidas ou não nos sistemas de informações ou bancos de dados da Administração Pública. Criou ainda os artigos 313, A e 313, B, que, respectivamente, criminalizam a inserção de dados

falsos em sistema de informações e a modificação ou alteração não autorizada de sistema de informações. Acrescentou o parágrafo primeiro ao artigo 325 criminalizando, em seu primeiro inciso, a conduta de permitir ou facilitar mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, acesso de pessoas não autorizadas a sistemas de informação ou banco de dados da Administração Pública. No inciso seguinte pune também aquele que se utiliza do acesso restrito.

d) Lei nº 11.829, de 25 de novembro de 2008: altera dispositivos do Estatuto da Criança e do Adolescente. Acrescenta o artigo 241-A que criminaliza oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo explícito ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente.

2. Projetos de Lei no Brasil

O projeto de lei de relatoria do Senador Eduardo Azeredo, número 76/2000, substitutivo de outros três projetos (76/2000, 137/2000 e 89/2003), que altera e acrescenta dispositivos no Código Penal e no Código Penal Militar, trouxe grande discussão a respeito de sua aplicabilidade e eficácia.

Dentre estes dispositivos apresentados no projeto, pode-se destacar o roubo de senha, difusão de código malicioso, denominado *phishing*, falsificação de qualquer dispositivo eletrônico, crime contra a honra praticado pela informática, furto por uso da informática.

O projeto trouxe, ainda, um glossário, definindo termos informáticos, como sistema informatizado, rede de computadores, defesa digital, seguindo técnica utilizada pelo artigo 327 do Código Penal, que define funcionário público.

O Anteprojeto de Reforma da Parte Especial do Código Penal, atento à importância que se tem dado ao assunto, estampou dentre as condutas puníveis a violação de programa de computador.

> Art. 210. Violar direitos de autor de programa de computador: Pena – Detenção, de seis meses a dois anos, ou multa. § 1º Se a violação consistir na reprodução, por qualquer meio, de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente: Pena – Reclusão, de um a quatro anos, e multa. § 2º Na mesma pena do parágrafo anterior incorre quem vende, expõe à venda, introduz no País, adquire, oculta ou tem em depósito, para fins de comércio, original ou cópia de programa de computador, produzido com violação de direito autoral. Ação penal § 3º Nos crimes previstos neste artigo, procede-se mediante queixa, salvo: I – quando praticados em prejuízo de entidade de direito público, autarquia, empresa pública, sociedade de economia mista ou fundação instituída pelo poder público; II – quando resultar prejuízo à ordem tributária ou as relações de consumo.

Encerrou no § 1º do artigo 303 discussão sobre itens informáticos serem ou não considerados documentos, equiparando os dados, instrução ou programa de computador constante de processamento ou comunicação de dados ou qualquer suporte físico para fins penais ao documento.

O Brasil, conforme mencionado anteriormente, por ser um dos locais de maior incidência dos crimes cibernéticos, deve ter constante preocupação com o tema e criar, sempre que se fizerem necessárias, leis que regulamentem questões ligadas ao mundo cibernético e que tornem puníveis seus infratores. Em muitos casos bastará uma pequena adequação às normas já vigentes.

Até o presente momento as leis existentes não seguem à risca as diretrizes da Convenção de Budapeste, de 2001, sobre crimes cibernéticos. O projeto de lei do Senador Azeredo é o que se tem de mais próximo ao preconizado na Convenção.

3. Leis no exterior

Nos países estrangeiros, principalmente nos mais desenvolvidos, a batalha travada contra o cibercrime, por meio da criação de legislação que estabelece medidas preventivas e punem seus infratores, já foi iniciada há anos.

Os Estados Unidos da América são os precursores no que tange ao combate ao cibercrime, seguidos de Portugal, Espanha, Alemanha e Itália.

Os Estados Unidos da América[205] deram os primeiros passos contra a criminalidade informática a partir dos ataques terroristas às torres gêmeas em Nova Iorque no ano de 2001. Desde então, há muita preocupação com esta recente modalidade delitiva. São, inclusive, signatários da Convenção de Cibercrimes de Budapeste, de 23 de novembro de 2001.

No Canadá, no ano de 2003, crimes informáticos foram inseridos no Código Penal. Atualmente há previsão penal informática nas seções 183, 242.2, 326, 342, 342.1, 430 e 487 do Código Penal canadense. É o Canadá signatário da Convenção de Budapeste.

Em Portugal, desde 1991, há legislação específica denominada Lei de Criminalidade Informática. Trata-se da Lei 109/91, de 17 de agosto de 1991.[206] Denota-se que seu surgimento se deu antes dos ataques terroristas aos EUA em setembro de 2001 e da Convenção de Budapeste, da qual os lusitanos também são signatários.

Na Espanha, assevera Horacio Fernández Delpech, citado por Rômulo de Andrade Moreira, que a legislação "es muy completa y precisa, ya que tipifica la gran mayoria de las conductas antijurídicas que hemos considerado como delitos informáticos o como delitos que se pueden cometer por medios informaticos".

A Alemanha, signatária da Convenção de Budapeste, criminaliza delitos informáticos tais como a espionagem ou alteração de dados e a sabotagem por computador no próprio Código Penal.

Rômulo Moreira aponta que no Peru, não obstante a ausência de legislação específica, o certo é que

> la doctrina y jurisprudecia de esse país ha considerado asimiladas a ciertas figuras comunes del Código penal del Peru a este tipo de delitos (e que) no Chile, a Lei n° 19.223/93 tipifica una série de delitos relacionados con a informática, como a sabotagem e a espionagem.[207]

---

[205]USAPA – USA Patriotic Act – lei aprovada no final de 2001 para agilizar a captura e punição de ataques eletrônicos. Tornam alguns ataques de *hackers* atos terroristas, sujeitando a penas extremamente severas. Punem publicação de informações que possam causar danos aos EUA.
FISA – Foreign Intelligence Survailance Act – possibilita monitoramento de agentes especiais estrangeiros nos EUA e facilita atuação de americanos em casos internacionais.
CSEA – Cybersecurity Enhancement Act – prevê pena mínima de dez anos de prisão para quem pratica crimes eletrônicos e punição imediata para quem, ilegalmente, acessa informações *in* DE LUCCA, Newton; SIMÃO FILHO, Adalberto (Coords.). op. cit., v. 2, p. 431.

[206]Vide anexo inteiro teor.

[207]MOREIRA, Rômulo de Andrade. Globalização e crime. *Revista do Tribunais*, São Paulo, ano 92, n. 811, p. 469-496, maio 2003.

Na Argentina, país não signatário da Convenção de Budapeste, foi, em 2008, aprovado Ato de Proteção de Informações que criminaliza condutas praticadas por *hackers*. Trata-se da Lei 26.388/2008.[208]

O Chile, não signatário da Convenção de Budapeste, criou a Lei 19.223, publicada em 7 de julho de 1993. Nela estão tipificadas várias condutas praticáveis por meio de computador.[209]

4. Convenção de Budapeste

Logo após os ataques de 11 de setembro de 2001, em 23 de novembro de 2001, em Budapeste, Hungria, foi editada a Convenção Europeia sobre crimes informáticos. Seu objetivo, fundado na preocupação com o rompimento de fronteiras ocasionado no espaço cibernético, bem como com o avanço da criminalidade, é traçar diretrizes buscando uniformidade mundial legislativa.

Observam Gills Lopes Macêdo Souza e Dalliana Vilar Pereira que a Convenção tem por objetivo traçar uma política criminal que seja comum a todos os países signatários, com vistas a proteger a sociedade das condutas praticadas no ciberespaço. Para tanto, prega a adoção de legislação adequada e cooperação internacional sistematizada.

Além de leis e cooperação entre nações, a Convenção invoca a indústria privada como aliada estatal no combate ao crime no ciberespaço.

Consta de seu preâmbulo que haverão de ser respeitados a Proteção dos Direitos do Homem e das Liberdades Fundamentais do Conselho da Europa, o Pacto Internacional sobre os Direitos Civis e Políticos da ONU, a Convenção das Nações Unidas sobre os Direitos da Criança e a Convenção da Organização Internacional do Trabalho sobre as Piores Formas do Trabalho Infantil.

---

[208]Vide anexo inteiro teor.
[209]Vide anexo inteiro teor.

A Convenção de Budapeste definiu os cibercrimes entendendo-os como ofensas levadas a efeito contra os sistemas e os dados informáticos, as infrações relacionadas a computadores, seu conteúdo, pornografia infantil e ofensas à violação de direitos autorais.[210]

Hoje, quarenta e sete países são signatários da Convenção, dentre os quais Hungria, Estados Unidos, Itália, França e Japão; destes, trinta ratificaram-na.[211]

O Brasil, assim como os demais países da América do Sul, ainda não é signatário da Convenção de Budapeste. No entanto, o Projeto de Lei substitutivo de três projetos anteriores, de autoria do Senador Eduardo Azeredo, aprovado pelo Senado Federal, conforme já dito, está, em parte, redigido de acordo com as orientações da Convenção de Budapeste.

Aliás, é da justificativa do Projeto de Lei substitutivo a ressalva de que embora o Brasil não seja signatário da Convenção de Budapeste, pode ser considerado um país em harmonia aos seus preceitos, porquanto atenda às deliberações contidas em seu preâmbulo.

Demais disso, a preocupação em se fazer uma lei vazada nos estritos termos em que apregoados pela Convenção é estampada na justificativa constante do Substitutivo:

> O presente Projeto de Lei, que atualiza o nosso Código Penal, o Código do Processo Penal, o Código Penal Militar, a Lei das Interceptações Telefônicas, a Lei da Repressão Uniforme, o Código do Consumidor, a Lei Afonso Arinos e o Estatuto da Criança e do Adolescente, coloca o Brasil em posição de destaque para que possa tratar e acordar de maneira diferenciada com os países signatários da Convenção de Budapest e outras, inclusive os EUA, país sede das maiores empresas de tecnologia da informação e sede dos maiores provedores de acesso à rede mundial de computadores.[212]

---

[210]Trabalho apresentado nos Anais do 1° Seminário Cibercrime e Cooperação Penal Internacional, organizado pelo CCJ da UFPB e pela Association Internacionale de Lutte Contra la Cybercriminalite (França), João Pessoa/PB, maio de 2009. SOUZA, Gills Lopes Macêdo; PEREIRA, Dalliana Vilar. A Convenção de Budapeste e as leis brasileiras. *Ministério Público do Estado do Amazonas*. Disponível em: <http://www.mp.am.gov.br/images/stories/A_convencao_de_Budapeste_e_as_leis_brasileiras.pdf>. Acesso em: 10 mar. 2011.

[211]COUNCIL OF EUROPE. Convention on Cybercrime. CETS No.: 185. Disponível em: <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG>. Acesso em: 29 abr. 2011.

[212]Vide anexo inteiro teor.

Verifica-se, portanto, que malgrado não seja o Brasil signatário da Convenção, é fato que dentro em breve o será. Saliente-se, contudo, que a ratificação sem reservas da Convenção trará implicações de ordem constitucional ao ordenamento jurídico brasileiro, de sorte que não há se apontar morosidade do país pelo simples fato de ainda não ser signatário. Em outras palavras, conquanto legisle e puna os delitos consagrados na Convenção, não há se ter pressa ou atropelos na sua ratificação.

CAPÍTULO VII. SOBRE A LEI APLICÁVEL

É sabido que a *internet*, no modelo virtual, rompeu fronteiras com resultados no mundo real. Antes dela, para adentrarmos em território estrangeiro, necessitávamos de permissão de entrada, com apresentação de identidade, em alguns casos visto expedido pelo próprio país a ser visitado e fiscalização das Autoridades Portuárias. Hoje, neste novo mundo, o virtual, em fração de segundos, eletronicamente, entramos e saímos de qualquer território existente no planeta.

Como consequência desta mutação que possibilita qualquer usuário navegar pelo planeta, independente de raça, religião ou poder aquisitivo, veio também a possibilidade de, em fração de segundos, o usuário praticar condutas tidas como ilícitas em qualquer lugar por onde ele navegue.

A inexistência de fronteiras para a criminalidade informática, porquanto com uma simples troca de dados ou o mero envio de um *e-mail*, uma informação é enviada e transita por diversos servidores até que encontre o seu destinatário. Não há como o internauta prever o caminho, quais os servidores que serão utilizados para que sua mensagem encontre o destino que lhe é reservado. Lembra o autor que "um *e-mail* enviado do Brasil para os Estados Unidos pode passar pelo Reino Unido, caso o fluxo de dados entre aqueles países estiver congestionado".[213]

Isto quer dizer que mesmo que um usuário envie um *e-mail* para uma pessoa que se encontra em sua frente esta mensagem pode navegar por servidores diversos, inclusive fora daquela cidade, estado ou país.

Se até pouco tempo atrás, para infringir a lei penal o infrator necessitava ir fisicamente ao local do crime e praticar a conduta típica; com a tecnologia, passou a poder alcançar a ilicitude à distância. Assim acontecia com o envio de uma bomba relógio ou com a utilização de um rifle de grande alcance. Todavia, a maioria dos ilícitos penais necessitava da presença física do agente no local do crime.

Com o surgimento do computador e de sua conexão instantânea em todo o planeta, podemos, com facilidade, ter condutas no hemisfério norte e resultados no hemisfério sul.

---

[213]ALBUQUERQUE, Roberto de Araújo de Chacon de. op. cit., p. 64.

Esta possibilidade, alcançada pela tecnologia, criou debate e preocupação sobre qual lei deverá ser aplicável a estes casos.

Alguns escritores já se aperceberam da imprescindibilidade de discutir o assunto: "A determinação do lugar em que o crime se considera praticado (*locus commissi delicti)* é decisiva no tocante à competência penal internacional".[214]

Apoiando-se na teoria da ubiquidade, mais de um país pode considerar-se competente para julgar um crime informático. Basta que tenhamos conduta e resultado ocorridos em países distintos ou só resultados ocorridos em pelo menos dois países.

Apoiado pela teoria da ação ou da atividade, será apto a julgar um processo o país no qual a conduta foi total ou parcialmente produzida.

Para a teoria do resultado, o lugar do crime é o local da produção do resultado, o local onde as consequências ou os efeitos do crime se tornaram manifestos. Na tentativa delitiva, seguindo esta teoria, considera-se como lugar do delito aquele onde o resultado seria produzido.

Que teoria deve ser adotada para determinar qual o país soberano para julgar e processar crimes informáticos? Se um vírus for transmitido a partir de um sistema informático situado no Reino Unido e, logo em seguida, for disseminado para uma série de provedores, e, por conseguinte, para computadores presentes em outros países, as consequências ou os efeitos do crime tornar-se-ão manifestos em várias unidades soberanas.

O país com jurisdição para julgar e processar crimes informáticos seria aquele onde o autor do crime estava fisicamente presente, o país onde os dados foram enviados, o país onde o efeito foi produzido, o país onde o provedor de acesso está localizado, ou o país onde a prova pode ser mais facilmente coletada?

Pode ser tecnicamente impossível determinar em que país os dados se localizavam antes de serem modificados. A transmissão de dados pode envolver tantas unidades soberanas que se acabe por determinar o país onde as consequências ou os efeitos do crime se tornaram manifestos pela primeira vez de uma maneira exclusivamente fortuita.[215]

---

[214]JESUS, Damásio Evangelista de. *Direito penal*: parte geral. São Paulo: Saraiva, 1985. v. 1, p. 111.
[215]ALBUQUERQUE, Roberto de Araújo de Chacon de. op. cit., p. 64-65.

Diferentemente do que afirmava, com razão à época, o Professor José Maria Rodriguez Devesa, o criminoso não tem mais uma base territorial. O citado Professor ensinava, ao falar sobre os pressupostos para aplicação da lei penal, que, preliminarmente, para aplicar a lei penal, em qualquer situação, àquele que tenha praticado o crime, haja uma base territorial.[216]

Com a *web* o criminoso não tem mais base territorial definida. Se a punição estatal penal ficar condicionada à descoberta da base territorial do criminoso, muito dificilmente se punirão os crimes informáticos, pois desta espécie delitiva, quando muito, descobre-se seu resultado e autoria.

O local da prática, passível de situar-se em qualquer ponto do planeta, se resume a digitações em aparelhos fixos ou móveis acessados a provedores de comunicação.

O Professor Ulrich Sieber, conforme já mencionado, sugere uma proposta mediadora rechaçando a interpretação dogmática da norma. Assinala que há diferença entre tecnologia *push* e tecnologia *pull.* Seria a tecnologia *push,* segundo Sieber, a situação em que os dados ofensivos ao direito são enviados do estrangeiro a um determinado sistema informático, ao passo que a tecnologia *pull*, dar-se-ia quando os dados fossem acessados no estrangeiro, a partir do país em questão. Quando os dados são enviados por meio de tecnologia *push* o resultado se daria onde aqueles foram recebidos. Por outro lado, quando os dados gravados em servidor estrangeiro são acessados mediante tecnologia *pull* o país onde foi praticada a ação sobejaria importância para o direito penal.[217]

Em outras palavras, de acordo com o Professor Sieber, a atenção do direito de um país estaria voltada para o local onde o direito foi ofendido e não para o local onde a conduta foi praticada ou o resultado se consumou. A atenção se voltaria para o local do resultado se o país em hipótese fosse o local que tivesse recebido (tecnologia *push*) o conteúdo ofensivo ao seu ordenamento. Da mesma forma, a atenção se voltaria ao local da conduta se o mesmo país fosse o território de onde o infrator acessou e importou (tecnologia *pull*) os arquivos contrários ao direito.

---

[216]RODRIGUEZ DEVESA, Jose Maria. *Derecho Penal Español*: parte general. 9. ed. Madrid: Dykinson, 1985. p. 221.

[217]Citado por SÁNCHEZ GARCIA DE PAZ, Isabel; BLANCO CORDERO, Isidoro. Problemas de derecho penal internacional en la persecución de delitos cometidos a través de internet. *Actualidad Penal*, n. 7, p. 181, 11-17, feb. 2002.

No entanto, não nos resolveria o problema da necessária identificação do *locus delicti,* pois, se analisada a questão sob a ótica dos dois países, tanto o país de onde foi enviado o arquivo ofensivo quanto o país receptor se sentirão ofendidos pela conduta. Como se vê, a teoria não tem o condão de restringir a jurisdição, mas o de buscar subsídio para que cada país a amplie.

Nos delitos digitais, conforme será abordado nas próximas páginas, devemos olhar com mais atenção os princípios que norteiam a aplicabilidade jurisdicional, que não o da ubiquidade.

Neste sentido, Albuquerque sustenta que quando mais de um Estado se considerar competente para julgar um mesmo crime informático, surgirão conflitos difíceis de serem solucionados. Talvez fosse melhor rever os conceitos sobre o lugar do crime, podendo não impedir que mais de uma jurisdição esteja envolvida na investigação e julgamento de um mesmo delito. Na investigação, dados podem estar armazenados no exterior, devendo buscar cada vez mais instrumentos de assistência mútua em matéria penal.[218]

1. Nos crimes informáticos

A tecnologia advinda com a informática trouxe aos criminosos uma relação de custo-benefício altamente compensadora, proporcionando-lhes novos recursos técnicos para colocar bens jurídicos em risco.[219]

O infrator, pela maior dificuldade de apuração dos fatos e da autoria, preferirá diversificar e distanciar o local da conduta daquele, do resultado, principalmente se em um deles a conduta for atípica ou tiver sanção reduzida.

Sobre a colheita probatória nos crimes informáticos, aborda Albuquerque[220] que quatro hipóteses relativas à busca e apreensão *on-line* de dados situados no exterior, com diferentes consequências podem ser traçadas. Num primeiro momento, autoridades policiais podem se deparar com um terminal de computador, e nele visualizar dados que estão armazenados no exterior. Podem também encontrar um terminal e efetuar a busca e

[218]ALBUQUERQUE, Roberto de Araújo de Chacon de. op. cit., p. 66.
[219]Id. Ibid., p. 3.
[220]Id. Ibid., p. 69.

apreensão *on-line* sem sequer saber que os dados estão armazenados no exterior. Terceiro, a polícia depara-se com o terminal e efetua a busca e apreensão *on-line* conhecedora de que os dados estão armazenados no exterior e, por fim, as autoridades policiais podem utilizar seu próprio terminal para acessar dados, sabendo que eles estão armazenados no exterior.

Sobre a legalidade desta colheita, o mesmo autor conclui que as consequências jurídicas em cada uma das hipóteses mencionadas serão diferentes. Na primeira hipótese, não haverá qualquer óbice à consulta dos dados. A polícia encontrou um terminal conectado a uma rede de computadores, no qual os dados apareciam na tela do monitor, sem que ela adotasse qualquer medida. Na segunda hipótese, é necessário observar se as autoridades policiais agiram com boa-fé. Se com boa-fé se conduziram, a prova não deve ser considerada ilícita. Quanto à terceira e quarta hipóteses, a polícia agiu de forma alheia ao direito, de sorte que não podiam efetuar a busca e apreensão *on-line* de dados. O correto seria se socorrer da cooperação jurídica em matéria penal e seus instrumentos. A prova é, dessarte, ilícita.[221]

Quanto ao posicionamento de Roberto de Albuquerque, comungamos em parte. Sendo alienígena a prova colhida, mesmo que agindo o agente de boa-fé, deve ser considerada imprestável, pois falta-lhe os requisitos legais para sua colheita.

Como se vê, além da maior chance que tem de não ser descoberto ao final de uma investigação, ou de ser descoberto apenas através de prova ilícita, o agente do delito informático quase sempre afasta a prisão em flagrante e a apuração imediata dos fatos.

Subtrair fisicamente o cofre de um banco, conduta que exige certo número de agentes, alguns deles funcionários do banco, armamento pesado, prévio estudo da rotina do banco e de sua segurança, investimento financeiro e um pouco de sorte, é muito mais arriscado e oneroso que operar a subtração financeira por meio do computador, estando do outro lado da rua ou do planeta. Sem levar em conta que a subtração física do dinheiro certamente poderá ser muito menor que aquela ocorrida pela simples transferência eletrônica. Logo, a conduta praticada fisicamente pelo agente se tornará cada vez mais escassa.

---

[221] O Brasil em dezembro de 2007 aderiu ao G-8 24 Hours Point of Contact Network, ligado ao G-8 Subgroup em Crime High-tech.

Os crimes praticados por meio da *internet* são caracterizados principalmente pela ausência física do criminoso, por isso mesmo é que são chamados de "crimes virtuais", pois não há a presença dos autores e seus asseclas.[222]

No mesmo trilho, não há mais dúvida de que este *modus operandi* virtual distancia ainda mais o delinquente de sua prisão ou condenação.

Apesar de termos que admitir que os crimes informáticos impróprios, que nada mais são que crimes comuns praticados por meio de um computador, em sua grande maioria, não carecem de legislação, são merecedores de ajustes; dentre eles destaca-se sua majoração justificada, pelo *modus operandi*¸ dificuldade de apuração delitiva e intelectualidade do agente.

Por estes breves apontamentos denota-se que a aplicação da lei penal no espaço cibernético precisa ser melhor regulada. Não há se aguardar a autorregulação do espaço virtual sob pena de, mais do que deixar impune uma gama de criminosos, criarem-se zonas de atrito entre nações soberanas e igualmente competentes para puni-los.

Neste sentido Winfried Hassemer sustenta que com o surgimento dos ataques informáticos aumenta a necessidade de controle por parte do Estado bem como a de utilizar tecnologia de informação, que se modernize constantemente.[223]

Como em todas as relações humanas, o direito deve ser invocado para regular e limitar mais esta realidade cotidiana. A vida humana, a cada dia, está mais ligada ao computador e à comunicação eletrônica.

Porque se reveste de características que esbarram nas diversas áreas da ciência jurídica, legislações foram criadas, adaptadas e, no Brasil, outra tramita no Congresso Legislativo,[224] com vistas à regulamentação do que se denominou "direito da informática".

Tipificaram-se condutas.[225] Estabeleceram-se proteções civis aos direitos autorais, às bases de dados, aos contratos eletrônicos, aos nomes de domínios[226], tributaram-se os

---

[222]TERCEIRO, Cecílio da Fonseca Vieira Ramalho. op. cit.

[223]HASSEMER, Winfried. Oportunidades para la privacidad frente a las nuevas necesidades de control y las tecnologías de la informacion. Traducción de Alfredo CHIRINO Sanchez, L. L. M. *Nueva Doctrina Penal*, Buenos Aires, p. 107, 1999.

[224]Projeto de Lei Substitutivo aos 76/2000 e 137/2000 da Câmara e ao PL 89/2003 do Senado.

[225]A Lei 9.983/2000 criou novas tipificações penais, inserindo-as no Código Penal sob os artigos 168 – A, 313 – A, 313 – B e 337 – A, além de alterar a redação dos artigos 153, 296, 297, 325 e 327. (BRASIL. *Código Penal,* cit.).

[226]BRASIL. Lei 9.610, de 19 de fevereiro de 1998. Altera, atualiza e consolida legislação sobre direitos autorais é dá outras providências. *Diário Oficial da União*, Brasília, DF, 19 fev. 1998.

serviços prestados pelos provedores de conteúdo e de acesso à *internet*[227]. Há, em resumo, atenção às relações jurídicas nascidas a partir da *internet*.

No entanto, igual atenção não recebeu o ciberespaço. Criminalizaram-se condutas, mas não se definiu o local de suas práticas. É preciso se ter em bons termos qual a extensão do braço punitivo do Estado para que, ao lado da segurança jurídica encontradiça no princípio da reserva legal, seja identificada a zona de alcance de suas leis.

Para Benedito Hespanha, a virtualização do ciberespaço foi desterritorializada. Sem território e espaço determinado, os programas, as informações e os hipertextos contêm dados virtuais no mundo da cibercultura.[228]

Para Peter Grabosky, o alcance global dos crimes informáticos é um dos seus aspectos mais significantes. A habilidade do criminoso em cometer crimes em um país com efeitos em vários outros é possível através da natureza global do ciberespaço. Conclui alertando que esta situação traz grandes desafios à detenção, investigação e condenação dos infratores.[229]

É cediço que repudiável a ideia de estender os domínios da lei estatal para além de suas fronteiras, por meio do princípio da competência universal, da extraterritorialidade, da nacionalidade ou da representação, ao argumento de que ofensiva ao conceito de soberania.

Não obstante esta verdade, a reflexão acerca da competência era questão de tempo e, hoje, quanto aos crimes informáticos, é medida necessária. Ao menos é uma vertente que não pode ser ignorada sob pena de sufocar a segurança jurídica que deve andar ao lado do direito penal, principalmente.

Sendo certo que o direito penal protege bens jurídicos de suma importância, bem como que tais bens são agredidos por condutas perpetradas por meio da rede mundial de computadores, inevitável, sempre que a lei existente não for o bastante para protegê-los, legislar-se a respeito.

---

[227]BRASIL. Lei Complementar 87, de 13 de setembro de 1996. Dispõe sobre o imposto dos Estados e do Distrito Federal sobre operações relativas à circulação de mercadorias e sobre prestações de serviços de transporte interestadual e intermunicipal e de comunicação, e dá outras providências. *Diário Oficial da União*, Brasília, DF. 13 set. 1996.

[228]HESPANHA, Benedito. O poder normativo da internet e a regulamentação dos crimes virtuais. *Justiça do Direito*, Rio Grande do Sul, v. 1, n. 16, p. 35, 2002.

[229]GRABOSKY, Peter. Computer crime: a criminological overview. New York. *Forum on Crime and Society*, v. 1, n. 1, p. 49, 2001.

Da mesma forma, não sendo possível resolver a competência jurisdicional dos países por meio dos princípios da teoria geral do crime hoje adotada, inarredável é a necessidade de regular o ciberespaço com vistas a afastar a incerteza da lei aplicável.

É praticamente impossível construir um sistema exauriente para a questão da determinação do lugar do crime, pois a *internet* não conhece barreiras físicas. Não há controle prévio, tampouco centralizado dos dados que circulam pela *internet*. É quase impossível monitorar o trânsito de tais dados.

As investigações policiais, por outro lado, quase sempre se mostram tardias, eis que o dinamismo que qualifica a informática não lhe é peculiar. Acordos internacionais podem ser aptos a controlar, ainda que de forma singela, o espaço virtual. É necessária uma sistemática harmônica internacional, sem o que não há se falar em investigação produtiva.[230]

Não obstante as condutas praticadas pela *internet* não tenham um território físico delimitado ou uma nacionalidade definida fora do ciberespaço, é certo que seu agente tem uma personalidade real, que vai além daquela utilizada no mundo virtual e produz efeitos no mundo real.

Para alguns autores, o espaço virtual é um novo mundo. No entanto, não há se esquecer que não existem dois mundos distintos, um virtual e um real. Apenas um mundo existe e nele devem se fazer aplicados e respeitados os valores de liberdade e dignidade da pessoa.[231]

Punir o agente que pratica crime virtual é um direito e um dever do Estado, porquanto desrespeitada encontra-se sua lei. No entanto, pelo simples fato de possuir o agente uma personalidade, é também um seu direito saber qual o Estado e a lei competente para punir-lhe, pois, do contrário, desrespeitada estará também sua Constituição.

"O cidadão do mundo virtual é, antes de tudo, um cidadão do mundo real e da mesma forma deve ser encarado o agente criminoso".[232] Sujeito de obrigações, mas também de direito, vale dizer.

---

[230]ALBUQUERQUE, Roberto de Araújo de Chacon de. op. cit., p. 14.
[231]TERCEIRO, Cecílio da Fonseca Vieira Ramalho. op. cit.
[232]DAOUN, Alexandre Jean; BLUM, Renato M. S. Opice. op. cit., p. 118.

A persecução estatal, embora legítima, não pode ser efetivada sem cautela. Assim como os direitos ofendidos pelo criminoso que atua no mundo virtual, outros direitos são igualmente defendidos pela norma, como a liberdade de expressão, a intimidade e a dignidade da pessoa humana.

Tem o cidadão, brasileiro ou não, o direito de saber qual a conduta proibida e qual a competência estatal para julgá-lo.

Feita esta ponderação, ressalvada a proteção dos direitos das pessoas que atuam na esfera virtual, qualquer afronta a direito penalmente tutelado é punível nos termos da legislação em vigor e, futuramente, nos termos em que forem legisladas as condutas virtuais penalmente relevantes.

D`Agostini explana que

> Diuturnamente são praticados crimes por Aspetto non di poco conto è quello relativo alla determinazione della legge penale applicabile, nonché i criteri di ripartizione della giurisdizione fra Stati nel caso di reati commessi per via telematica. Il mondo di Internet non consente una delimitazione territoriale all' accessibilità dei dati immessi, o alla loro raggiungibilità e disponibilità, permettendo la diffusione e la circolazione mondiale del materiale inserito, compreso quello illecito o lesivo. La creazione di questo *cyber-spazio* che si espande oltre i confini del território degli Stati nazionali, pone il delicato problema di individuare quale possa essere il giudice competente 'territorialmente' e in ragione di ciò quale debba essere la legge, tra le molte potenzialmente applicabili, regolatrice del fatto realizzato via Internet. Attualmente vengono prospettati, a livello Internazionale, due diversi approcci: considerare come luogo per la determinazione del giudice competente e all contempo della legge applicabile quello dell'immissione in Rete dei dati (luogo dell'azione), oppure, al contrario, dare risalto al luogo della ricezione degli stessi da parte dei destinatari (luogo dell'evento).[233]

Sob uma contemporânea ótica cibernética, o infrator que pratica um delito informático a distância continua dirigindo-se ao *locus delicti* só que não mais fisicamente, agora eletronicamente, através de uma rede de comunicação.

Devemos aceitar que para os delitos informáticos não existem fronteiras. São praticados no espaço cibernético e, como se sabe, este é "terra" de ninguém, pelo menos no sentido literal que o termo "terra" pode denotar.

---

[233]D`AGOSTINI, David et al. (Coord.). *Diritto penale dell'informatica dai computer crimes alla digital forensic*. Folì, Itália: Experta, 2007. p. 175-176.

Não existe legislação específica sobre o tema. Os princípios que norteiam a aplicação da lei penal no espaço seriam o bastante para dirimir eventual conflito de competência entre dois países acerca da lei aplicável?

Discute-se a possibilidade de regular o espaço utilizado pelos internautas. No entanto, não se pode olvidar que a lei penal do país que primeiro legislar sobre o ciberespaço pode conflitar com a lei de outro que o fizer posteriormente.

A competência para legislar é soberana em todos os países livres. Como submeter um cidadão de um país às leis de outro, quando os dois se dizem competentes para julgá-lo por crime informático?

Grande parte dos países adotou a teoria da ubiquidade quanto ao lugar do crime, colocando em frequente conflito mencionada competência.

A questão se torna ainda mais difícil se lembrarmos que os crimes informáticos apresentam interesses econômicos e visões culturais diversas.[234]

Frequentemente, teremos condutas autorizadas em determinado ordenamento jurídico que, quando praticadas em Nação diversa, nesta tornam-se ilícitas. Da mesma forma, em determinada nação teremos penas e questões processuais diversas das existentes em outros países.

Em comunicação da Comissão Europeia para o Conselho e Parlamento da Comunidade (COM 2000), alertam Aboso e Zapata[235] que "los crímenes informáticos son cometidos a través del ciberespacio y no se detienen ante las convencionales fronteras estatales".

No entanto, na era digital, vários países podem ser tidos como competentes para punir uma mesma conduta. Uma mesma ação criminosa pode ser entendida como ofensiva a mais de um ordenamento jurídico.

Pode também uma conduta ser iniciada em um país, consumada noutro e resultar em ofensa à lei de um terceiro. Um agente, do Brasil, utilizando um provedor japonês, pode enviar um *e-mail* para periódicos eletrônicos americanos ofendendo a honra objetiva de um italiano residente na Inglaterra.

---

[234]ABOSO, Gustavo Eduardo; FLORENCIA ZAPATA, María. op. cit., p. 8.
[235]Id. Ibid., p. 7.

A respeito, o Professor Scarance discorre que "os crimes por computador são crimes em que o agente está em um local e o resultado é produzido em outro, no mesmo país ou em país diverso".[236]

A punição do agente dependerá, nestes exemplos, da definição que o Estado dá ao conceito de lugar do crime. Entendido como lugar do crime o local onde o resultado se consumou, no último exemplo seria competente para aplicar a lei penal o quarto Estado (Inglaterra).

Por outro lado, entendido como o local que pisava o agente quando iniciou a conduta, há duas posições – para a primeira seria o primeiro Estado (Brasil) e, para a segunda, o Estado onde se encontra o provedor (Japão) é que seria competente para punir-lo.

No entanto, se eleito como local do crime o espaço em que a conduta se consumou, a competência para a reprimenda seria do terceiro Estado (Estados Unidos da América).

A definição da competência se torna um pouco mais complexa se ao exemplo acrescentarmos o fato de que pode cada um dos Estados adotar teorias diferentes.

Pode ainda, por exemplo, ser adotada a teoria do resultado por todos os Estados envolvidos, mas o crime ter sido praticado pela *internet* e, por isso mesmo, conseguir produzir o mesmo resultado em diversos países a um só tempo.

O Brasil, quanto ao local do crime, adotou a teoria mista, considerando praticado o crime tanto no local da conduta quanto no do resultado.[237]

Praticada a conduta ou um só fragmento dela no Brasil, ainda que o restante da conduta e o resultado se produzam em outro país, em regra, a lei e a jurisdição brasileira são aplicáveis.[238]

Da mesma forma, praticada a conduta noutro país, mas tendo o resultado ocorrido em nosso território, ou simplesmente nele deveria ocorrer, é o Brasil, salvo convenções, tratados ou regras de direito internacional, competente para punir o agente criminoso. Nesta situação haverá necessidade de o delito estar incluído dentre aqueles que a lei brasileira autoriza a extradição.

---

[236]FERNANDES, Antonio Scarance. op. cit., p. 18.
[237]COSTA, Fernando José da. *Direito penal*: parte geral: 1º a 120. 2. ed. São Paulo: Atlas, 2007. p. 14.
[238]COSTA JR., Paulo José da; COSTA, Fernando José da. op. cit., p. 85-86.

Superando esta primeira etapa, para aplicabilidade da lei nacional necessita-se da entrada do agente em território nacional. Esta resta infrutífera caso o delito seja daqueles que não se admite extradição ou se o país em que o agente se encontra negar o pedido de extradição.

Adotada a teoria do resultado por um país, este se dirá competente para punir o agente que praticou uma conduta em um outro país. Este último, por sua vez, se adepto for da teoria da conduta, dir-se-á competente para punir o agente que praticou a conduta em seu território.

Esta discussão, embora solucionável pelo direito interno de cada país, é candente quando travada entre dois ou mais países. Ainda se o resultado se sucedeu em mais de um Estado, teremos vários países aptos a aplicar sua soberania quanto àquela conduta. O problema não é descobrir qual o Estado competente, mas sim afirmar exclusividade de um ou de outro quando ambos entendem-se detentores do *jus puniendi.*

Não sem certo grau de tensão, a competência entre dois países ofendidos por uma mesma conduta, não obstante cada Estado tenha sua fórmula para solucionar conflitos de competência, acaba se definindo por acordos e vias diplomáticas.

Não há nada de concreto nesta fórmula, portanto. A competência, embora atribuída a mais de um país, será exercida por um ou por outro país conforme o caso concreto e as relações diplomáticas existentes entre ambos quando da ocorrência do fato.

Mas e quando o local do crime é o espaço cibernético? "Existe ainda o problema da territorialidade, para saber de onde vem o crime. Qual o provedor? De onde vêm as fotos ou filmes divulgados? Quem as produziu? Qual a real data do fato ali mostrado?"[239] E quando o resultado é simultaneamente produzido em vários Estados Nação?

Quanto à aplicação no espaço cibernético da lei penal, aduzem Aboso e Zapata

> Haciento un resumen de lo dicho hasta aqui, se puede observar que la aplicación espacial de la ley penal encuentra una fuerte escollo al momento de aplicar la ley nacional por el hecho de que la mayoria de las compañias prestadoras y distribuidoras de Internet están amparadas bajo la jurisdición americana, donde el resguardo de la libertad de expresión encuentra una justificación más amplia. Este valladar no es una justificación menor – propria de la que se hizo mención más arriba ya que, si bien se puede estar de acuerdo en principio con la solución

[239]NOGUEIRA, Sandro D'Amato. *Pedofilia e o tráfico de menores pela internet*: o lado negro da web. Disponível em: <http://www.criminal.com.br>. Acesso em: 29 set. 2010.

> aplicada en ambos casos jurisprudenciales referidos, lo cierto es que la posibilidad real de enjuiciar a los directivos o responsables de las sociedades involucradas parece ser una suerte de desideratum.[240]

Novidade se apresenta ao direito quando se fala em crimes praticados pelo computador. O ciberespaço não permite, muitas vezes, a segura afirmação de que a conduta foi praticada neste ou naquele país.

Um *e-mail* enviado por um internauta a outro que reside do outro lado da rua, ou mesmo a quem com ele divide o escritório, em fração de segundos, antes de ser por este recebido, poderá ter passado por vários outros lugares em diversos países localizados a milhares de quilômetros de distância, conforme orientação do roteador.

Por força da falta de uma estrutura centralizada da *internet*, não há como o internauta prever o caminho que sua mensagem percorrerá. Como se disse, um *e-mail* enviado do Brasil aos Estados Unidos pode passar pelo Reino Unido, se congestionado estiver o fluxo de dados daqueles países.[241]

Um *e-mail* com assertivas difamatórias ou material pornográfico envolvendo crianças e adolescentes espalhados a milhares de computadores pelo redor do mundo terá ferido o ordenamento de tantos países quantos tenha percorrido?

Além da discussão a respeito da localidade do delito e da aplicabilidade jurisdicional, países ainda diversificam punições relacionadas ao mesmo crime. A pena aplicada a um determinado delito pelo ordenamento de um país pode ir além ou ficar aquém do preceito secundário estampado na lei de outro.

É possível ainda que a pena prevista como retribuição a um crime em um país seja de espécie diferente em outro. Pode-se pretender punir o crime com pena privativa de liberdade no país A e com pena capital no país B.

Tem-se ainda questões diversas como a transação penal, extinção de punibilidade, suspensão condicional de um processo ou de uma pena, que podem ser aplicáveis em alguns países e inaplicáveis em outros.

---

[240]ABOSO, Gustavo Eduardo; FLORENCIA ZAPATA, María. op. cit., p. 33.
[241]ALBUQUERQUE, Roberto de Araújo de Chacon de. op. cit., p. 65.

Qual seria a competência jurisdicional? Entregaria o país mais liberal o agente, seja ou não ele um seu cidadão, ao outro que se sentiu ofendido? Ser-lhe-ia exigível a entrega do agente à nação menos liberal para que nesta seja punido sem ofender-lhe o direito?

Imaginemos um resultado criminoso ocorrido no Brasil, como a eutanásia, aqui tipificada como homicídio privilegiado, com conduta praticada em outro país que não a incrimina, sendo que este nega a extradição deste infrator ao Brasil.

Antes da era informática, discutir esta hipótese era inviável. Com o computador e a *internet* uma pessoa de qualquer local do mundo pode invadir o computador de um hospital e praticar esta conduta, sem maiores dificuldades, desde que quebradas as barreiras de segurança informática daquele hospital.

Cite-se como exemplo também a bigamia. O Brasil a incrimina, e países como a África do Sul, Sudão, Tanzânia e Nepal, contudo, a tem por inofensiva.

Se um brasileiro casado em país que permite a bigamia, do Brasil, pela *internet*, se casa novamente com outra mulher no mesmo país do primeiro matrimônio, deve o mesmo, prevalecendo a teoria mista da territorialidade, encontrando-se no Brasil, responder pela ofensa ao direito brasileiro, se no país onde o resultado se produziu não houve ofensa alguma?

Vejamos ainda o caso da violação à intimidade informática. O Brasil não incrimina esta conduta, todavia, países como Alemanha, Áustria, Canadá, Dinamarca, Estados Unidos, Finlândia, França, Irlanda, Israel, Japão, Luxemburgo, Países Baixos, Nova Zelândia, Noruega, Reino Unido e Suécia adotam leis específicas que protegem o armazenamento, coleta e transmissão de dados pessoais.

O agente que, do Brasil, pelo computador ligado à *internet*, pratica na Noruega invasão à intimidade divulgando dados pessoais sigilosos de um norueguês, na Noruega, responderá por algum crime? O Brasil autorizará sua extradição se nele for naturalizado ou residente?

Antigamente, nas inaugurais aulas de direito penal os Professores invocavam, quando tratavam do tema "local do crime", o agente que disparava a arma de fogo com vista a atingir alguém que se encontrava doutro lado da fronteira e que, depois de atingido, corria para terceiro país no qual vinha a falecer.

De quem seria a competência para punir o assassino?

Em tempos modernos, certamente já se inauguram tais aulas com os exemplos de crimes informáticos. Muito provavelmente se discuta em salas de aulas o crime de *bullying* praticado pela *internet* ou contravenção penal de jogar pôquer na internet, realidade no dia-a-dia.

Como seria resolvida a questão de conduta praticada do Brasil, através de um provedor estrangeiro que legitima tal prática, jogando pôquer e utilizando-se de cartão de crédito expedido por país que, da mesma forma, não veta tal conduta? Hoje, pela teoria mista adotada pelo nosso Código, responderia pela lei brasileira por ter, no território nacional praticado a conduta.

Embora latente a discussão sobre a necessidade ou não de novas tipificações com vistas a punir condutas praticadas por meio da *internet*, nada se discute no âmbito do Direito Penal acerca da jurisdição aplicável nos crimes informáticos que transcendem o território nacional.

Para muitos a *internet* é um paradigma da liberdade, um mundo digital onde os controles convencionais não servem para nada e onde não existe hierarquia. Conclui afirmando que querer regular a *internet* é como querer regular o tempo.[242]

Sobre o tema jurisdição na *internet*, Dias Pereira[243] afirma ser um dos mais complexos e delicados do direito cibernético. Divide esta problemática em três pontos: a) qual seria o Tribunal competente para julgar o crime? b) qual seria a lei aplicável ao litígio e c) como reconhecer em um Estado as decisões proferidas por Tribunais de outro Estado?

2. Direito interno ou internacional

Como já se disse, o agente pode praticar a conduta em um país, mas o resultado de sua conduta ocorrer em outro. É neste diapasão que no mundo atual se tem a punição do crime como um interesse comum de todas as nações.

Antes de adentrarmos na discussão a respeito da conduta e do resultado criminoso nos crimes informáticos, para a partir daí invadir a aplicabilidade da soberania estatal,

[242]LÓPEZ ZAMORA, Paula. op. cit., p. 96.
[243]PEREIRA, Alexandre Dias. A jurisdição na internet segundo o regulamento 44/2001 (e as alternativas extrajudiciais e tecnológicas). *Boletim da Faculdade de Direito, Universidade de Coimbra*, Coimbra, 2001.

abordaremos, sucintamente, o tema ligado à aplicabilidade do direito interno ou internacional nos crimes informáticos.

Uma lei internacional, dotada de coercitividade, afastaria de vez discussão sobre a competência para punir o agente e asseguraria o direito a todos de não ser processado, condenado e, principalmente, punido duas vezes pela prática de um mesmo crime.

Todavia, porque diversas são as culturas ao redor do mundo e o conceito de soberania é um só em todo ele, a coerção só é possível por um país dentro do seu território. Deve a lei ter força bastante para alcançar a conduta criminosa que de uma forma ou outra tenha atingido os valores sociais do seu país, sem, contudo, atingir a soberania de outro país.

Se em determinados crimes a lei nacional não se revestir de força bastante para romper as barreiras geográficas, dará azo à impunidade e perpetuação da conduta que se visa extirpar.

Num primeiro plano, a lei penal apenas tem validade nos limites do território do Estado soberano que a editou.

A definição do espaço territorial em que se dota de eficácia a lei penal é necessária para preservação da ordem internacional, a qual restaria abalada se um Estado soberano interviesse nas relações sociais, criminosas ou não, existentes em outros Estados também soberanos.[244]

A conduta delituosa, quando resvala na esfera dos direitos protegidos pela norma penal, desafia punição estatal como resposta à prática criminosa. No entanto, quando a prática da conduta é contra bens jurídicos que não são objetos de tutela penal, o direito punitivo do Estado sobre ela não pode incidir, porque atípica.

Ocorre que, conforme pontuado por Chacon, o direito penal não está aparelhado adequadamente para fazer frente à criminalidade informática. Isto cria uma incerteza na sociedade sobre o que é e o que não é permitido. Ele pode delimitar com clareza o que se pode e o que não se pode fazer com a tecnologia da informação, contribuindo para criar

[244]ROCHA, Fernando A. N. Galvão da. op. cit., p. 98.

entre os usuários da informática uma consciência sobre as regras jurídicas que devem ser respeitadas.[245]

Não há dúvida quanto à necessidade de tipificar as novas condutas reprováveis praticadas pelo computador.

Contudo, condutas praticadas com o auxílio do computador e que já são tidas por criminosas, pelos motivos antes apresentados, em sua maioria, merecem apenas pequenos ajustes, como um aumento em sua sanção.

Conforme explana Vicente Greco Filho, não há necessidade de tipificar os crimes praticados através da internet. Esta é apenas um meio, como outro qualquer, pelo qual o infrator pratica a conduta típica.[246]

Como dito alhures, o furto, praticado por computador, será da mesma forma um crime de subtração de coisa alheia móvel.

O que se reclama, a par das tipificações que se fazem necessárias, é ter em bons termos os princípios que norteiam a teoria do lugar do crime, erigindo-os à condição de solucionadores dos conflitos de competência para julgar os crimes informáticos ou especificar de maneira adequada, e de modo a afastar a insegurança do tribunal de exceção, qual seria o regulamento a ser seguido para se alcançar o conhecimento de qual o juízo e a lei aplicável a cada caso.

Porquanto vigore o princípio da reserva legal em todos os estados democráticos de direito, os diversos ordenamentos jurídicos definem a possibilidade de aplicar a lei nacional, independentemente do território em que pisava o delinquente quando da prática do fato típico.

A Lei de Introdução ao Código Civil, fonte básica dos princípios que norteiam as comunicações das leis internacionais com as leis brasileiras, estabelece que a lei nacional tem vigência em todo o país.

A aplicação da lei penal nacional, dentro e fora do país, contudo, é questão mais intimamente ligada ao conceito de soberania.

---

[245] ALBUQUERQUE, Roberto de Araújo de Chacon de. op. cit., p. 40.
[246] Neste sentido, GRECO FILHO, Vicente. op. cit.

Além de cuidar da aplicação da lei penal no seu espaço geográfico e ficto, o Estado tem o dever de fazê-la alcançar também os delitos que se prontificou a reprimir por tratado, convenção ou regras de direito internacional, tais como o genocídio, a tortura e os atentados contra o meio ambiente, mesmo quando além dos limites geográficos nacionais.[247]

O estudo do âmbito espacial da lei penal sobeja importância, vez que o fenômeno da internacionalização do delito, mormente no âmbito virtual, não permite a restritiva aplicação da lei penal ao território do país que a editou.

Malgrado se trate de um direito penal internacional com o compromisso de cada Estado punir determinados crimes, independentemente do local onde foram praticados, a punição terá assento no direito interno de cada país.

Bettiol, amparado por Quadri, afirmou que tais normas seriam de direito penal internacional, porquanto tidas como normas de direito internacional e se referiam ao estudo do modo pelo qual os ordenamentos jurídicos internos de cada país proveem com referência à matéria penal, à resolução dos problemas que são impostos ao Estado, do qual emana este ordenamento, por força da sua coexistência com outros Estados, no âmbito da comunidade internacional superior.[248]

Na mesma esteira, Luiz Regis Prado entende que, nos casos em que um delito ofender interesses de mais de um Estado, se todos eles conferirem a si o direito de puni-lo, surgirá o Direito Penal Internacional, como um ramo do Direito Penal apto a regular os problemas penais que se apresentarem no âmbito internacional, com vistas à prevenção e resolução dos conflitos que venham a surgir entre as nações.[249]

São, em verdade e de acordo com Mirabete, "normas de direito penal interno, já que não estabelecem preceitos ou sanções destinadas a outros Estados" [250], sem embargos de, comumente, ser a aplicação da lei no espaço discutida em sede de convenções, tratados ou regras de direitos internacionais.

Comunga da mesma ideia Anibal Bruno de Oliveira Firmo, para quem o direito penal, quando transpõe os limites nacionais, é ainda direito público interno de um país,

---

[247]DOTTI, René Ariel. op. cit., p. 276.
[248]BETTIOL, Giuseppe. op. cit., v. 1, p. 187.
[249]PRADO, Luiz Regis. op. cit., v. 1, p. 200.
[250]MIRABETE, Julio Fabbrini. op. cit., p. 72.

mesmo nas relações com o direito estrangeiro. Argumenta que não seria apropriada a terminologia "internacional" para designar as regras criadas por órgãos internacionais ou as medidas que resultam de tratados e acordos entre nações, com vistas à prevenção ou repressão de fatos que interessam aos signatários, tais como as referentes ao tráfico de mulheres e à segurança das vias de comunicação, "que, embora tenham por origem atos de Direito internacional, se tornam Direito Penal interno, consagradas em leis próprias de cada país".[251]

De mais a mais, "a existência de um direito internacional pressupõe um organismo internacional, que se superponha às nações, que tenha condições de ditar leis e impor sanções".[252]

Não são dotadas de coercitividade as normas internacionais. Apenas o seriam se, a exemplo do pacto social de uma nação, por meio do qual o povo entrega sua soberania ao Estado, as nações se rendessem a um só governo que o representasse, abrindo mão de sua soberania frente aos demais países para com eles formar um só povo.

Poder-se-ia falar em um direito internacional se as normas fossem dotadas de força bastante para fazer valer seus preceitos e sanções em relação às diversas nações.[253]

Por este motivo, melhor razão assiste a Magalhães Noronha ao ponderar que embora muitos denominem direito penal internacional, bem de ver tratar-se de direito interno, embora relacionado com o direito alienígena.[254]

Neste contexto é que se insere a problemática dos crimes praticados pela *internet*. A conduta criminosa praticada no espaço cibernético, em regra, relaciona o direito de mais um país soberano.

3. Da lei aplicável aos crimes informáticos

A *internet* é realidade no cotidiano social, assim como também o é a prática de uma conduta delitiva. No entanto, porque aliados, nova gama de delitos foi criada.

---

[251]BRUNO, Aníbal. op. cit., p. 230.
[252]COSTA JR., Paulo José da; COSTA, Fernando José da. op. cit., p. 83.
[253]FRAGOSO, Heleno Cláudio. op. cit., p. 131.
[254]NORONHA, E. Magalhães. op. cit., p. 84.

Igualmente, criminosos viram na *internet* um novo modo de execução para ampla gama de crimes já existentes, como o furto, o estelionato e a lavagem de dinheiro. Outros foram criados, como a implantação de vírus em computador de terceiros com fins diversos, como o de ser copiado de qualquer navegação realizada naquela máquina. Com estes vírus o agente passa a obter informações confidenciais, documentos profissionais, senhas eletrônicas, movimentações bancárias, dentre outras.

Todavia, não há até o momento qualquer regra que permita posicionar o exegeta acerca da lei aplicável ao crime informático. Antes da *internet*, tanto conduta quanto resultado eram, na maioria das vezes, praticados dentro de um mesmo território, motivo que levou grande parte das nações a adotar a teoria mista ou da ubiquidade quanto ao local do delito. De acordo com esta teoria, considera-se como lugar do delito tanto aquele em que a conduta ou parte dela foi realizada, quanto aquele em que o resultado foi ou deveria ter sido consumado.

Tanto pela maior dificuldade na apuração dos fatos e da autoria, quanto pela ainda duvidosa aplicabilidade da lei penal através deste *modus operandi*, é mais comum que os delitos praticados por meio da *internet* tenham o resultado em território diverso daquele em que pisava o agente quando da prática da conduta. Vale dizer, uma vez mais, nos crimes informáticos, muito raramente conduta e resultado acontecem no mesmo território.

Um norte que permita um posicionamento se faz necessário, eis que as regras de territorialidade contidas tanto na Parte Geral de nosso Código Penal, quanto nas legislações alienígenas, sem dúvida alguma, foram concebidas quando sequer era imaginável a prática delituosa por meio de um aparelho ligado em rede a milhares de quilômetros de distância.

É preciso saber qual o Estado competente para punir o criminoso virtual e qual o direito que deverá regular-lhe a conduta, revelar-lhe sua pena. Devido ao fato de a *internet* não ser regulada por uma entidade, governo ou empresa, pode ser acessada de qualquer ponto do planeta e por qualquer pessoa, seja qual for sua nacionalidade.

Sobre o tema, Paula López Zamora explana que um dos aspectos que reclama regulação da rede é o da necessidade de determinar claramente qual a legislação aplicável e a jurisdição competente para conhecer os diferentes assuntos nela sucedidos. O

deslocamento das condutas na rede exige uma regulação concisa que determine o órgão aplicador da norma e a própria norma que deverá ser aplicada.[255]

Os princípios dirimentes dos conflitos de competência entre dois ou mais Estados previstos nos ordenamentos penais de diversos países, ainda que bastantes para regular os novos embates acerca da lei penal aplicável, quando consagrados não previam a existência do dito espaço virtual, onde por um meio de comunicação e de um computador, as pessoas eletronicamente se transportam para qualquer lugar do planeta. Assim, estes princípios dirimentes devem ser repensados.

Não há nação legitimada a regulamentar o uso da *internet* em âmbito mundial, pois o espaço cibernético não pertence a qualquer Estado.

No entanto, determinados países permitem algumas condutas praticadas pela *internet*, outros não. O espaço é não regulável, mas a ofensa que pode ser levada a efeito por uma conduta nele praticada pode e deve ser punida por lei.

Para tornar o tema ainda mais complexo, temos nos delitos informáticos a figura do provedor. Uma espécie de responsável pelo transporte de dados comandados pelo agente (conduta) a um lugar (o do resultado). Qual a real participação deste provedor na prática delituosa?

Pode a lei indiferente à conduta (ou que lhe autoriza) entrar em choque com as leis de outro país soberano que as tem por criminosa? Qual o argumento que se invocará para absolver ou condenar uma pessoa com base nesta ou naquela lei? Entre dois países soberanos as leis estão em pé de igualdade. Não há de se escolher com fulcro na álea ou no grito qual a lei aplicável.

Por esta razão, embora não se possa pretender uniformização legislativa em todo o mundo acerca do que é ou não é crime, a convergência de leis no que tange à aplicável é medida indispensável. Esta é, inclusive, uma das metas da Convenção de Budapeste.

As regras de aplicabilidade da lei penal são já conhecidas pelo ordenamento jurídico brasileiro. As regras consagradas aos crimes em geral se aplicam aos crimes informáticos, pois estes, de uma ou de outra forma, constituem espécie criminosa.

---

[255]LÓPEZ ZAMORA, Paula. op. cit., p. 100.

Todavia, pelo simples fato de os crimes informáticos, através de um provedor, permitirem ao agente ofender o ordenamento jurídico de múltiplas nações, simultaneamente, o princípio da territorialidade, por si só, não estanca a interpretação possível sobre a lei aplicável, tampouco diz com qualquer grau de certeza qual o Estado competente para punir-lhe. Tal uniformidade seria alcançada se um só país se encontrasse na condição de lugar do *iter criminis*. Sendo impossível ter um só local do crime quando vários territórios sofreram reflexos da conduta, deve o direito apontar qual critério a ser utilizado. Solução adequada seria a universalização das normas no mundo digital. Por inúmeras razões culturais, políticas e econômicas, esta solução é praticamente inalcansável, no entanto.

Para Celso Valin, a teoria da atividade deveria ser a aplicada nos crimes informáticos, dando ênfase para o local onde a conduta foi praticada. Ela evitaria a questão da extradição do agente e tornaria a apuração mais rápida e precisa[256].

Defendendo a mesma posição encontramos José de Castro Meira Júnior[257], que entende como jurisdição não só o lugar para processar e julgar o agente, mas também o lugar para investigar. Desta forma, a lei do país onde o crime foi cometido seria a mais aplicável, respeitando ainda o direito de defesa do agente, a colheita de provas com maior segurança e mais facilidade em capturar o agente.

Aduzem Caravaca e González[258] que há também teoria que defende a aplicabilidade da teoria do resultado. Segundo esta, seria competente para punir o infrator o país em cujas terras tivesse ocorrido o evento danoso. Salientam que o crime não só pode ter início em um país e terminar em outro, como também o resultado pode ocorrer em vários países.

Se hipoteticamente superada esta discussão, mesmo para os defensores desta posição, o problema persistiria se o resultado ocorresse em mais do que um território, o que nos crimes informáticos tornou-se usual.

---

[256]VALIN, Celso. A questão da jurisdição e da territorialidade nos crimes praticados pela internet. In: VOVER, Aires José (Org.). *Direito, sociedade e informática*: limites e perspectivas da vida digital. Florianópolis: Fundação Boiteux, 2000. p. 117.

[257]MEIRA JUNIOR, José de Castro. A tutela penal dos cybercrimes e o projeto de lei contra os crimes de informática. *Revista da Fundação Escola Superior do Ministério Público do Distrito Federal e Territórios*, Brasília, v. 15, p. 132, dez. 2007.

[258]CALVO CARAVACA, Alfonso Luis; CARRASCOSA GONZÁLEZ, Javier. *Conflictos de leyes i conflictos de jurisdición em internet*. Madrid: Ed. Colex, 2001. p. 110.

Enfrentando o tema, Chacon conclui que, mesmo não sendo a solução mais prática, podendo inclusive gerar conflitos de jurisdição entre os países envolvidos, a melhor solução seria admitir a competência dos países envolvidos para julgar um crime informático, em respeito ao princípio da ubiquidade.[259]

Ocorre que, apesar de num primeiro momento parecer solucionada a discussão no país responsável pela apuração e julgamento dos agentes, no instante em que alcançar decisões contraditórias, certamente enfrentará dificuldade quanto à sua aplicabilidade.

Sobre o tema aduz Scarance que os crimes por computadores têm como característica a universalidade, além de serem crimes que facilitam o anonimato.[260]

No Brasil, quanto à territorialidade, aplicar-se-á nossa legislação a todo crime cometido no território nacional. Quanto ao lugar do crime, adotamos a Teoria da Ubiquidade (ou mista, ou da unidade), isto é, considera-se praticado o crime em qualquer lugar em que se realiza um dos momentos de sua marcha, vale dizer, o lugar em que ocorre qualquer das fases do *iter criminis*, assim como o lugar em que se opera ou deveria se operar o resultado.

Por esta teoria, basta que qualquer fase da atividade criminosa ou do resultado ocorra em território nacional para que o Estado encontre amparada legalmente sua pretensão punitiva.

O Código de Processo Penal, ao tratar da competência jurisdicional, seguindo a teoria do resultado, estabeleceu como critério primeiro de determinação o lugar onde se consumar a infração. Todavia, esta regra de competência tem por pressuposto a inexistência de qualquer conflito de territorialidade.

Da mesma forma, malgrado a inovação trazida pela Lei 9.099, de 1995, no que tange à competência jurisdicional, visto que seguindo a teoria da atividade estabelece o foro de acordo com o lugar em que se pratica a ação e não onde esta se consuma[261], não modificou o fato de que a competência interna tem por pressuposto a resolução territorial.

---

[259]ALBUQUERQUE, Roberto de Araújo de Chacon de. op. cit., p. 77-78.

[260]FERNANDES, Antonio Scarance. Crimes praticados pelo computador: dificuldade na apuração dos fatos. *Boletim do Instituto Manoel Pedro Pimentel*, São Paulo, n. 10, p. 26-27, dez. 1999.

[261]GRINOVER, Ada Pellegrini; GOMES FILHO, Antonio Magalhães; FERNANDES, Antonio Scarance; GOMES, Luiz Flávio. *Juizados Especiais Criminais*: comentários à Lei 9.099, de 26.09.1995. São Paulo: Ed. Revista dos Tribunais, 1996. p. 74.

Em outras palavras, o Código Penal, ao adotar a Teoria da Ubiquidade, trouxe para a competência punitiva brasileira os crimes cujo *iter criminis* ou resultado se desenvolveu em solo pátrio. Assim, quando o Código de Processo Penal erige o juízo do local do resultado como competente, o faz apenas para delimitar, dentre os juízes brasileiros, qual o competente para julgar a ação, pois, como ensina o professor Antonio Scarance Fernandes, a Constituição Federal brasileira vedou expressamente os tribunais de exceção e assegurou o processamento e julgamento da causa por juiz previamente determinado.[262]

Convém salientar que o crime, por ser um instituto divisível apenas para fins doutrinários, é punido como um todo pelo Estado, ainda que apenas parte da execução aconteça em seu território. Igualmente, para efeitos de territorialidade e validade da lei penal no espaço, considera-se, no crime tentado, o lugar do crime, qualquer lugar onde se tenha praticado uma das condutas executivas do delito, bem como o lugar onde deveria ter ocorrido o resultado, caso não fosse interrompido por circunstância alheia à vontade do agente criminal.

O tema foi enfrentado pelo Tribunal francês[263], mais precisamente pela 11ª Sala da Corte de Apelação de Paris, em 10 de novembro de 1999, denominado Monsieur D.J. contra FCO Fiduciaire. Tratava-se de um texto calunioso publicado em um *site* de *internet* passível de consulta em qualquer lugar do mundo, sem destinatário específico.

Para o Tribunal, a possibilidade oferecida pela rede de acessar um texto de qualquer lugar do planeta não seria suficiente para, no país de acesso, ser aplicada sua legislação, mas possível aplicação da lei francesa ao caso, mesmo tendo na Suíça ocorrido o resultado, porquanto estampado no artigo 113-6 do Código Penal francês que "La ley penal francesa es aplicable a todo crimen cometido por um francês fuera del território de La República".

A doutrina vem afirmando que merece atenção especial a definição do *locus delicti* nos crimes informáticos, dada a ausência de fronteira na rede, citando como exemplo os cassinos virtuais. Salienta que, neste tipo de crime, o servidor (origem) está instalado em um país no qual a prática do jogo é permitida, no entanto o usuário se conecta de outro

[262]FERNANDES, Antonio Scarance. *Processo penal constitucional*. 6. ed. São Paulo: Ed. Revista dos Tribunais, 2010. p. 124.
[263]ABOSO, Gustavo Eduardo; FLORENCIA ZAPATA, María. op. cit., p. 36-37.

país, no qual a atividade é proibida, donde surge a indagação acerca da existência ou não de ilícito penal.[264]

Neste sentido, a Convenção sobre a Criminalidade informática previu em seu artigo 22, parágrafo 5º, que quando mais de uma parte reivindicar a competência com relação a uma infração definida na Convenção, as partes deverão, quando for apropriado, consultar-se para determinar a jurisdição mais apropriada para processar.[265]

Sobre a teoria da ubiquidade adotada pelo Brasil, quanto ao lugar do crime, manifesta-se Gilberto Martins de Almeida afirmando que é desejável regular compatibilização de leis de diferentes países e o critério acerca da lei aplicável. Pondera, contudo, que o Brasil adota a teoria da ubiquidade e, por tal motivo, se entende competente sempre que alguma parte de um ilícito penal é cometida em seu território.[266]

Na Espanha, onde também se agasalha a teoria da ubiquidade, sem embargo de a teoria da territorialidade ser a regra, Ricardo Mata, em trabalho sobre a criminalidade informática, no mesmo sentido conclui que

> estas dificultades basadas en la vinculación territorial a la persecución de los ilícitos penales hacen ver inmediatamente la necesidad de una armonización legislativa y cooperación internacional en esta materia, sin las que no se puede proporcionar una respuesta eficaz a esta nueva forma de criminalidad.[267]

É de se ver que, mesmo nos crimes informáticos, a teoria da atividade haverá de ser aplicada quanto ao *locus delicti.* Com conduta e resultado em diferentes países, o local da conduta do agente deve prevalecer.

Pela teoria da atividade, mesmo que no país do resultado aquela conduta não seja criminalizada, o país da conduta aplicará sua lei.

Uma vez mais, havendo conduta e resultado em países diversos que não comungam da mesma posição, teremos duas situações: a) país da conduta criminaliza fato que o do

---

[264]DAOUN, Alexandre Jean. Crimes informáticos, cit., p. 204.
[265]Art. 22 Jurisdicion parágrafo 5º: "When more than one Party claims jurisdiction over na alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution" Vide anexo inteiro teor.
[266]DAOUN, Alexandre Jean. Crimes informáticos, cit., p. 204.
[267]MATA Y MARTÍN. Ricardo. *Temas de direito da informática e da internet*. Porto, Portugal: Coimbra Ed., 2004. p. 235.

resultado não criminaliza; b) país da conduta não criminaliza fato que o país do resultado criminaliza.

Se, nestes casos, adotássemos a teoria do resultado, na primeira hipótese não teríamos crime, já que no local onde o resultado ocorreu não há tipificação. Já na segunda hipótese, se aplicada a teoria mista ou do resultado, teríamos crime, só que no país onde o resultado ocorreu, estando o agente no país da conduta.

Para tanto, necessitaríamos de tratados e convenções aptos a resolver esta questão, extraditando o agente. Caso não existam tais acordos, caberia ao país do resultado pedir a extradição do infrator para então aplicar sua jurisdição.

Evidente, contudo, que se o país no qual ocorreu a conduta não considera crime ou, mesmo considerando, não promove a persecução penal, o país onde se deu o resultado e considera crime, fará o pedido de extradição, sem muita chance de êxito.

Cumpre registrar, por outro lado, que é fato que a localização do provedor por vezes é utilizada como espécie de blindagem pelos criminosos. Narra o promotor Roberto Lyra, que um pedófilo brasileiro, investigado no Brasil, migrou para o *site* de Portugal, donde enviou fotos de adultos fazendo sexo com crianças para um *hacker* que colaborava com as investigações. Ao desconfiar de que estava sendo investigado pela polícia, o dito pedófilo debochou de todos que o investigavam argumentando que jamais seria preso, pois estava em um provedor no exterior.[268]

A respeito desta dificuldade, Scarance esclarece que, nos crimes praticados através de provedores estrangeiros ou pessoas localizadas no exterior, a necessária expedição de rogatória contribui para dificultar a investigação e apuração dos delitos informáticos. A cooperação internacional ou convênio poderiam agilizar as mencionadas providências.[269]

Assim, discutia-se se o local do delito à distância poderia ser o do provedor, responsável pela execução deste comando determinado pelo agente.

A discussão ganhou notoriedade na Alemanha quando, em 1995, um servidor de *internet* alemão[270], filial de outro servidor americano, armazenou fotos pornográficas de menores de idade mantendo relações sexuais, de origem desconhecida, e por isso foi em

---

[268]NOGUEIRA, Sandro D'Amato. *Pedofilia e o tráfico de menores pela internet*: o lado negro da web, cit.
[269]FERNANDES, Antonio Scarance. Crimes praticados pelo computador: dificuldade na apuração dos fatos. *Revista de Ciências Criminais*, cit., p. 19.
[270]ABOSO, Gustavo Eduardo; FLORENCIA ZAPATA, María. op. cit., p. 40-41.

primeira instância condenado como coautor pela conduta omissiva de não ter instalado filtros capazes de evitar o citado armazenamento e distribuição.

Em segunda instância, tal decisão foi reformada para absolver o acusado sob o argumento de que havia uma relação de subordinação além da inexistência de dolo típico, exigido pelo parágrafo 184 StGB. Por fim, sustentou-se dispositivo que prevê a falta de responsabilidade do provedor responsável pela transmissão de comunicação, trazida pela Lei de Serviços Telemáticos, inc. 3º do parágrafo 5.

Ainda sobre o servidor alemão, o Tribunal decidiu que o responsável pelo acesso, não tendo influenciado ou participado de sua elaboração, não pode ser responsável pelo conteúdo no material ali armazenado. Tratar-se-ia de responsabilidade penal objetiva, inadmissível no direito penal.

As questões acima discutem a responsabilidade penal ou não do provedor quanto aos crimes informáticos; nosso trabalho analisa apenas e tão somente se o *locus delicti* dos crimes informáticos pode ou não ser o local onde o provedor está sediado.

Após os dados passarem pelo provedor de presença, denominado *Network Access Points* (NAP's) e deste para o de passagem, tudo por conta do roteador, viajam por inúmeros destinos chegando a provedores *backbones*. Sustentar *locus delicti* neste último ou qualquer daqueles por onde o pacote de dados viajou, certamente, dará azo a ideia de que o local do cometimento do delito poderia ser qualquer um destes locais de passagem dos dados.

Quando muito, em se tratando de provedores, poderão ser invocados acerca da sua responsabilização penal ou não pelo conteúdo que neles é veiculado. Malgrado não seja objeto do presente estudo, faz-se mister externar nosso entendimento no sentido de que este funciona como um mero *longa manus* da prática delituosa, sendo que o responsável pela conduta é sempre o agente. Tal teoria vem enraizada no princípio da comunicação e livre manifestação de expressão, que na era digital ganhou mais força.

Contudo, não descartamos a participação delitiva destes provedores, que, quando cientes da ilicitude, auxiliam sua prática delitiva. Todavia, mesmo que partícipes, nada influenciariam a discussão enfrentada quanto ao *locus delicti* nos crimes informáticos, qual seja, conduta ou resultado.

Benedito Hespanha sustenta uma regulamentação normativa própria de comunicação. Para ele não há na sociedade cibernética território nem fronteiras. No entanto, alerta para a carência de soluções jurídicas e de regulação legal específica, já que os novos relacionamentos virtuais produzem efeitos e consequências no mundo normativo da ordem jurídica.[271]

José Caldas cita dois casos paradigmáticos ocorridos nos Estados Unidos. Um dos casos envolvia a operadora de *internet* chamada *Compuserv Inc*, a qual fornecia aos usuários acesso a banco de dados. Ocorre que foram veiculadas em seu banco de dados mensagens difamatórias acerca de organizadores e desenvolvedores de uma determinada revista eletrônica. Ao argumento de que a prestadora de serviços não tem condições de exercer controle sobre o conteúdo do que é veiculado, a ação foi julgada improcedente.

Posteriormente, outro caso julgado foi desfavorável a outra prestadora de serviços do mesmo gênero. Isso porque foi entendido que ela exercia controle sobre o conteúdo veiculado em seus *bulletin boards*. Todavia, o diferencial, neste caso, é que foi constatado que esta segunda empresa vendia o seu serviço ostentando controle de conteúdo por meio de filtragem e censores humanos, de forma que aplicou a responsabilidade pelo controle.[272]

[271]HESPANHA, Benedito. op. cit., p. 45.
[272]GOIS JR, José Caldas. op. cit., p. 130-131.

CONCLUSÃO

Muito se tem discutido acerca das novas condutas praticáveis a partir da *internet*, propiciadas pelo computador ou aparelho ligado em rede. Delas derivam as lícitas e as ilícitas. Nestas o Direito Penal em alguns casos deve ser aplicado.

Sabe-se que um dos assuntos que merece destaque e aprofundamento acerca da criminalidade informática refere-se ao local de sua prática. Sobre o tema, salvo melhor juízo, não existe uma obra na literatura nacional ou alienígena que trate dele, especificamente. Quando muito, o que se lê são trechos ou capítulos a respeito.

Pouco, ou mesmo nada, se aproveitará das leis penais contra os delitos informáticos em todo o mundo se não houver prévia definição de qual delas será aplicada ao caso concreto.

A conduta prevista em lei penal deve ser anterior à sua prática no mundo fenomênico, sob pena de infringir o princípio da reserva legal, da anterioridade da lei penal. Igualmente, porque constitucionalmente assegurado pelo juiz natural, deve o infrator conhecer qual das várias leis ofendidas será a competente para puni-lo e qual dos Estados estará habilitado a aplicá-la.

Fomentar a criação de tipos penais ou a aplicação dos já existentes às novas condutas criminosas perpetradas pelo computador em rede, sem a paralela definição das regras que levarão à validade da lei penal no espaço, equivale a não tipificar condutas, pois, num ou noutro caso, a conduta, se não aplicável, torna-se irreprochável pelo Direito Penal.

Neste diapasão é que se entende necessário enfrentar a questão do *locus delicti* e, por conseguinte, a identificação do ordenamento jurídico aplicável a cada caso.

Com a globalização e a necessidade de o direito acompanhá-la, o planeta foi, através da comunicação digital, interligado. O direito, da mesma forma deve, na medida do possível, promulgar leis equiparadas na colaboração entre Nações, na definição de territorialidade e lugar do crime, nos crimes e sanções etc.

Não há dúvidas que diversos países criarão resistências, tanto pela diversidade cultural quanto pelo princípio da soberania. O trabalho da humanidade exige tentativas de demonstrar a estas nações o objetivo destas adequações.

Primeiramente há que se ter em conta que o interesse universal deve prevalecer ao interesse interno. Da mesma forma, há que se levar em consideração que os crimes informáticos terão ampla vantagem frente ao direito e, consequentemente, frente à proteção do homem e da sociedade, se ausente a colaboração entre Estados. Fato que a comunidade universal donde adviria o ordenamento jurídico que envolveria toda a humanidade, como pregou Immanuel Kant[273], se mostra já existente. O que ainda não se apresentou a ela, comunidade, foi o famigerado ordenamento.

Ressalta-se que a Constituição Federal brasileira, desde a Emenda Constitucional 45/2004, permite ao Estado receber abertamente as normas decorrentes de tratados internacionais quando tais discorrerem sobre direitos fundamentais. Os Professores Ada Pellegrini Grinover, Antonio Scarance Fernandes e Antonio Magalhães, dentre outros, também entendem que o artigo 5º § 2º da Constituição da República é claro em permitir a adoção de outros direitos e garantias não estampados no texto constitucional, desde que o sejam em tratados internacionais dos quais o Brasil seja parte.[274]

Trata-se de tendência que os luminares do direito já se aperceberam há décadas. Norberto Bobbio ensinava que, para que seja possível a paz jurídica, excelente remédio seria a criação do superestado ou estado mundial.[275]

É por este caminho que têm trilhado as nações em pequenos passos. É o que demonstram a criação das Nações Unidas e grupos menores como União Europeia e Mercosul.

Embora não sejam dotados de coercitividade, como costuma ocorrer no direito interno de cada país, os tratados internacionais, quando subscritos por nações que se comprometem se submeterem às suas cláusulas, têm sido grande aliado da paz, haja vista

---

[273]KANT, Immanuel. *Para a paz perpétua*. Rianxo, Espanha: Instituto Galego de Estudos de Segurança Internacional e da Paz, 2006.

[274]GRINOVER, Ada Pellegrini; FERNANDES, Antonio Scarance; GOMES FILHO, Antonio Magalhães. *As nulidades no processo penal*. 7. ed. São Paulo: Malheiros Ed., 2001.

[275]BOBBIO, Norberto. *Teoria do ordenamento jurídico*. Tradução de Maria Celeste C. J. Santos. 10. ed. Brasília: Ed. da UnB, 1999.

comumente serem cumpridos com base no talvez mais internacional dos princípios, o *pacta sunt servanda.*

Novamente valendo-se dos ensinamentos do mestre italiano:

> O universalismo jurídico ressurge hoje não mais como crença num eterno Direito natural, mas como vontade de constituir um Direito positivo único, que recolhe em unidade todos os Direitos positivos existentes, e que seja produto não da natureza, mas da história, e esteja não no início do desenvolvimento social e histórico (como o Direito natural e o estado de natureza), mas no fim. A ideia do Estado mundial único é a ideia-limite do universalismo jurídico contemporâneo.[276]

Além disso, se a globalização é o pomo dos grandes conflitos internacionais, é também um agente de igual importância no cumprimento dos tratados internacionais, pois os Estados se tornaram dependentes uns dos outros, no âmbito econômico, social, tecnológico, cultural e ecológico.

É tendência mundial, portanto, senão por causas nobres como a paz e o reconhecimento dos direitos humanos, ao menos por questões econômico-políticas, a idealização de leis que se superponham a nações soberanas. Assim foi que a Emenda Constitucional 45/2004 incluiu o § 4º ao artigo 5º da Constituição da República e determinou a submissão do país à Corte Penal Internacional.

Na mesma esteira em que se criou um Tribunal Internacional para julgar responsáveis por crimes de maior gravidade, faz-se mister a criação de uma lei em que se defina a competência jurisdicional das nações nos crimes informáticos, pois detentores de igual gravidade – se não no que tange às garantias e direitos humanos, ao menos no que concerne à convivência pacífica entre as nações e seus ordenamentos penais internos.

Como já ensinara o Professor Miguel Reale[277], os fatos antecedem o direito, pois este é a norma criada a partir da valoração que a sociedade dá àqueles. Em outras palavras, o direito estará sempre um passo atrás dos fatos. O passo social já foi dado – a comunidade humana se tornou universal, resta, agora, saber quanto tempo mais precisará o homem para entender a necessidade de discutir um ordenamento que permita sua harmônica convivência.

---

[276]BOBBIO, Norberto. op. cit., p. 164.
[277]REALE, Miguel. op. cit.

Quer nos parecer, assim, que outra forma de solução não há, senão adotar como critério de solução do conflito de jurisdição, a teoria da atividade com consideráveis temperamentos. Explica-se. Havendo conduta e resultado em países diversos, se ao menos dois países entenderem criminosa a conduta e se disserem no direito de punir o agente criminal, deverá o país no qual for praticada a conduta puni-lo.

Se a conduta for praticada nas mesmas circunstâncias acima, mas apenas os países no qual o resultado ocorreu tiver por criminosa a conduta, haverá de ter jurisdição aquele que primeiro alcançar o criminoso. Observe-se que, para tanto, o país no qual se deu o resultado haverá de ter o agente em seu território para que proceda sua punição, porque como já foi dito, dificilmente o país que não criminaliza a conduta haverá de extraditar o então delinquente. Todavia, caso o faça, punirá o agente aquele que tiver o pedido de extradição atendido.

Caso apenas o país onde foi praticada a conduta a entenda por criminosa, isto é, se o resultado ocorrer em países que consideram lícita a conduta perpetrada, terá o país no qual foi a conduta praticada o direito de punir. No entanto, com igual razão não terá muita chance de êxito no pedido de extradição que vier a ser necessário caso o agente lá não se encontre mais.

Pois bem. O critério para estabelecer a jurisdição está sugestionado. Mas por que a preferência ao país da conduta e não ao do resultado?

Por primeiro, acreditamos que este tenha mais condições de realizar as investigações e a persecução penal. Com efeito, o trabalho de investigação será mais facilmente deflagrado e concluído no país onde a conduta foi praticada. Da mesma forma, sendo certo que a extradição encontra óbices às vezes intransponíveis, dificilmente o país no qual o resultado foi percebido conseguirá punir o agente criminal, ainda que o tenha processado e condenado à revelia.

Demais disso, não se pode olvidar que o critério se torna mais facilmente aplicável e alheio a conflitos na medida em que o resultado, embora perceptível em vários países, em um só será praticada a conduta. Ou seja, adotamos também a teoria da atividade como a adequada aos crimes informáticos, por se tratar da menos conflitante quanto à aplicabilidade da lei penal entre países, também nos frequentes casos em que o resultado suceder em mais de uma nação.

Ter-se-á por respeitada a soberania das nações com o critério acima, pois as nações ofendidas, diga-se, onde o resultado foi produzido, poderão aplicar o seu direito se, e somente se, o país no qual foi praticada a conduta não a considerar criminosa ou, assim a considerando, não promover a devida ação penal e for o acusado extraditado ao país onde se deu o resultado ou nele adentrar espontaneamente.

Sustentamos também que não é possível discutir como local do delito o território onde se encontra o provedor de *internet*, ao argumento de que parte do crime ali se desenvolvera.

O provedor, mesmo que considerado coautor do crime não deve influenciar o *locus delicti*. Deve-se levar em conta como local da conduta aquele em que o agente se encontrava e como local do resultado onde o bem foi lesado ou ameaçado de lesão.

O provedor é um mero espaço virtual por onde correm os dados determinados pelo agente, através de pacotes identificados por numeração, conforme já explanado.

De Lege Ferenda

Ao estudar o direito penal informático, um dos temas de maior destaque está relacionado ao local do delito. É sabido que na era digital o envolvimento de mais de uma nação no *iter criminis* deixou de ser exceção para se tornar regra.

Sem uma definição em nível mundial do lugar do crime e do país apto a julgá-lo, passaremos a discutir qual nação será soberana para julgar cada caso, com vistas a afastar as inevitáveis ofensas ao princípio *non bis in idem*.

Após aprofundamento no tema, apresentamos sugestão de alteração da teoria adotada quanto ao *locus delicti* nos crimes informáticos.

Não obstante a ideia encontrada não esgote o assunto, pretende-se dela fazer ponto de partida para a discussão do tema, na esperança de que futuramente outras pessoas estudem a respeito e se pronunciem sobre tão latente problema encontrado no ordenamento jurídico pátrio.

Isso posto, tem-se que o artigo 6º do Código Penal, à época em que concebido, mais precisamente em 1984, orientou-se por uma criminalidade presencial. Assim, considera

praticado o crime no local onde se der a conduta, bem como no local onde o resultado for ou deve ser produzido.

Como se concluiu nesta pesquisa, o crime informático poderá ocorrer, de acordo com o critério do resultado, em mais de um país, simultaneamente, bem como encontrar o território de vários outros como base durante a sua execução, mas nunca será praticado, do ponto de vista da conduta, em países plurais.

Desta forma, sendo certo que adotada a teoria encampada pelo nosso artigo 6º do Código Penal também para dirimir a territorialidade do crime informático, conflitos territoriais apresentar-se-ão no que tange ao lugar do resultado como local do crime, mister se faz, por exceção, restringir, apenas no que tange aos crimes informáticos, o lugar do crime ao local da conduta.

Neste diapasão, a inserção de um Parágrafo Único ao artigo 6º do Código Penal, com redação que considerasse praticado o crime informático no lugar em que ocorreu a ação ou omissão, desde que criminosa também fosse a conduta nesse lugar, poria fim ao problema da delimitação da competência jurisdicional.

Note-se, todavia, que por tal regra o local do crime seria determinado pelo local da conduta (teoria da atividade ou da ação), no entanto, desde que o local da conduta também a considerasse criminosa. Do contrário, ressalvado estaria o direito do Estado, em cujo território se deu o resultado, de punir o agente criminal.

REFERÊNCIAS BIBLIOGRÁFICAS

ABOSO, Gustavo Eduardo; FLORENCIA ZAPATA, María. *Cibercriminalidad y derecho penal*. Buenos Aires: Editorial B de F, 2006.

ALBUQUERQUE, Roberto de Araújo de Chacon de. *A criminalidade informática*. 2003. Tese (Doutorado em Direito Penal) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2003.

AZEVEDO, David Teixeira de. *Atualidades no direito e processo penal*. São Paulo: Método, 2001.

AZNAR, H. Medios de comunicación y esfera pública: el papel de la autorregulación. In: BUENDÍA, Manuel. *Deontologia y autorregulación informativa.* México, D.F., 2000.

BETTIOL, Giuseppe. *Direito penal*. Tradução brasileira e notas do Professor Paulo José da Costa Junior e do magistrado Alberto Silva Franco. São Paulo: Ed. Revista dos Tribunais, 1966. v. 1.

BITENCOURT, Cezar Roberto. *Tratado de direito penal*: parte geral. 8. ed. São Paulo: Saraiva, 2003. v. 1.

BLUM, Renato M. S. Opice et al. (Coord.). *Direito eletrônico*: a internet e os tribunais. Bauru, SP: EDIPRO, 2001.

BOBBIO, Norberto. *Teoria do ordenamento jurídico*. Tradução de Maria Celeste C. J. Santos. 10. ed. Brasília: EdUNB, 1999.

BOTTINI, Pierpaolo Cruz. *Crimes de perigo abstrato e princípio da precaução na sociedade de risco*. 1. ed. São Paulo: Ed. Revista dos Tribunais, 2007. v. 1.

BRASIL. *Código Penal.* 13. ed. São Paulo: Ed. Revista dos Tribunais, 2011.

_____. Constituição (1988). *Constituição da República Federativa do Brasil, de 5 de outubro de 1988*. 13. ed. São Paulo: Ed. Revista dos Tribunais, 2011.

_____. Lei 8.069 de 13 julho de 1990. Dispões sobre o Estatuto da Criança e do Adolescente, e dá outras providências. *Diário Oficial da União*, Brasília, DF, 16 jul. 1990; ret. 27 set. 1990.

BRASIL. Lei 8.078 de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. *Diário Oficial da União*, Brasília, DF, 12 set. 1990.

_____. Lei 9.610 de 19 de fevereiro de 1998. Altera, atualiza e consolida legislação sobre direitos autorais é dá outras providências. *Diário Oficial da União*, Brasília, DF, 19 fev. 1998.

_____. Lei 11.690 de 10 de junho de 2008. Altera dispositivos do Decreto-Lei nº 3.689, de 3 de outubro de 1941 – Código de Processo Penal, relativos à prova, e dá outras providências. *Diário Oficial da União*, Brasília, DF, 10 jun. 2008.

_____. Lei 12.403 de 4 de maio de 2011. Altera dispositivos do Decreto-Lei nº 3.689, de 3 de outubro de 1941 - Código de Processo Penal, relativos à prisão processual, fiança, liberdade provisória, demais medidas cautelares, e dá outras providências. *Diário Oficial da União,* Brasília, DF, 05 maio 2011.

_____. Lei Complementar 87 de 13 de setembro de 1996. Dispõe sobre o imposto dos Estados e do Distrito Federal sobre operações relativas à circulação de mercadorias e sobre prestações de serviços de transporte interestadual e intermunicipal e de comunicação, e dá outras providências. *Diário Oficial da União*, Brasília, DF. 13 set. 1996.

BRUNO, Aníbal. *Direito penal*. 3. ed. Rio de Janeiro: Forense, 1967.

BUENO, P. A. T. A. C. Notícia histórica do direito penal brasileiro. In: BITTAR, Eduardo Carlos Bianca (Org.). *História do direito brasileiro*. São Paulo: Atlas, 2003. v. 1.

CALVO CARAVACA, Alfonso Luis; CARRASCOSA GONZÁLEZ, Javier. *Conflictos de leyes i conflictos de jurisdición em internet*. Madrid: Ed. Colex, 2001.

CARRAZA, Roque Antonio. Aplicações da cibernética ao direito em outras nações (Experiências e resultados. Opinião dos juristas). *Justitia*, São Paulo, ano 36, v. 94, p. 55-76, jan./mar. 1974.

CASTRO, Carla Rodrigues Araújo de. *Crimes de informática e seus aspectos processuais*. Rio de Janeiro: Lumen Juris, 2001.

CHAVES, Antônio. Aspectos jurídicos da juscibernética: direito de autor do programador. *Revista de Informação Legislativa*, Brasília, ano 19, n. 73, p. 280, jan./mar. 1982.

COLLI, Maciel. *Ciências penais:* perspectivas e tendências da contemporaneidade. A problemática detrás da responsabilização penal (objetiva) pela prática de um cibercrime. Curitiba: Juruá, 2011.

COSTA, Fernando José da. *Direito penal*: parte geral: 1º a 120. 2. ed. São Paulo: Atlas, 2007.

COSTA, José de Faria. Algumas reflexões sobre o estatuto dogmático do chamado "direito penal informático". *Revista Jurídica da Universidade Moderna*, v. 1, 1998.

COSTA JR., Paulo José da. *Código Penal comentado.* 9. ed. rev. e atual. São Paulo: DPJ Ed., 2007.

_____. *Curso de direito penal*. 9. ed. São Paulo: Saraiva, 2008.

_____. *O direito de estar só*. 4. ed. São Paulo: Ed. Revista dos Tribunais, 2007.

_____. *Tutela penal da intimidade*. São Paulo: Ed. Revista dos Tribunais, 1969.

_____; COSTA, Fernando José da. *Curso de direito penal*. 12. ed. São Paulo: Saraiva, 2010.

D`AGOSTINI, David et al. (Coord.). *Diritto penale dell'informatica dai computer crimes allá digital forensic*. Folì, Itália: Experta, 2007.

DAOUN, Alexandre Jean. Crimes informáticos. In: BLUM, Renato M. S. Opice et al. (Coord.). *Direito eletrônico*: a internet e os tribunais. Bauru, SP: EDIPRO, 2001. p. 203-221.

_____; BLUM, Renato M. S. Opice. *Cybercrimes.* In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto (Coords.). *Direito & internet*: aspectos jurídicos relevantes. São Paulo: Quartier Latin, 2008.

DE LUCCA, Newton; SIMÃO FILHO, Adalberto (Coords.). *Direito & internet*: aspectos jurídicos relevantes. São Paulo: Quartier Latin, 2008. v. 2.

DOTTI, René Ariel. *Curso de direito penal*: parte geral. Rio de Janeiro: Forense, 2002.

FERNANDES, Antonio Scarance. Crimes praticados pelo computador: dificuldade na apuração dos fatos. *Boletim do Instituto Manoel Pedro Pimentel*, São Paulo, n. 10, p. 26-27, dez. 1999.

_____. Crimes praticados pelo computador: dificuldade na apuração dos fatos. *Revista de Ciências Criminais*, São Paulo, ano 3, 1999.

_____. *Processo penal constitucional*. 6. ed. São Paulo: Ed. Revista dos Tribunais, 2010.

FERRARI, Eduardo Reale. *Medidas de segurança e direito penal no Estado democrático de direito.* São Paulo: Ed. Revista dos Tribunais, 2001.

FERREIRA, Ivette Senise. A criminalidade informática. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto (Coords.). *Direito & internet*: aspectos jurídicos relevantes. São Paulo: Quartier Latin, 2008. v. 2.

_____; BAPTISTA, Luiz Olavo (Coords.). *Novas fronteiras do direito na era digital*. São Paulo: Saraiva, 2002.

FINKELSTEIN, Maria Eugênia. Fraude eletrônica. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto (Coords.). *Direito & internet*: aspectos jurídicos relevantes. São Paulo: Quartier Latin, 2008. v. 2.

FIORILLO, Celso Antonio Pacheco. *Curso de direito ambiental brasileiro*. 12. ed. rev., atual. e ampl. São Paulo: Saraiva, 2011.

_____ (Org.). *Revista Brasileira de Direito da Comunicação Social e Liberdade de Expressão*. 1. ed. São Paulo: Fiuza, 2011.

FRAGOSO, Heleno Cláudio. *Lições de direito penal*: parte geral. Ed. rev. e atual. por Fernando Fragoso. Rio de Janeiro: Forense, 2004.

FRANÇA, Antonio de S. Cibernética jurídica. *Revista de Direito Civil, Imobiliário, Agrário e Empresarial*, São Paulo, ano 10. p. 118-135, jul./set. 1986.

GAGLIARDI, Pedro Luiz Ricardo. *Crimes cometidos com o uso de computador*. São Paulo, 1999. (Doutorado em Direito Penal) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 1999.

GARCIA, Dinio Santis. *Introdução a informática jurídica*. São Paulo: Ed. Universidade de São Paulo, 1976.

GIANNOTTI, Edoardo. *A tutela constitucional da intimidade*. Rio de Janeiro: Forense, 1987.

GOIS JR, José Caldas. *O direito na era das redes*: a liberdade e o delito no ciberespaço. Bauru, SP: EDIPRO, 2001.

GOMES, Mariângela Gama de Magalhães. O princípio da proporcionalidade no direito penal. 1. ed. São Paulo: Ed. Revista dos Tribunais, 2003. v. 1.

GOUVÊA, Sandra. *O direito na era digital.* Rio de Janeiro: Mauad, 1997.

GRABOSKU, Peter. *Computer crime*: a criminological overview. New York: Forum on Crime and Society, 1,1, 2001.

GRABOSKY, Peter. Computer crime: a criminological overview. New York. *Forum on Crime and Society*, v. 1, n. 1, p. 49, 2001.

GRECO FILHO, Vicente. Algumas observações sobre o direito penal e a internet. *Boletim IBCCRIM*, São Paulo, ed. especial, ano 8, n. 95, out. 2000.

GRINOVER, Ada Pellegrini; FERNANDES, Antonio Scarance; GOMES FILHO, Antonio Magalhães. *As nulidades no processo penal*. 7. ed. São Paulo: Malheiros Ed., 2001.

_____; GOMES FILHO, Antonio Magalhães; FERNANDES, Antonio Scarance; GOMES, Luiz Flávio. *Juizados Especiais Criminais*: comentários à Lei 9.099, de 26.09.1995. São Paulo: Ed. Revista dos Tribunais, 1996.

HASSEMER, Winfried. Oportunidades para la privacidad frente a las nuevas necesidades de control y las tecnologías de la informacion. Traducción de Alfredo CHIRINO Sanchez, L. L. M. *Nueva Doctrina Penal*, Buenos Aires, p. 107, 1999.

HESPANHA, Benedito. O poder normativo da internet e a regulamentação dos crimes virtuais. *Justiça do Direito*, Rio Grande do Sul, v. 1, n. 16, 2002.

HUNGRIA, Nelson. *Comentários ao Código Penal*. Rio de Janeiro: Revista Forense, 1955.

INELLAS, Gabriel Cesar Zaccaria de. *Crimes na internet.* 2. ed. São Paulo: Juarez de Oliveira, 2009.

JESUS, Damásio Evangelista de. *Direito penal*: parte geral. São Paulo: Saraiva, 1985. v. 1.

KANAAN, João Carlos. *Informática global*: tudo o que você precisa saber sobre informática. São Paulo: Pioneira, 1998.

KANT, Immanuel. *Para a paz perpétua*. Rianxo, Espanha: Instituto Galego de Estudos de Segurança Internacional e da Paz, 2006.

LAWRENCE, Lessig. *The future of ideas*: the fate of the commons in a connected world. New York: Random House, 2001.

LEONARDI, Marcel. *A responsabilidade civil dos provedores de serviços de internet*. São Paulo: Juarez de Oliveira, 2005.

LIBERO, Giuseppe Carrella Maria; TRIBERTI, Cesare. *Internet aspetti tecnic, tematiche sociali, incidenze giuridiche civili e penali*. Milano: Edizioni Maros, 2000.

LIMA, Paulo Marco Ferreira. *Crimes de computador e segurança computacional*. Campinas, SP: Millennium Ed., 2005.

LÓPEZ ZAMORA, Paula. *El ciberespacio y su ordenación*. Madrid: Difusión Jurídica y Temas de Actualidad, 2006.

LORENZETTI, Ricardo. L. *Comercio electrônico.* Buenos Aires: Abeledo Perrot, 2000.

LOSANO, Mario G. *Lições de informática jurídica*. São Paulo: Resenha Tributária, 1974.

MARQUES, José Frederico. *Tratado de direito penal*. Campinas: Bookseller, 1997.

MARTINS, A. G. Lourenço; MARQUES, J. A. Garcia; DIAS, Pedro Simões. *Cyberlaw em Portugal*: o direito das tecnologias da informação e comunicação. Ed. Centro Atlântico, Portugal, 2004.

MARZOCHI, Marcelo de Luca. *Direito.br*: aspectos jurídicos da internet no Brasil. São Paulo: LTr, 2000.

MATA Y MARTÍN. Ricardo. *Temas de direito da informática e da internet*. Porto, Portugal: Coimbra Ed., 2004.

MEIRA JUNIOR, José de Castro. A tutela penal dos cybercrimes e o projeto de lei contra os crimes de informática. *Revista da Fundação Escola Superior do Ministério Público do Distrito Federal e Territórios*, Brasília, v. 15, p. 117-159, dez. 2007.

MESTIERI, João. *Teoria elementar de direito criminal*. Rio de Janeiro: Cadernos Didáticos, 1971.

MIRABETE, Julio Fabbrini. *Manual de direito penal*. 22. ed. São Paulo: Atlas, 2005.

MOREIRA, Rômulo de Andrade. Globalização e crime. *Revista do Tribunais*, São Paulo, ano 92, n. 811, maio 2003.

MUAKAD, Irene Batista . *O infanticídio*: análise da doutrina médico legal e da prática judiciária. São Paulo: Ed. Mackenzie, 2002.

NALINI, José Renato. *Justiça.* São Paulo: Ed. Canção Nova, 2008.

NOGUEIRA, Sandro D`Amato. *Crimes de informática.* Lema/SP: BH Ed., 2008.

_____. *Pedofilia e o tráfico de menores pela internet*: o lado negro da web. Disponível em: <http://www.criminal.com.br>. Acesso em: 29 set. 2010.

NORONHA, E. Magalhães. *Direito penal.* São Paulo: Saraiva, 1977.

_____. *Direito penal*. São Paulo: Saraiva, 1997.

NUCCI, Guilherme de Souza. *Código Penal comentado*. 9. ed. São Paulo: Ed. Revista dos Tribunais, 2008.

PASCHOAL, Janaína Conceição. *Direito penal*: parte geral. 1. ed. Barueri/SP: Manole, 2003. v. 1.

PEREIRA, Alexandre Dias. A jurisdição na internet segundo o regulamento 44/2001 (e as alternativas extrajudiciais e tecnológicas). *Boletim da Faculdade de Direito, Universidade de Coimbra*, Coimbra, 2001.

PEREIRA, Ricardo Alcântara. *Direito eletrônico*. Bauru, SP: EDIPRO, 2001.

PIMENTEL, Alexandre Freire. *O direito cibernético*: um enfoque teórico e lógico-aplicativo. Rio de Janeiro: Renovar, 2000.

PINHEIRO, Patricia Peck. *Direito digital*. 4. ed. São Paulo: Saraiva, 2010.

PIRAGIBE, Célia. *Indústria da informática*: desenvolvimento brasileiro e mundial. Rio de Janeiro: Campus, 1985.

PLANTULLO, Vicente Lentini. *Estelionato eletrônico*: segurança na internet. 1. ed Curitiba: Juruá, 2006.

PRADO, Luiz Regis. *Curso de direito penal brasileiro*: parte geral, arts. 1º a 120. 7. ed. São Paulo: Ed. Revista dos Tribunais, 2007.

REALE, Miguel. *Lições preliminares de direito*. São Paulo: Saraiva, 2006.

REALE JÚNIOR, Miguel. *Instituições de direito penal*: parte geral. 3 ed. Rio de Janeiro: Forense, 2009.

_____; PASCHOAL, Janaína Conceição (Orgs.). *Mulher e direito penal*. Rio de Janeiro: Forense, 2007.

RIEM, Glauco. *Privacy e sicurezza*. Napoli: Edizioni Simone. 2002.

ROCHA, Fernando A. N. Galvão da. *Direito penal*: curso completo: parte geral. 2 ed. Belo Horizonte: Del Rey, 2007.

ROCHA FILHO, Valdir de Oliveira. *O direito e a internet*. 1 ed. Rio de Janeiro: Forense Universitária, 2002.

RODRIGUEZ DEVESA, Jose Maria. *Derecho Penal Español*: parte general. 9. ed. Madrid: Dykinson, 1985.

ROSSINI, Augusto. *Informática, telemática e direito penal*. São Paulo: Memória Jurídica Ed., 2004.

SÁ, Alvino Augusto de; SHECAIRA, Sérgio Salomão (Orgs.). *Criminologia e os problemas da atualidade*. 1. ed. São Paulo: Atlas, 2008.

SALT, Marcos. Delitos informáticos de carácter econômico. In: MAIER, Julio B. J. (Comp.). *Delitos no convencionales.* Buenos Aires: Editores del Puerto, 1994.

SALVADOR NETTO, Alamiro Velludo. *Finalidades da pena*: conceito material de delito e sistema penal integral. 1. ed. São Paulo: Quartier Latin, 2009. v. 1.

SÁNCHEZ GARCIA DE PAZ, Isabel; BLANCO CORDERO, Isidoro. Problemas de derecho penal internacional en la persecución de delitos cometidos a través de internet. *Actualidad Penal*, n. 7, 11-17 feb. 2002.

SANTOS, Antonio Jeová. *Dano moral na internet*. São Paulo: Método, 2001.

SANTOS, Coriolano Aurélio Almeida Camargo. Atual cenário dos crimes cibernéticos no Brasil. *OAB/São Paulo*. Disponível em: <http://www2.oabsp.org.br/asp/comissoes/sociedade_informacao/artigos/crimes_ciberneticos.pdf>.

SANTOS, Juarez Cirino. *Direito penal*. Rio de Janeiro: Forense, 1985.

SETTE, Luiz Augusto Azevedo. Dados sobre a proteção jurídica do software no Brasil. In: BLUM, Renato M. S. Opice et al. (Coord.). *Direito eletrônico*: a internet e os tribunais. Bauru, SP: EDIPRO, 2001. p. 611-630.

SHECAIRA, Sergio Salomão. *Criminologia.* 2. ed. rev., atual. e ampl. São Paulo: Ed. Revista dos Tribunais, 2008.

_____. *Responsabilidade penal da pessoa jurídica*. 3. ed. Rio de Janeiro: Elsevier, 2010. v. 1.

SILVA, Regina Beatriz Tavares; SANTOS, Manoel J. Pereira. *Responsabilidade civil na internet e nos demais meios de comunicação*. São Paulo: Saraiva, 2007.

SILVA, Rita de Cássia Lopes da. *Direito penal e sistema informático.* São Paulo: Ed. Revista dos Tribunais, 2003.

SILVEIRA, Renato de Mello Jorge. *Fundamentos da adequação social em direito penal.* São Paulo: Quartier Latin, 2010.

SIMAS FILHO, Mario. A face bandida. *Isto É*, São Paulo, n. 1496, 13 jun. 1998.

SMITH, Adam. *A riqueza das nações*: investigação sobre sua natureza e suas causas. Tradução de Luiz João Baraúna. São Paulo: Nova Cultural, 1996. v. 1 e 2.

SOUZA, Gills Lopes Macêdo; PEREIRA, Dalliana Vilar. A Convenção de Budapeste e as leis brasileiras. *Ministério Público do Estado do Amazonas*. Disponível em: <http://www.mp.am.gov.br/images/stories/A_convencao_de_Budapeste_e_as_leis_brasileiras.pdf>. Acesso em: 10 mar. 2011.

SZNICK, Valdir. *Novos Crimes e novas penas no direito penal*. São Paulo: Livr. e Ed. Universitária de Direito, 1992.

TERCEIRO, Cecílio da Fonseca Vieira Ramalho. *O problema na tipificação penal dos crimes virtuais*. Disponível em: <http://www.ibccrim.org.br>. Acesso em: 15 jun. 2002.

VALIN, Celso. A questão da jurisdição e da territorialidade nos crimes praticados pela internet. In: VOVER, Aires José (Org.). *Direito, sociedade e informática*: limites e perspectivas da vida digital. Florianópolis: Fundação Boiteux, 2000.

VELASCO NÚÑEZ, Eloy. *Delitos contra y a através de las nuevas tecnologias*: cómo reducir su impunidad? Madrid: Consejo General del Poder Judicial, 2006.

VIANNA, Túlio Lima. *Fundamentos de direito penal informático.* Rio de Janeiro: Forense, 2003.

VIEIRA, Sonia Aguiar do Amaral. *Inviolabilidade da vida privada e da intimidade pelos meios eletrônicos*. 1. ed. São Paulo: Juarez de Oliveira, 2002.

VOVER, Aires José (Org.). *Direito, sociedade e informática*: limites e perspectivas da vida digital. Florianópolis: Fundação Boiteux, 2000.

WIENER, Norbert. *Cibernética e sociedade*: uso humano de seres humanos. São Paulo: Cultrix, 1954.

***Sites* Consultados**

AGÊNCIA O ESTADO. Disponível em: <http://www.oestado.com.br>. Acesso em: 27 jun. 2000.

ARTEWEB. Disponível em: <http://www.arteweb.com.br/telefonica>. Acesso em: 26 jun. 2010.

BBS WIKI. Disponível em: <http://bbs.wikia.com>.

BUSCALEGIS. Disponível em: <http://www.buscalegis.ufsc.br/revistas/index.php/buscalegis/article/viewFile/10722/10287>. Acesso em: 14 jan. 2010.

CERT.br. *Cartilha de Segurança para a Internet*. Disponível em: <http:/cartilha.cert.br>. Acesso em: 26 abr. 2011.

_____. *Evolução do número de hosts do Brasil*. Disponível em: <http://cetic.br/hosts/index.htm>. Acesso em: 25 abr. 2011.

_____. Evolução do números de domínios. Disponível em: <http://www.cetic.br/dominios>. Acesso em: 25 abr. 2011.

CJB.NET. Disponível em: <http://www.euodeiosandy.cjb.net>. Acesso em: 26 jun. 2010.

COUNCIL OF EUROPE. Convention on Cybercrime. CETS No.: 185. Disponível em: <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG>. Acesso em: 29 abr. 2011.

CRIMINAL. Disponível em: <http://www.criminal.com.br>.

DICIONÁRIO de Informática. Disponível em: <http://www.dicweb.com/ww.htm>. Acesso em: 11 mar. 2011.

DICIONÁRIO UOL Tecnologia. Disponível em: <HTTP://tecnologia.uol.com.br/dicionarios>/. Acesso em: 16 abr. 2011.

DIGA não ao Bullying. Disponível em: <http://www.diganaoaobullying.com.br/bullying.htm>. Acesso em: 10 mar. 2011.

DIGA não à Erotização Infantil. Pedofilia na internet: números no Brasil são assustadores. Disponível em: <http://diganaoaerotizacaoinfantil.wordpress.com/2007/08/11/pedofilia-na-internet-numeros-no-brasil-sao-assustadores/>. Acesso em: 10 mar. 2011.

ESTATÍSTICAS dos Incidentes Reportados ao CERT.br. Disponível em: <http://www.cert.br/stats/incidentes>. Acesso em: 25 abr. 2011.

ESTATÍSTICAS sobre a Internet no Brasil. Disponível em: <http://www.tobeguarany.com/internet_no_brasil.php>. Acesso em: 14 jan. 2010.

FOLHA.COM. Disponível em: <http://www1.folha.uol.com.br/cotidiano>. Acesso em: 19 abr. 2011.

O GLOBO. Disponível em: <http://oglobo.globo.com/pais/noblat/posts/2010/06/11/sucesso-mundial-cala-boca-galvao-299364.asp>. Acesso em: 15 mar. 2011.

GUIA DO HARDWARE. Disponível em: <http://www.guiadohardware.net>.

IBCCRIM. Instituto Brasileiro de Ciências Criminais. Disponível em: <http://www.ibccrim.org.br>.

IDG NOW. Disponível em: <http://idgnow.uol.com.br/internet/2010/02/11/em-2011-declaracao-do-imposto-de-renda-sera-feita-apenas-pela-internet/>. Acesso em: 27 abr. 2011.

_____. Disponível em: <http://idgnow.uol.com.br/internet>. Acesso em: 04 jun. 2006.

INDEX MUNDI. Comparação entre países. *Número de servidores internet*. Disponível em: <http://www.indexmundi.com/g/r.aspx?v=140&l=pt>. Acesso em: 11 mar. 2011.

INVASOR de rede obteve dados pessoais de usuários, diz Sony. Disponível em: <http://www1.folha.uol.com.br/tec/907412-invasor-de-rede-obteve-dados-pessoais-de-usuarios-diz-sony.shtml>. Acesso em: 27 abr. 2011.

JACK Kevorkian. Disponível em: <http://pt.wikipedia.org/wiki/Jack_Kevorkian>. Acesso em: 10 mar. 2011.

MADCAPPS. Disponível em: <http://www.madcapps.com>. Acesso em: 15 mar. 2011.

NÚMERO de usuários de internet no mundo alcança os 2 bilhões. Diponível em: <http://g1.globo.com/tecnologia/noticia/2011/01/numero-de-usuarios-de-internet-no-mundo-alcanca-os-2-bilhoes.html>. Acesso em: 25 abr. 2011.

OECD. Disponível em: <http://www.oecd.org/home/0,3305,en_2649_201185_1_1_1_1_1,00.html>. Acesso em: 06 jan. 2010.

REGISTRO.BR. Estatísticas. Disponível em: <http://www.registro.br/estatisticas.html>. Acesso em: 16 fev. 2011.

SAFER NET. *Brasil é o campeão de crimes eletrônicos na América do Sul*. Disponível em: <http://www.safernet.org.br/site/noticias/brasil-%C3%A9-campe%C3%A3-crimes-eletr%C3%B4nicos-am%C3%A9rica-sul>. Acesso em: 16 fev. 2011.

_____. Disponível em: <http://www.denunciar.org.br/twiki/bin/view/SaferNet/WebHome>. Acesso em: 08 jan. 2010.

SENADO FEDERAL. Disponível em: <http://www.senado.gov.br>.

SUBMARINO. Disponível em: <http://submarino.com.br>. Acesso em: 27 abr. 2011.

SUPERIOR TRIBUNAL DE JUSTIÇA. Disponível em: <http://www.stj.jus.br>. Acesso em: 15 mar. 2011.

SYMANTEC. Relatório da Symantec sobre ameaças de segurança na internet detecta que atividade maliciosa continua a crescer em velocidade recorde. Disponível em: <http://www.symantec.com/pt/br/about/news/release/article.jsp?prid=20090414_01>. Acesso em: 06 jan. 2010.

TELECO. Inteligência em Telecomunicações. Disponível em: <http://www.teleco.com.br/internet.asp>. Acesso em: 04 jun. 2006.

THE UCLA ONLINE INSTITUTE FOR CYBERSPACE LAW AND POLICY. Disponível em: <http://gseis.ucla.edu/iclp/internet.html>. Acesso em: 29 abr. 2011.

WIKIPEDIA. Disponível em: <http://pt.wikipedia.org>.

WORD TRADE ORGANIZATION. Disponível em: <http://www.wto.org>. Acesso em: 03 fev. 2011.

GLOSSÁRIO[278]

ARP ou *Address Resolution Protocol* trata-se de um protocolo utilizado para encontrar um endereço da camada de enlace (Ethernet, por exemplo) a partir do endereço da camada de rede (como um endereço IP). O emissor difunde em *broadcast* um pacote ARP contendo o endereço IP de outro *host* e espera uma resposta com um endereço MAC respectivo. Cada máquina mantém uma tabela para reduzir a carga na rede. O ARP não está restrito a redes IP ou Ethernet, apesar de ser utilizado em outros protocolos de rede. Permite que o endereço IP seja independente do endereço Ethernet, mas apenas funciona se todos os *hosts* o suportarem.

Bit: menor unidade de dado que um sistema informático pode processar. Unidade mínima de informação possível de ser interpretada e armazenada pelo computador. Um bit pode assumir, apenas um de dois valores: 1(um) ou 0(zero). Qualquer circuito eletrônico é baseado em transistores, componentes extremamente simples, que permitem apenas dois estados: podem estar ligados ou desligados. Já que todo tipo de dado a ser processado precisa ser codificado em seqüências destes dois valores, foi criado o sistema binário, que permite representar qualquer tipo de informação, ou de operação aritmética através da combinação dos números 1 e 0, chamados de bit. Um único bit permite apenas duas combinações (1 ou 0), dois bits permitem 4 combinações, 3 bits permitem 8 combinações e assim por diante. Com 8 bits, temos o suficiente para um caracter de texto no sistema ASCII, com 24 bits temos o suficiente para um ponto numa imagem true-color, com 128 bits, temos o suficiente para gerar uma sofisticada chave de encriptação.

Boot: execução automática de instruções, apresentada no instante em que um computador é ligado. Bootstrap. É o processo de inicialização do micro, onde é lido primeiramente o BIOS e em seguida carregado o sistema operacional e programas. O termo bootstrap poderia ser traduzido para o Português como "levantar-se puxando as próprias botas". A

[278]Glossário elaborado a partir da tese de doutorado de Roberto de Araújo Chacon de Albuquerque, orientada pelo Professor Miguel Reale Jr., na Faculdade de Direito da USP, p. 198-201 (ALBUQUERQUE, Roberto de Araújo de Chacon de. op. cit.), do Dicionário de termos técnicos de informática - Guia do Hardware - escrito por Carlos E. Morimoto, Disponível em: <http://www.guiadohardware.net>. DICIONÁRIO de Informática. Disponível em: <http://www.dicweb.com/ww.htm>. Acesso em: 11 mar. 2011 e DICIONÁRIO UOL Tecnologia. Disponível em: <HTTP://tecnologia.uol.com.br/dicionarios>. Acesso em: 16 abr. 2011.

idéia tem uma certa semelhança com o processo de boot de um PC, onde ele se inicializa sozinho. Durante o Boot, são checados os componentes instalados no PC, contada a memória RAM, realizados testes rápidos para verificar se tudo está funcionando adequadamente e se não existem conflitos de Hardware, etc. Terminados os testes, o BIOS irá procurar o sistema operacional, na ordem estabelecida na opção "Boot Sequence" do Setup. A lista inclui o drive de disquetes, o HD, o CD-ROM, ou mesmo boot através do chip de Boot da placa de rede (caso tenha). Ao localizar o sistema operacional o BIOS executa os arquivos que iniciam seu carregamento e dá lugar a ele. A partir daí é com a Janela, o Pinguin, o Diabinho ou que mais esteja instalado no PC.

Browser: software para navegação na internet. V. Navegador.

Chat: salas de bate-papo, em tempo real, na internet. [Ing.] (Bate-papo). Programa que possibilita conversa em tempo real pelo computador entre internautas, por meio de linhas digitadas que podem aparecer ou não na tela de todos os usuários.

Chip: circuito eletrônico integrado. [Ing.] (lasca) Forma reduzida para microchip. [Junção das palavras micro (pequeno em grego + chip (lasca em inglês)]. Pastilha feita de material semicondutor, normalmente o silício, sobre a qual são implantados circuitos integrados. Desenvolvido pela norte-americana Intel, 1971, possibilitou a miniaturizaçao e barateamento dos equipamentos eletrônicos.

Computador: armazenador de dados. Toda máquina capaz de receber, armazenar e processar dados, de modo organizado e previamente programado e devolvê-los com a resposta para uma tarefa específica.

Correio eletrônico: correspondência enviada pela internet. [Do inglês, *e-mail*] Programa que permite a troca de mensagens pela Internet, criado, em 1971, por Ray Tomlison.

Cracker: especialista em informática (hacker) praticante de condutas ilícitas. [Ing. Substantivo do agente do verbo to crack, rachar]. Aficionado por informática, profundo conhecedor de linguagens de programação, que se dedica à compreensão mais íntima do funcionamento de sistemas operacionais e a desvendar códigos de acesso a outros

computadores. Ao contrário do hacker, utiliza seus conhecimentos para quebrar senhas de acesso a redes, provedores, programas e computadores com fins criminosos. Cf. Hacker.

Dado: qualquer informação armazenada, processada ou transmitida por sistema informático, incluindo programa de computador [Lat. Datum) Representação de uma informação, instrução, ou conceito, de modo que possa ser armazenada e processado por um computador.

Disco rígido: disco magnético inserido no computador, capaz de armazenar grande quantidade de dados. [Do inglês Hard disk] Suporte não removível e interno ao computador, para armazenamento magnético, de alta capacidade de dados digitais. Compõe-se de um conjunto de discos delgados, superpostos, revestidos de material magnético. É o componente onde estão armazenadas cópias do sistema operacional, programas, aplicativos, documentos e arquivos. Esse conteúdo é passível de alteração ou remoção.

Domínio: Conjunto de endereços na Internet organizado de forma hierárquica. O domínio superior identifica a área geográfica como ".br ou .edu". O segundo nível identifica uma organização, empresa ou outro local único na Internet. Um nome de domínio consiste de uma seqüência de nomes separados por ponto, por exemplo, www.uol.com.br, podendo ser entendida como a versão legível do endereço IP.

DoS (Denial of Service Attacks): remessa deliberada de uma grande quantidade de dados a um website, com o fim de levá-lo ao colapso.
[Ing. Sigla para Denial of Service] (Negação de serviço). Método utilizado por crackers para tirar um site da Internet. Aproveita-se de uma deficiência do protocolo TCP, que para estabelecer a conexão entre dois computadores, requer o envio de três mensagens: a solicitação da conexão; sua confirmação e a tréplica, em que é pedido o início da transmissão. A solicitação de comunicação é enviada para um endereço de resposta falso. O servidor envia a confirmação de recebimento do pedido de conexão para esse endereço e fica paralisado aguardando a resposta. Como milhares de pedi idênticos são feitos simultaneamente, a máquina tem esgotada sua capacidade e pára de funcionar. V. DdoS.

DOS: [Sigla em inglês para Disk Operating Systems] Designação genérica para os sistemas operacionais carregados a partir de uma unidade de disco, quando o computador é inicializado. Desprovido de interface gráfica, atende a comandos digitados pelo operador. Foi gradativamente substituído, nos PCs, a partir do surgimento dos sistemas operacionais de interface gráfica e amigável como o Windows.

E-mail: mensagem transmitida pela internet.

Hacker: grande conhecedor e as vezes invasor de sistemas informáticos. [Ing. Substantivo do agente do verbo to hack, abrir caminho com golpes cortantes]. Aficionado por informática, profundo conhecedor de linguagens de programação, que se dedica à compreensão mais íntima do funcionamento de sistemas operacionais e a desvendar códigos de acesso a outros computadores. O hacker não gosta de ser confundido com um cracker, pois ao contrário deste, não invade sistemas com fins criminosos, mas para ampliar seus conhecimentos ou pela satisfação de detectar suas possíveis falhas de segurança. Cf. Cracker.

Hacking: invasão de sistemas informáticos.

Hardware: unidade tangível do computador, o equipamento.
[Ing.] (Ferragens). Parte física de um computador e de seus periféricos.

Host: Computador ligado permanentemente à Rede, que mantém um repositório de serviços para outros computadores na internet. Também é chamado de nó, *in* http://tecnologia.uol.com.br/dicionarios/

Ícone: símbolo gráfico que permite identificar uma função, podendo ter, na internet, a mesma utilidade de um link.

ICQ: Software para comunicação entre internautas. [Ing. Forma reduzida, baseada na fonética da expresão I seek you] (Eu procuro você). Programa para bate-papo virtual, que avisa ao usuário em tempo real, quando seus interlocutores estão conectados à rede.

Além do bate-papo dispõe dos recursos de correio eletrônico e troca de arquivos. Executado em segundo plano permite o uso de outras aplicações.

Keytroke-logging: É um programa de computador que monitora as teclas usadas na digitação. Na maioria das vezes, ele vem com um cavalo-de-tróia e é utilizado para se descobrir login e senha de *e-mail*s e até mesmo de contas bancárias.

Link: vínculo de hipertexto que, ao ser acionado, remete o internauta a outra página da Web. [Ing.] (Vínculo). Forma reduzida de Hyperlink. V.Hiperlink. [Neo. formado pela junção das palavras hiper(texto) + link]. (Hipervínculo) Palavra, expressão ou imagem que permitem o acesso imediato à outra parte de um mesmo, ou outro documento, bastando ser acionado pelo ponteiro do mouse. Num hipertexto, um link, na forma de palavra ou expressão, vem sublinhado ou grafado em cor distinta da utilizada para o resto do texto.

Lista de discussão: listas de debate automatizadas via internet.

Mailbox: a caixa de correio, o espaço do disco rígido utilizado para armazenar *e-mail*s.

Modem: dispositivo que permite o envio de dados via linha telefônica. [Ing. acrôn. Mo(dulation) Dem(odulation)] (Modulação/Demodulação). Dispositivo sob a forma de periférico ou placa de circuito interna ao computador, que permite a comunicação entre computadores, por meio de linha telefônica. Seu princípio de funcionamento se baseia na modulação (conversão dos dados digitais do computador para freqüências de áudio do sistema telefônico) e vice-versa (demodulação).

Monitor: dispositivo de exibição de dados e imagens.

Mouse: dispositivo manual de entrada de dados, com ou sem fio. [Ing.] (Rato) Periférico que controla os movimentos do cursor na tela do computador, permitindo a abertura de programas e de menus e a seleção e execução de diversas funções por meio de um clique, entre outras funções. É composto por uma pequena caixa plástica, com dois ou três botões, dependendo do modelo, e um dispositivo de detecção mutidirecional acionado por um esfera localizada em sua parte inferior. Foi inventado pelo norte-americano Douglas

Engelbart, engenheiro e técnico em radares, nascido em 1925, no estado do Oregon. Apresentado publicamente, pela primeira vez em 1968 na Fall Joint Computer Conference, em São Francisco (EUA), o mouse só passou a ser usado na década dos 80. O primeiro computador a utilizá-lo foi o Xerox Star. Sua popularização, entretanto, deu-se quando foi incorporado ao Apple Lisa (1983). Passaram-se três décadas de sua invenção até que, Engelbart tivesse o reconhecimento por sua criação. Ele recebeu o prêmio Lemelson-Mit, no valor de US$ 500 mil. Na época de sua invenção foram-lhe pagos apenas U$ 10 mil pela venda da patente.

Navegador: o mesmo que browser.

Newsgroup: grupo de discussão no espaço virtual. [Ing.] (Grupo de Notícias). Como se dividem os grupos de discussão, segundo sua área de interesse.

Nickname: pseudônimo utilizado na internet. [Ing.] (Apelido). Pseudônimo que um indivíduo utiliza ao entrar numa sala de bate-papo.

Offline: não conectado em rede. [Ing.] (Fora de linha). Diz-se do periférico que esteja desconectado de um computador ou de um computador em relação à rede. Cf. Online.

Online: conectado em rede. [Ing. On, significando posição, em; ou continuidade + Line, linha] (Em linha, linha contínua). Termo utilizado para designar quando um computador está conectado à uma rede ou qualquer tipo de comunicação entre computadores. Cf. Offline.

Output: ação de transferência de dados do computador para o usuário. [Ing.] Resultado do processamento de uma informação enviada a um computador .

Palmtop: espécie de computador portátil, dentre outros existentes. Organizador pessoal desenvolvido por Jeff Hawkins e lançado pela Palm Computing, hoje Palm Inc., em 1996, inicialmente com o nome de Pilot. Sucesso comercial, tornou-se sinônimo de computadores de mão.

Periféricos: mouse, impressora, scanner, monitor. Todo o dispositivo que se pode conectar à CPU de um computador, como por exemplo, monitor, mouse, teclado, caixa de som, impressora, câmara digital, etc.

Print-out: cópia impressa de dados de um sistema informático.

Programa de computador: o mesmo que software.

RAM (Random Acess Memory) memória de acesso aleatório, que retém dados enquanto houver suprimento de energia elétrica. [Ing. Sigla para Random Acces Memory] (Memória de Acesso Randômico) Área da memória de um computador, cujo conteúdo pode ser lido e gravado. Armazena temporariamente dados e instruções de que o processador necessita para execução de tarefas. É responsável pelos cálculos, busca de dados e execução de programas e aplicativos. Seu conteúdo é apagado sempre que o computador é desligado. Quanto maior for a memória RAM maior será a velocidade de processamento do computador. Cf. ROM.

Rede: conexão à internet.

Redes de computadores: conjunto de sistemas informáticos interconectados.
Conjunto de computadores interligados, de modo a permitir aos usuários o compartilhamento de programas e arquivos. Uma rede pode ser permanente, quando a conexão é feita por cabo, ou temporária, quando por linha telefônica.

ROM (Read Only Memory): memória exclusiva de leitura. [Ing. Sigla para Read Only Memory] (Memória Somente para Leitura). Área da memória de um computador, cujo conteúdo pode ser lido, mas não modificado. Contém as informações necessárias para fazer o computador entrar em operação assim que é ligado e para ler um disquete ou CD-ROM. Cf. RAM.

Servidor: computador que armazena págnias na Web. Computador central, em uma rede, responsável pela administração e fornecimento de programas e informações aos demais computadores a ele conectados. O mesmo que host.

Sistema informático: compreende o conjunto formado pelo hardware e software.

Site: o mesmo que website. [Ing.] (Sítio). Conjunto de documentos escritos em linguagem HTML, pertencentes a um mesmo endereço (URL), disponível na Internet. Erroneamente é empregado como sinônimo de homepage. Cf. Homepage.

Software: unidade intangível do computador, programa que o instrui como executar uma tarefa. [Ing. Soft = suave ware = utensílio]. Termo cunhado por analogia a hardware. Conjunto de instruções, programas e dados a eles associados, empregados durante a utilização do computador. O mesmo que programa ou aplicativo.

Spam: recebimento de *email* não solicitado, normalmente com propaganda comercial. Mensagem não solicitada enviada por correio eletrônico a um grande número de destinatários, contendo correntes, publicidade, material pornográfico, propostas de enriquecimento fácil, pedidos de ajuda para pessoas necessitadas, histórias absurdas etc.

Suporte de dados: disquete, CD-ROM, cartão bancário etc.

Toolkits: toolkit é um conjunto de widgets, elementos básicos de uma GUI. Normalmente são implementados como uma biblioteca de rotinas ou uma plataforma para aplicativos que auxiliam numa tarefa.

Virtual/virtualidade: termo empregado no mundo digital para se referir ao que diz respeito a comunicação em rede.

Vírus: programa de computador que danifica ou copia outros programas ao ser executado. Programa desenvolvido com intenção nociva, que inserido em um computador, pode causar queda da sua performance, destruição de arquivos e disco rígido, ocupar espaço livre de memória, entre outros danos. As formas mais comuns de contaminação são os disquetes e arquivos enviados por correio eletrônico. Ex. Melissa.

Web: designação comum para World Wide Web. [Ing.] (Teia). Forma reduzida de se referir à WWW.

Webpages: textos da WWW que são armazenados em servidores da Web.

Website: conjunto de arquivos conectados entre si que são exibidos via internet.

World Wide Web: conjunto interligado de documentos em hipertexto, que se convencionou chamar de páginas da Web. [Ing.] (Teia de Alcance Mundial) Conjunto interligado de documentos escritos em linguagem HTML armazenados em servidores HTTP ao redor do mundo. Foi concebida pelo físico inglês Tom Berners-Lee em 1989.

WWW: abreviatura para World Wide Web.

ANEXO A

INTERNATIONAL REVIEW OF CRIMINAL POLICY - UNITED NATIONS MANUAL ON THE PREVENTION AND CONTROL OF COMPUTER-RELATED CRIME

The burgeoning of the world of information technologies has, however, a negative side: it has opened the door to antisocial and criminal behavior in ways that would never have previously been possible. Computer systems offer some new and highly sophisticated opportunities for law-breaking, and they create the potential to commit traditional types of crimes in non-traditional ways. In addition to suffering the economic consequences of computer crime, society relies on computerized systems for almost everything in life, from air, train and bus traffic control to medical service coordination and national security. Even a small glitch in the operation of these systems can put human lives in danger. Society's dependence on computer systems, therefore, has a profound human dimension. The rapid transnational expansion of large-scale computer networks and the ability to access many systems through regular telephone lines increases the vulnerability of these systems and the opportunity for misuse or criminal activity. The consequences of computer crime may have serious economic costs as well as serious costs in terms of human security.

CONTENTS

Introduction

1. When future historians scrutinize the second half of the twentieth century, they will be reviewing what is sure to be known as the Information Revolution. Humankind has progressed further in the last 50 years than in any other period of history. One of the reasons for this rapid advance in technology is the computer. Technological capabilities have increased at an accelerating pace, permitting ever larger and more sophisticated systems to be conceived and allowing ever more sensitive and critical functions to be assigned to them.1

2. Indeed, the world is undergoing a second Industrial Revolution. Information technology today touches every aspect of life, irrespective of location on the globe. Everyone's daily activities are affected in form, content and time by the computer. Businesses, Governments and individuals all receive the benefits of this Information Revolution. While providing tangible benefits in time and money, the computer has also had an impact on everyday< life, as computerized routines replace mundane human tasks. 2 More and more of out businesses, industries, economies, hospitals and Governments are becoming dependent on computers. Computers are not only used extensively to perform the industrial and economic functions of society but are also used to perform many functions upon which human life itself depends. medical treatment and air traffic control are but two examples. Computers are also used to store confidential data of a political, social, economic or personal nature. They assist in the improvement of economies and of living conditions in all countries. Communications, organizational functioning and scientific and industrial progress have developed so rapidly with computer technology that our form of living has changed irreversibly.

3. With the computer, the heretofore impossible has now become possible, The computer has allowed large volumes of data to be reduced to high-density, compact storage, nearly imperceptible to the human senses, It has allowed an exponential increase in speed, and even the most complex calculations can be completed in milliseconds. The miniaturization of processors has permitted worldwide connectivity and communication. Computer literacy continues o grow.

4. The burgeoning of the world of information technologies has, however, a negative side: it has opened the door to antisocial and criminal behavior in ways that would never have previously been possible. Computer systems offer some new and highly sophisticated opportunities for law-breaking, and they create the potential to commit traditional types of crimes in non-traditional ways. In addition to suffering the economic consequences of computer crime, society relies on computerized systems for almost everything in life, from air, train and bus traffic control to medical service coordination and national security. Even a small glitch in the operation of these systems con put human lives in danger. Society's dependence on computer systems, therefore, has a profound human dimension. The rapid transnational expansion of large-scale computer networks and the ability to access many systems through regular telephone lines increases the vulnerability of these systems and the opportunity for misuse or criminal activity. The consequences of computer crime may have serious economic costs as well as serious costs in terms of human security.

A. The international problem

5. Laws, criminal justice systems and international cooperation have not kept pace with technological change. Only a few countries have adequate laws to address the problem, and of these, not one has resolved all of the legal, enforcement and prevention problems.

6. When the issue is elevated to the international scene, the problems and inadequacies are magnified. Computer crime is a new form of transnational crime and effectively addressing it requires concerted international cooperation. This can only happen, however, if there is a common framework for understanding what the problem is and what solutions there may be.

7. Some of the problems surrounding international cooperation in the area of computer crime and criminal law can be summarized as follows:

1. The lack of global consensus on what types of conduct should constitute a computer-related crime;

2. The lack of global consensus on the legal definition of criminal conduct;

3. The lack of expertise on the part of police, prosecutors and the courts in this field;

4. The inadequacy of legal powers for investigation and access to computer systems, including the inapplicability of seizure powers to intangibles such as computerized data;

5. The lack of harmonization between the different national procedural laws concerning the investigation of computer-related crimes;

6. The transnational character of many computer crimes;

7. The lack of extradition and mutual assistance treaties and of synchronized law enforcement mechanisms that would permit international cooperation, or the inability of existing treaties to take into account the dynamics and special requirements of computer-crime investigation.

B. Regional action

8. Examination of these questions has already occurred to some degree at the international and regional levels. In particular, the Organisation for Economic Co-operation and Development (OECD) and the Council of Europe have produced guidelines for policy makers and legislators.

9. In 1983, OECD undertook a study of the possibility of an international application and harmonization of criminal laws to address the problem of computer crime or abuse. In 1986, it published Computer-Related Crime: Analysis of Legal Policy, a report that surveyed the existing laws and proposals for reform in a number of Member States and recommended a minimum list of abuses that countries should consider prohibiting and penalizing by criminal laws, for example, computer fraud and forgery, the alteration of computer programs and data and the copyright and interception of the communications or other functions of a computer or telecommunication system. A majority of members of the Committee on Information, Computer and Communications Policy also recommended that criminal protections should be developed for other types of abuse, including the theft of trade secrets and unauthorized access to, or use of, computer systems.

10. Following the completion of the OECD report, the Council of Europe initiated its own study of this issue with a view to developing guidelines to assist legislators in determining what conduct should be prohibited by the criminal law and how this should be achieved, having regard for the

conflict of interest between civil liberties and the need for protection. The minimum list of OECD was expanded considerably by adding other types of abuses that were recommended as deserving of the application of the criminal law. The Select Committee of Experts on Computer-Related Crime of the Committee on Crime Problems examining these questions also addresses other areas, such as privacy protection, victims, prevention, procedural issues such as the international search and seizure of data banks, and international cooperation in the investigation and prosecution of computer crime. Recommendation R(89)9 of the Council of Europe on computer-related crime, which contains guidelines for national legislatures, was adopted by the Committee of Ministers of the Council of Europe on 13 September 1989.

11. In 1992, OECD developed a set of guidelines for the security of information systems, which is intended to provide a foundation on which States and the private sector may construct a framework for the security of information systems. In that same year, the Council of Europe began a study that will concentrate on procedural and international cooperation issues related to computer crime and information technology.

C. The need for global action

12. Despite these international efforts, much remains to be accomplished in order to achieve international cooperation. While much of the international work has so far been centered in western European and OECD countries, the potential extent of computer crime is as broad as the extent of the international telecommunication systems. All regions of the world must become involved in order to prevent this new form of criminality.

13. Ensuring the integrity of computer systems is a challenge facing both developed and developing countries. It is predicted that within the next decade, it will be necessary for developing nations to experience significant technological growth in order to become economically self-sufficient and more competitive in world markets. As dependence on computer technology grows in all nations, it will be crucial to ensure that the rate of technological dependence does not outstrip the rate at which the corresponding social, legal and political frameworks are developing. It is important to plan for security and crime prevention at the same time that computer technology is being implemented.

14. The participation of both developed and developing nations in international computer-crime initiatives is an encouraging trend. For example, the three associated conferences on computer crime at Würzburg in October 1992 were attended by delegates from Africa, Asia, eastern and western Europe, Latin America, the Middle East and North America. An adequate response to computer crime requires that both developed and developing nations should encourage regional and international organizations to examine the issue and promote crime prevention programs on a national level.

15. This strategy is necessary, both immediately and in the long term, to ensure international cooperation and to foster the political will to create a secure information community and the universal criminalization of computer crime.

D. Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders

16. Following the Seventh United Nations Congress on the Prevention of Crime and the Treatment of Offenders, which took place in 1985, the Secretary-General prepared a report entitled "Proposals for concerted international action against forms of crime identified in the Milan Plan of Action" (E/AC.57/1988/16). Computer crime was discussed in paragraphs 42-44 of that report.

17. In preparation for the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, the Asia and Pacific Regional Preparatory Meeting indicated concern with the effects of technological progress, as reflected in computer crimes (A/CONF.144)RPM.2).

18. At the 12th plenary meeting of the Eighth Congress, which took place in 1990, the representative of Canada introduced a draft resolution on computer-related crimes on behalf of the 21 sponsors. At its 13th plenary meeting, the Congress adopted the resolution, in which it, inter alia, called upon Member States to intensify their efforts to combat computer crime by considering, if necessary, the following measures:

1. "Modernization of national criminal laws and procedures, including measures to:

- Ensure that existing offences and laws concerning investigative powers and admissibility of evidence in judicial proceedings adequately apply and, if necessary, make appropriate changes;
- In the absence of laws that adequately apply, create offences and investigative and evidentiary procedures, where necessary, to deal with this novel and sophisticated form of criminal activity;
- Provide for the forfeiture or restitution of illegally acquired assets resulting from the commission of computer-related crimes;

2. Improvement of computer security and prevention measures, taking into account the problems related to the protection of privacy, the respect for human rights and fundamental freedoms and any regulatory mechanisms pertaining to computer usage;

3. Adoption of measures to sensitize the public, the judiciary and law enforcement agencies to the problem and the importance of preventing computer-related crimes;

4. Adoption of adequate training measures for judges, officials and agencies responsible for the prevention, investigation, prosecution and adjudication of economic and computer-related crimes;

5. Elaboration, in collaboration with interested organizations, of rules of ethics in the use of computers and the teaching of these rules as part of the curriculum and training in informatics;

6. Adoption of policies for the victims of computer-related crimes which are consistent with the United Nations Declaration of Basic Principles of Justice for Victims of Crime and Abuse of

Power, including the restitution of illegally obtained assets, and measures to encourage victims to report such crimes to the appropriate authorities". 5

19. In its resolution, the Eighth Congress also recommended that the Committee on Crime Prevention and Control should promote international efforts in the development and dissemination of a comprehensive framework of guidelines and standards that would assist Member States in dealing with computer-related crime and that it should initiate and develop further research and analysis in order to find new ways in which Member States may deal with the problem of computer-related crime in the future. It also recommended that these issues should be considered by an ad hoc meeting of experts and requested the Secretary-General to consider the publication of a technical publication on the prevention and prosecution of computer-related crime.

I. The Phenomenon of Computer Crime

A. Definition of computer crime

20. It is difficult to determine when the first crime involving a computer actually occurred. The computer has been around in some form since the abacus, which is known to have existed in 3500 B.C. in Japan, China and India. In 1801 profit motives encouraged Joseph Jacquard, a textile manufacturer in France, to design the forerunner of the computer card. This device allowed the repetition of a series of steps in the weaving of special fabrics. So concerned were Jacquard's employees with the threat to their traditional employment and livelihood that acts of sabotage were committed to discourage Mr. Jacquard from further use of the new technology. A computer crime had been committed.

21. There has been a great deal of debate among experts on just what constitutes a computer crime or a computer-related crime. Even after several years, there is no internationally recognized definition of those terms. Indeed, throughout this Manual the terms computer crime and computer-related crime will be used interchangeably. There is no doubt among the authors and experts who have attempted to arrive at definitions of computer crime that the phenomenon exists. However, the definitions that have been produced tend to relate to the study for which they were written. The intent of authors to be precise about the scope and use of particular definitions means, however, that using these definitions out of their intended context often creates inaccuracies. A global definition of computer crime has not been achieved; rather, functional definitions have been the norm.

22. Computer crime can involve criminal activities that are traditional in nature, such as theft, fraud, forgery and mischief, all of which are generally subject everywhere to criminal sanctions. The computer has also created a host of potentially new misuses or abuses that may, or should, be criminal as well.

23. In 1989, expanding on work that had been undertaken by OECD, the European Committee on Crime Problems of the Council of Europe produced a set of guidelines for national legislators that enumerated activities that should be subject to criminal sanction. By discussing the functional characteristics of target activities, the Committee did not attempt a formal definition of computer crime but left individual countries to adapt the functional classification to their particular legal systems and historical traditions.

24. The terms "computer misuse" and "computer abuse" are also used frequently, but they have significantly different implications. Criminal law recognizes the concepts of unlawful or fraudulent intent and of claim of right; thus, any criminal laws that relate to computer crime would need to distinguish between accidental misuse of a computer system, negligent misuse of a computer system and intended, unauthorized access to or misuse of a computer system, amounting to computer abuse. Annoying behavior must be distinguished from criminal behavior in law.

25. In relation to the issue of intent, the principle of claim of right also informs the determination of criminal behavior. For example, an employee who has received a password from an employer, without direction as to whether a particular database can be accessed, is unlikely to be considered guilty of a crime if he or she accesses that database. However, the principle of claim of right would not apply to the same employee who steals a password from a colleague to access that same database, knowing his or her access is unauthorized; this employee would be behaving in a criminal manner.

26. A distinction must be made between what is unethical and what is illegal; the legal response to the problem must be proportional to the activity that is alleged. It is only when the behavior is determined to be truly criminal that criminal prohibition and prosecution should be sought. The criminal law, therefore, should be employed and implemented with restraint.

B. The extent of crime and losses

27. Only a small portion of crimes come to the attention of the law enforcement authorities. In his book Computer Security, J. Carroll states that "computer crime may be the subject of the biggest cover-up since Watergate". While it is possible to give an accurate description of the various types of computer offences committed, it has proved difficult to give an accurate, reliable overview of the extent of losses and the actual number of criminal offences. At its Colloquium on Computer Crimes and Other Crimes against Information Technology, held at Würzburg, Germany, from 5 to 8 October 1992, AIDP released a report on computer crime based on reports of its member countries that estimated that only 5 per cent of computer crime was reported to law enforcement authorities.

28. The number of verifiable computer crimes is not, therefore, very high. This fact notwithstanding, authorities point out that the evidence of computer crime discernible from official statistical sources, studies and surveys indicates the phenomenon should be taken seriously.

29. The American Bar Association conducted a survey in 1987: of 300 corporations and government agencies, 72 claimed to have been the victim of computer-related crime in the 12-month period prior to the survey, sustaining losses estimated to range from $ 145 million to $ 730 million. In 1991, a survey of security incidents involving computer-related crime was conducted at 3,000 Virtual Address Extension (VAX) sites in Canada, Europe and the United States of America. Seventy-two per cent of the respondents said that a security incident had occurred within the previous 12-month period; 43 per cent indicated that the security incident they had sustained had been a criminal offence. A further 8 per cent were uncertain whether they had sustained a security incident. Similar surveys conducted around the world report significant and widespread abuse and loss.

30. Law enforcement officials indicate from their experience that recorded computer crime statistics do not represent the actual number of offences; the term "dark figure", used by criminologists to refer to unreported crime, has been applied to undiscovered computer crimes. The invisibility of computer crimes is based on several factors. First, sophisticated technology, that is, the immense, compact storage capacity of the computer and the speed with which computers function, ensures that computer crime is very difficult to detect. In contrast to most traditional areas of crime, unknowing victims are often informed after the fact by law enforcement officials that they have sustained a computer crime. Secondly, investigating officials often do not have sufficient training to deal with problems in the complex environment of data processing. Thirdly, many victims do not have a contingency plan for responding to incidents of computer crime, and they may even fail to acknowledge that a security problem exists.

31. An additional cause of the dark figure is the reluctance of victims to report computer offences once they have been discovered. In the business sector, this reluctance is related to two concerns. Some victims may be unwilling to divulge information about their operations for fear of adverse publicity, public embarrassment or loss of goodwill. Other victims fear the loss of investor or public confidence and the resulting economic consequences. Some experts have suggested that these factors have a significant impact on the detection of computer crime.

C. Perpetrators of computer crime

32. History has shown that computer crime is committed by a broad range of persons: students, amateurs, terrorists and members of organized crime groups. What distinguishes them is the nature of the crime committed. The individual who accesses a computer system without further criminal

intent is much different from the employee of a financial institution who skims funds from customer accounts.

33. The typical skill level of the computer criminal is a topic of controversy. Some claim that skill level is not an indicator of a computer criminal, while others claim that potential computer criminals are bright, eager, highly motivated subjects willing to accept a technological challenge, characteristics that are also highly desirable in an employee in the data-processing field.

34. It is true that computer criminal behavior cuts across a wide spectrum of society, with the age of offenders ranging from 10 to 60 years and their skill level ranging from novice to professional. Computer criminals, therefore, are often otherwise average persons rather than supercriminals possessing unique abilities and talents. 8 Any person of any age with a modicum of skill, motivated by the technical challenge, by the potential for gain, notoriety or revenge, or by the promotion of ideological beliefs, is a potential computer criminal.

35. According to a number of studies, however, employees represent the largest threat, and indeed computer crime has often been referred to as an insider crime. One study estimated that 90 per cent of economic computer crimes were committed by employees of the victimized companies. A recent survey in North America and Europe indicated that 73 per cent of the risk to computer security was attributable to internal sources and only 23 per cent to external criminal activity.

36. As advances continue to be made in remote data processing, the threat from external sources will probably increase. With the increasing connectedness of systems and the adoption of more user-friendly software, the sociological profile of the computer offender may change.

37. Owing to the greater complexity of certain computer routines and augmented security measures, it is becoming increasingly unlikely that any one person will possess all the information needed to use a computer system for criminal purposes. Organized computer criminal groups, composed of members from all over the world, are beginning to emerge. Corresponding with this increasing cooperation in criminal activity, the escalating underground use of electronic bulletin boards for clandestine criminal communication has been detected around the world. Rapidly improving telecommunication technology has added to the threat from external sources. Computer-based voice mailbox systems, for example, are being used by the computer criminal community to exchange stolen access numbers, passwords and software.

38. The advent of viruses and similar mechanisms whereby computer software can be made to act almost on its own initiative poses a new and significant threat. Sophisticated viruses and devices such as "logic bombs" and "trojan horses", discussed below, can be targeted for specific objectives at specific industries to commit a variety of traditional criminal offences, from mere mischief of extortion. These crimes, furthermore, can be committed immediately or can be planted to spring at a future date.

39. Computer criminals have gained notoriety in the media and appear to have gained more social acceptability than traditional criminals. The suggestion that the computer criminal is a less harmful individual, however, ignores the obvious. The current threat is real. The future threat will be directly proportional to the advances made in computer technology.

D. The vulnerability of computer systems to crime

40. Historically, economic value has been placed on visible and tangible assets. With the increasing appreciation that intangible data can possess economic value, they have become an economic asset that can be targeted for crime. Tangible assets in the computer environment, therefore, often have a double value. The replacement cost of a piece of computer equipment may represent only a small portion of the economic loss caused by the theft of, or damage to, that equipment. Of much greater significance is the value of the information lost or made unaccessible by the misappropriation or damage.

41. Computer systems are particularly vulnerable to threats because of a number of interacting factors. The more significant of these are analysed briefly below.

1. Density of information and processes

42. Storage technology has allowed the development of filing systems that can accommodate billions of characters of data on-line. Providing different access privileges for different users of such systems is often difficult. A further problem lies in the fact that, owing to the methods for accessing stored information, a single error can have widespread impact. This fact can be used to great advantage by a party who wants to corrupt data or disrupt service.

43. At the same time, memory management techniques allow many independent processes to be supported concurrently within a single operating system. Independent data files can be combined to produce new and unforeseen relationships. Data items may be linked to produce a new item with a higher level of sensitivity than the original discrete data components. The centralization of information and processing functions provides an attractive target for the infiltrator or saboteur intent on attacking the functions or information assets of an organization.

44. The density of data stored on such media as tapes, diskettes, cassettes and microfilms means that the loss or theft of such items can be very significant.

2. System accessibility

45. Before security became a significant design criterion, the goal was often to provide the maximum computing capability to the largest possible user community. Access concerns once confined to the restricted computer room area must now be extended to remote terminal locations and interconnecting communications links. However, remote terminal stations and transmission

circuits are often not subject to the same controls as those in the main centre. Two forms of attack that exploit remote access are the use of fraudulent identification and access codes to obtain the use of system resources and the unauthorized use of an unattended terminal, logged on by an authorized person.

46. Because of the desire to give system users maximum capability, unrestricted access privileges are often granted rather than allowing only the privileges necessary to perform an intended function. A transaction-oriented system permitting read-only or inquiry-only access offers a greater degree of protection than a system offering full programming capability.

47. Many systems in current use offer very limited ability to control user capabilities related to passive data and programs on a read-only, read-write or execute basis. This situation frequently necessitates operating on the assumption that every user has the capability to use the full computing potential of the operating system. A known penetration technique that utilizes this weakness involves disguising user instructions intended for clandestine purposes as a common utility, such as a file-copying routine, or inserting them into an existing routine. When the illicit code is activated, it performs functions more privileged than were intended for that user.

48. Finally, computer control functions are normally made accessible to numerous support and maintenance personnel. Tampering with software or hardware logic to obtain extended privilege or to disable protection features has been known to occur. The exposure provided through increasingly easy access to electronic data processing (EDP) resources is an important contributor to the vulnerability of modern computer systems.

3. Complexity

49. The typical operating environment of medium- and large-scale systems is characterized by support for local batch, remote batch, interactive and, occasionally, real-time user modes. Typical operating systems contain from 200,000 to 25 million individual instructions. The number of logic states that are possible during execution in a multiprogramming or multiprocessing environment approaches infinity. It is not surprising that such systems are not fully understood by anyone, including the designers, or that they are often unreliable. It is only possible to prove the presence of errors, not their absence, and any system error can result in down time or a potential security fault. Even when systems have been carefully designed, errors in implementation, maintenance and operation can still occur. The prospective infiltrator can be expected to take full advantage of the uncertainties created by system complexity. Incidents have been noted where deliberate attempts to confuse operators, or to interrupt systems by attacking little-known weaknesses, have been instrumental in producing security violations.

4. Electronic vulnerability

50. The reliance of computer systems on electronic technology means that they are subject to problems of reliability, fragility, environmental dependency and vulnerability to interference and interception. On systems using telecommunications, these vulnerabilities extend to the whole communications network in use.

51. Traditional forms of electronic eavesdropping can be readily adapted to exploit data-processing systems. They include wire-tapping and bugging, the analysis of electromagnetic radiations from equipment and monitoring of the cross-talk induced in adjacent electrical circuits. Interconnecting data communications circuits also suffer the same vulnerabilities, and communications on them can be subject to misrouting. A variation on wire-tapping involves the illegal use of a minicomputer to intercept data communications and to generate false commands or responses to other system components.

52. In the commission of a fraud, electronic technology has an advantage over manual data manipulation, which generally leaves behind an audit trail. Computer data, however, can be instantly changed or erased with minimal chance of detection, by, for example, a virus or logic bomb. The computer criminal can easily modify systems to perpetrate the fraud and then cover the evidence of the offence. It is suggested, moreover, that data processing is protected by only one tenth of the controls afforded to the same process in the manual environment, an insufficiency that facilitates the opportunity to commit crime without detection.

53. The performance of EDP systems may also be adversely affected by electromagnetic interference. Conducted or radiated electrical disturbances can interfere with the operation of electronic equipment. The system may suffer only very temporary and intermittent impairment, measurable in microseconds and from which recovery is possible, or it may suffer complete equipment failure, resulting in an inability to process.

54. All hardware is susceptible to failure through ageing, physical damage and environmental change. To ensure that error propagation is confined to non-sensitive functions, i.e., that the system fails safely, malfunctions must be detected immediately. Progress is being made towards this goal, but few designs in current use offer the desired level of reliability.

5. Vulnerability of electronic data-processing media

55. It is sometimes inferred that a degree of security is provided by the inability of humans to translate machine-readable data in the form of punched holes in cards or tape, magnetic states on tapes, drums and disks, and electrical states in processing or transmission circuits. In practice, not only can such computerized information codes be readily interpreted by most technical personnel, but the data obscurity created has the additional negative effect of creating identification and accounting problems.

56. Because the contents of most EDP media are not visually evident, data-processing personnel are often required to handle sensitive files without being aware they are doing so. As a result, the control of data items becomes a problem. Scratched tapes, discarded core memories can all contain residual data that may demand special attention. Because identity and accountability have been lost, safeguards are frequently relaxed for these items even though the same information is protected elsewhere in the system. The ease with which such sources of information can be utilized has resulted in several well-publicized system penetrations.

6. Human factors

57. As discussed above, employees represent the greatest threat in terms of computer crime. It is not uncommon, operators, media librarians, hardware technicians and other staff members to find themselves in positions of extraordinary privilege in relation to the key functions and assets of their organization. A consequence of this situation is the probability that such individuals are frequently exposed to temptation.

58. A further complication is the tendency on the part of management to tolerate less stringent supervisory controls over EDP personnel. The premise is that the work is not only highly technical and specialized but difficult to understand and control. As an example systems software support is often entrusted to a single programmer who generates the version of the operating system in use, establishes password or other control lists and determines the logging and accounting features to be used. In addition, such personnel are often permitted, and sometimes encouraged, to perform these duties during non-prime shift periods, when demands on computer time are light. As a result, many of the most critical software development and maintenance functions are performed in an unsupervised environment. It is also clear that operators, librarians and technicians often enjoy a degree of freedom quite different from that which would be considered normal in a more traditional employment area.

59. There is another factor at play in the commission of computer crime. Criminological research has identified a variation of the Robin Hood syndrome: criminals tend to differentiate between doing harm to individual people, which they regard as highly immoral, and doing harm to a corporation, which they can more easily rationalize. Computer systems facilitate these kinds of crimes, as a computer does not show emotion when it is attached. 12

60. Situations in which personnel at junior levels are trusted implicitly and given a great deal of responsibility, without commensurate management control and accountability, occur frequently in the EDP environment. Whether the threat is from malicious or subversive activities or from honest errors on the part of staff members, the human aspect is perhaps the most vulnerable aspect of EDP systems.

E. Common types of computer crime

61. All stages of computer operations are susceptible to criminal activity, either as the target of the crime or the instrument of the crime or both. Input operations, data processing, output operations and communications have all been utilized for illicit purposes. The more common types of computer-related crime are categorized next.

1. Fraud by computer manipulation

62. Intangible assets represented in data format, such as money on deposit or hours of work, are the most common targets of computer-related fraud. Modern business is quickly replacing cash with deposits transacted on computer systems, creating an enormous potential for computer abuse. Credit card information, as well as personal and financial information on credit-card clients, have been frequently targeted by the organized criminal community. The sale of this information to counterfeiters of credit cards and travel documents has proven to be extremely lucrative. Assets represented in data format often have a considerably higher value than traditionally targeted economic assets, resulting in potentially greater economic loss. In addition, improved remote access to databases allows the criminal the opportunity to commit various types of fraud without ever physically entering the premises of the victim.

63. Computer fraud by input manipulation is the most common computer crime, as it is easily perpetrated and difficult to detect. Often referred to as "data diddling", it does not require any sophisticated computer knowledge and can be committed by anyone having access to normal data-processing functions at the input stage.

64. Program manipulation, which is very difficult to discover and is frequently not recognized, requires the perpetrator to have computer-specific knowledge. It involves changing existing programs in the computer system or inserting new programs or routines. A common method used by persons with specialized knowledge of computer programming is the trojan horse, whereby computer instructions are covertly placed in a computer program so that it will perform an unauthorized function concurrent with its normal function. A trojan horse can be programmed to self-destruct, leaving no evidence of its existence except the damage that it caused. 13 Remote access capabilities today also allow the criminal to easily run modified routines concurrently with legitimate programs.

65. Output manipulation is effected by targeting the output of the computer system. The obvious example is cash dispenser fraud, achieved by falsifying instructions to the computer in the input stage. Traditionally, such fraud involved the use of stolen bank cards. However, specialized computer hardware and software is now being widely used to encode falsified electronic information on the magnetic strips of bank cards and credit cards.

66. There is a particular species of fraud conducted by computer manipulation that takes advantage of the automatic repetitions of computer processes. Such manipulation is characteristic of the specialized "salami technique", whereby nearly unnoticeable, "thin slices" of financial transactions are repeatedly removed and transferred to another account. 10

2. Computer forgery

67. Where data are altered in respect of documents stored in computerized form, the crime is forgery. In this and the above examples, computer systems are the target of criminal activity. Computers, however, can also be used as instruments with which to commit forgery. The created a new library of tools with which to forge the documents used in commerce. A new generation of fraudulent alteration or counterfeiting emerged when computerized colour laser copiers became available. 14 These copiers are capable of high-resolution copying, the modification of documents and even the creation of false documents without benefit of an original, and they produce documents whose quality is indistinguishable from that of authentic documents except by an expert.

3. Damage to or modifications of computer data or programs

68. This category of criminal activity involves either direct or covert unauthorized access to a computer system by the introduction of new programs known as viruses, "worms" or logic bombs. The unauthorized modification, suppression or erasure of computer data or functions with the internet to hinder normal functioning of the system is clearly criminal activity and is commonly referred to as computer sabotage. Computer sabotage can be the vehicle for gaining economic advantage over a competitor, for promoting the illegal activities of ideologically motivated terrorists or for stealing data or programs (also referred to as "bitnapping") for extortion purposes. In one reported incident at London, Ontario, in 1987, a former employee of a company sought unsuccessfully to sabotage the computer system of the company by inserting a program into the system that would have wiped it out completely.

69. A virus is a series of program codes that has the ability to attach itself to legitimate programs and propagate itself to other computer programs. A virus can be introduced to a system by a legitimate piece of software that has been infected, as well as by the trojan horse method discussed above.

70. The potential purposes of viruses are many, ranging from the display of harmless messages on several computer terminals to the irreversible destruction of all data on a computer system. In 1990, Europe first experienced a computer virus, used to commit extortion in the medical research community. The virus threatened to destroy increasing amounts of data if no ransom was paid for the "cure". A significant amount of valuable medical research data was lost as a result.

71. A worm is similarly constructed to infiltrate legitimate data-processing programs and to alter or destroy the data, but it differs from a virus in that it does not have the ability to replicate itself. In a medical analogy, the worm can be compared to a benign tumor, the virus to a malignant one. However, the consequences of a worm attack can be just as serious as those of a virus attack: for example, a bank computer can be instructed, by a worm program that subsequently destroys itself, to continually transfer money to an illicit account.

72. A logic bomb, also known as a "time bomb", is another technique by which computer sabotage can be perpetrated. The creation of logic bombs requires some specialized knowledge, as it involves programming the destruction or modification of data at a specific time in the future. Unlike viruses or worms, however, logic bombs are very difficult to detect before they blow up; thus, of all these computer crime schemes, they have the greatest potential for damage. Detonation can be timed to cause maximum damage and to take place long after the departure of the perpetrator. The logic bomb may also be used as a tool of extortion, with a ransom being demanded in exchange for disclosure of the location of the bomb.

73. Irrespective of motive, the fact remains that the use of viruses, worms and logic bombs constitutes unauthorized modification of legitimate computer data or programs and thus fall under the rubric computer sabotage, although the motive of the sabotage may be circumstantial to the alteration of the data.

4. Unauthorized access to computer systems and service

74. The desire to gain unauthorized access to computer systems can be prompted by several motives, from simple curiosity, as exemplified by many hackers, to computer sabotage or espionage. Intentional and unjustified access by a person not authorized by the owners or operators of a system may often constitute criminal behavior. Unauthorized access creates the opportunity to cause additional unintended damage to data, system crashes or impediments to legitimate system users by negligence.

75. Access is often accomplished from a remote location along a telecommunication network, by one of several means. The perpetrator may be able to take advantage of lax security measures to gain access or may find loopholes in existing security measures or system procedures. Frequently, hackers impersonate legitimate system users; this is especially common in systems where users can employ common passwords or maintenance passwords found in the system itself.

76. Password protection is often mischaracterized as a protective device against unauthorized access. However, the modern hacker can easily circumvent this protection using one of three common methods. If a hacker is able to discover a password allowing access, then a trojan horse program can be placed to capture the other passwords of legitimate users. This type of program can

operate concurrently with the normal security function and is difficult to detect. The hacker can later retrieve the program containing the stolen passwords by remote access.

77. Password protection can also be bypassed successfully by utilizing password cracking routines. Most modern software effects password security by a process that converts a user's selected password into a mathematical series, a process known as encryption. Encryption disguises the actual password, which is then almost impossible to decrypt. Furthermore, legitimate security software has been developed that allows access to data only after it checks encrypted passwords against a dictionary of common passwords so as to alert system administrators of potential weakness in security. However, this same security process can be imitated for illegitimate purposes. Known as a "cracker" program when used for illegitimate purposes, these tools encrypt some or all of the data of the system. This creates a dictionary of data to compare with cracker software, for the purpose of identifying common passwords and gaining access to the system. A variety of these system-specific encryption routines can be obtained from hacker bulletin boards around the world and are regularly updated by the criminal community as security technology develops.

78. The third method commonly used to access a system is the "trapdoor" method, whereby unauthorized access is achieved through access points, or trapdoors, created for legitimate purposes, such as maintenance of the system.

79. The international criminal hacker community uses electronic bulletin boards to communicate system infiltration incidents and methods. In one case, details of a Canadian attempt to access a system were found on suspects in an unrelated matter in England; they had removed the material from a bulletin board in Germany. This sharing of information can facilitate multiple unauthorized infiltrations of a system from around the globe, resulting in staggering telecommunication charges to the victim.

80. With the development of modern telecommunications system, a new field for unauthorized infiltration was created. Personal telecommunications have been expanded with the advent of portable, cellular telecommunication devices. The criminal community has responded to these advances by duplicating the microchip technology.

81. Modern telecommunications systems are equally vulnerable to criminal activity. Office automation systems such as voice mail boxes and private business exchanges are, in effect, computer systems, designed for the convenience of users. However, convenience features such as remote access and maintenance capabilities, call-forwarding and voice-messaging are easily infiltrated by computer criminals.

82. Modern telecommunications systems, like other computer systems, are also susceptible to abuse by remote access. The integration of telecommunications systems means that once one system is accessed, a computer operator with sufficient skill could infiltrate the entire

telecommunications network of a city. The usual motive for telecommunications crime is to obtain free telecommunications services. However, more innovative telecommunications fraud has also been uncovered, and telecommunications systems have been used to disguise other forms of criminal activity.

5. Unauthorized reproduction of legally protected computer programs

83. The unauthorized reproduction of computer programs can mean a substantial economic loss to the legitimate owners. Several jurisdictions have dictated that this type of activity should be the subject of criminal sanction. The problem has reached transnational dimensions with the trafficking of these unauthorized reproductions over modern telecommunication networks.

II. SUBSTANTIVE CRIMINAL LAW PROTECTING THE HOLDER OF DATA AND INFORMATION

A. Background

84. The criminal codes of all countries have, up to the present, predominantly protected tangible and visible objects. Although protection for information and other intangible things or values existed before the middle of the twentieth century, it did not play an important role until very recently. The last few decades have seen significant changes: the development from industrial to post-industrial society, the increasing value of information in economics, culture and politics, and the growing importance of computer technology have led to legal challenges and new legal responses to information law. In the 1970s, the resulting change of paradigm, from corporeal to incorporeal objects, began to touch substantive criminal law, in several waves of computer crime legislation.

85. A new doctrine of criminal information is emerging in the area of al legal science, founded on the still-developing concepts of information law and the law of information technology. In accordance with modern cybernetics and informatics, information law now recognizes information as a third fundamental factor in addition to matter and energy. Based on empirical analysis, this concept evaluates information both as a new economic, cultural and political asset and as being specifically vulnerable to unique forms of crime.

86. It is obvious in the new approach that the legal evaluation of corporal objects differs considerably from the evaluation of incorporeal (information) objects. First, there is an important conceptual distinction between information and data that is both technologically and legally relevant. Information is a process or relationship that occurs between a person's mind and a stimulus. Data, whether in corporeal or incorporeal (e.g. electromagnetic impulse) form, constitute a stimulus. Data are merely a representation of information or of some concept. Information is the

interpretation that an observer applies to the data. Different information may be received from the same data, depending on their interpretation. Thus, when data are destroyed or appropriated, it is the representation that is destroyed or appropriated and not the actual information, idea or knowledge. The latter may still subsist in a person's mind or in another copy of the data.

87. The second difference concerns the protection of the proprietor or holder of corporeal and incorporeal objects. Whereas corporeal objects are more exclusively attributed good that flows freely in a free society. It is not itself subject, therefore, to exclusive protection in the same way as tangible property. A third difference between the legal regimes of tangibles and intangibles is that, in protecting information, not only must one consider the economic interests of its proprietor or holder, but one must also preserve the interests of those persons concerned with the contents of the information. This aspect results in new issues of privacy protection, which is dealt with in chapter III.

88. Paragraphs 89-115 investigate how far the various national systems protect the holder of information and paragraphs 116-126 examine activities undertaken in this field of law on the international level.

B. The development of national law

89. Two primary issues are raised by the use of legislation to protect the holder or processor of data or information. First, to what extent is the criminal law an adequate appropriate mechanism for guaranteeing the integrity and correctness of data or information? Secondly, when or how should the interests of proprietors or holders in the exclusive use or secrecy of data or information be protected?

1. The integrity and correctness of data

The integrity of data

90. Until the 1980s, in most legal systems the integrity of computer-stored data was covered by general provisions regarding damage to property, vandalism or mischief. However, these provisions were developed to protect tangible objects; thus their application in the information sphere posed new questions. In a few criminal codes the mere erasure of data without damaging the physical medium does not fall under the traditional provisions regarding damage to property, since electrical impulses are not considered to be corporeal property and interference with the use of physical medium is not considered to be destruction. However, the prevailing opinion in most countries considers the deliberate damage or destruction of data on tapes or disks to be equivalent to damage to, or interference with the use of, property (i.e. vandalism) de lege data, since the use of the tape or disk has been affected.

91. To clarify the situation, new legislation has been enacted in many countries. Some countries amended the traditional statues on mischief, vandalism or damage to tangible property; others created specific provisions. The legislation of a few countries covers all kind of documents, not only computer-stored data. In the United States, a number of state laws contain more specific sanctions for the insertion or intrusion of a computer virus, and on the federal level, a provision sanctions the reckless causing of damage when a federal computer system is intentionally accessed without authorization. Some legal systems also include specific qualifications for computer sabotage that leads to the obstruction of business or of national security.

The correctness of data

92. Owing to its fragmentary character, criminal law is too blunt an instrument to guarantee the general correctness of data, especially its informational content. Only in specific cases, such as balance sheet items, medical reports or other specific documents, can it attempt to guarantee the preservation of faultless data.

93. Some of the most important criminal law provisions covering the integrity, as well as he correctness, of specific data are provisions on forgery, which guarantee the authenticity of a document for the statement that it contains. In some countries, the provisions on forgery require visual readability of statements embodied in a document and, for this reason, do not cover electronically stored data. With the intention of giving electronically based documents the same legal protection as paper-based declarations, some enacted or proposed new statues on forgery that relinquish visual perceptibility. De lege lata, courts in other countries came to the same result.

False data as a means to attack other legally protected interests

94. Traditionally, the involvement of computer data (e.g. in the case of murder committed by the manipulation of a computerized hospital supervision system) does not create specific legal complications. The respective legal provisions are formulated in terms of result, and it is completely irrelevant if the result is achieved with the involvement of a computer.

95. In the area of financial manipulations the situation is different. In many legal systems the statutory definitions of theft, larceny and embezzlement require that the offender take an "item of another person's property". In such systems, the provisions are not applicable if the perpetrator appropriates deposit money. In many countries, these provisions also cause difficulties in regard to the manipulation of financial transactions through automated cash dispensers. The statutory provisions on fraud in some legal systems demand the deception of a person. They cannot be used when a computer is deceived. Statutory definitions of breach of trust or abus de confiance, which exist in several countries, sometimes apply only to offenders in high positions and not to punchers, operators or programmers; some provisions also have restrictions on which objects may be

protected. Consequently, many legal systems have looked for solution de lege data without overstretching the wording of existing provisions, and new laws on computer fraud have been enacted in many countries. Such clarifications or amendments should be considered, if necessary.

2. The exclusive use of data or information

96. The exclusive use of information by its holder is protected by three legal instruments: (a) new, computer-specific statutes concerning illegal access to or use of computer systems; (b) the general rules of intellectual property law, especially copyright law; and (c) the general rules of trade secret law, especially the provisions on economic espionage.

Special statutes protecting exclusive access to and use of computer systems

97. In many countries, since the 1980s, the protection of computer data by the general provisions of trade secret law and intellectual property law has not been considered to be sufficient. In response to the new cases of hacking, many States developed new statutes protecting a "formal sphere of secrecy or privacy" for computer data by criminalizing illegal access to or use of another person's computer, thereby also protecting the computer data contained therein. This new legislation became necessary because, in most countries, protection of this "formal sphere or privacy" against illegal access to computer-stored data and computer communication could not be guaranteed by traditional criminal provisions.

98. As far as wire-tapping and the interception of data communications are concerned, the traditional wire-tap statutes of most legal systems refer only to the interception of communications. Therefore, legislative proposals that cover wire-tapping and other forms of electronic surveillance or the interception of computer system functions or communications have been put forth in many countries. When enacting legislation in this area, it is important that the new law should address interception in all of its possible forms, whether of communications to, from or within a computer system, or of inadvertent or advertent emissions of radiation.

99. Similarly, traditional provisions on trespassing and forgery often cannot be used. In all countries, the applicability of traditional penal provisions to unauthorized access to data-processing and storage systems is generally difficult. Therefore, new legislative provisions concerning such access have been enacted in many countries. These provisions demonstrate various approaches. Some criminalize "mere" access to EDP systems; other punish access only in cases where the accessed system is protected by security measures or where the perpetrator has harmful intentions or where data obtained, modified or damaged. Some countries combine several of these approaches in a single provision covering both "mere" access (in the form of a basic hacking offence) and qualified forms of access (in the form of a more serious ulterior offence with more severe sanctions).

100. One problem concerns the circumstances under which an initially authorized access may become unauthorized or may otherwise turn into a criminal action. In most countries, the new provisions deal only with the initial unauthorized access, thus criminalizing only the acts of outsiders; other countries also proscribe unauthorized use of or presence in systems, thus also criminalizing use or "time theft" by both outsiders and employees. A special solution to protect employees can be found in the California state law, which does not apply to employees if their use is within the scope of their employment or, in the case of uses outside the scope of employment, the use does not result in any injury or the value of the used services does not exceed $100.

101. The discussion about initially authorized access demonstrates that illegal access to computer systems is closely connected to, and partly overlaps with, the criminalization of unauthorized use of computers (i.e. both use without authority and time theft), although up to the present this close relationship has not yet been generally realized by all countries. De lege ferenda in most civil law countries the problem of illegal use of computers is reduced to the illegal use of computer hardware and discussed within the context of furtum usus of corporeal property. In this context many civil law countries reject a general criminalization of furtum usus of tangibles (with some exceptions, such as for moto vehicle joyriding) and consequently do not incorporate a provision against the illegal use of computers or time theft in their new computer crime laws. However, there are (mainly Nordic) countries that have a legal tradition of criminalizing the unauthorized use of corporeal property, so that the new reform proposals of these countries also criminalize the unauthorized use of computer systems. Many common law countries or parts thereof (e.g. Canada and many States of the United States) have recognized the relationship between access and use, and in statutory definitions subsume either "access" or "use" into the other concept, thereby creating a single legal concept that address both situations for the purposes of the new penal provisions. Since the unauthorized use of computer systems generally presupposes unauthorized access to that system, an adequate access or use provision could at the same time cover the other delict as well.

102. A further distinction that is sometimes recognized is one between (a) the unauthorized obtaining of computer services or time that is ordinarily provided for a fee and (b) the unauthorized use of computer systems in general. The delict in respect of the former is the unauthorized obtaining of computer services without payment of the requisite fee, thereby causing the owner of the system to suffer a financial loss. In some countries, such abuse is covered by general theft of service laws. The statutes of other countries, however, are limited to the unlawful use, waste or withdrawal of electricity. General theft and fraud statutes may be applicable in some countries, while in other countries specific provisions have had to be enacted to deal with this type of theft of service.

103. The delict in respect of the mere unauthorized use of the computer is the violation of the exclusive use rights of the owner. Addressing this problem raises all of the issues previously discussed in relation to the issues of unauthorized access and unauthorized use.

Intellectual property law

104. The concept of intellectual property law has been predicated both on the recognition of natural rights in intellectual property and on the policy of encouraging the creation of works by granting a certain premium to the creators. In the field of information technology, this concept is especially important for the protection of computer programs and semiconductor topographies.

Computer programs

105. Depending on the circumstances, trade secret protection may apply to computer-stored date, including computer programs themselves. However, since these legal devices are restricted to secret programs, special relationships and/or specific acts of accessing information, they are not sufficient to guarantee secure trade with respect to computer programs in general. The price discrepancy between expensive originals of computer programs and cheaper unauthorized reproductions is so vast that there is a demand in all countries for the more comprehensive regulation of these activities. Protective systems could be expanded to include non-secret programs and could be applicable to third parties.

106. In recent years, many countries have debated the scope of copyright law, given that patent law can protect only a small number of programs, such as those that include a technical invention. With the aim of avoiding legal uncertainty, many countries have expressly provided copyright protection for computer programs by way of legislative amendments. This fundamental recognition of the need to copyright computer programs can, however, only be regarded as a first step. The creation of effective copyright protection for computer programs raises explicitly the question of the appropriate scope of copyright protection, as well as some additional problems. Until now, these questions have been solved in disparate and often unsatisfactory ways in many countries.

107. The role op penal copyright protection has also been evaluated differently in various countries. In the past, copyright law in common law systems rarely, if ever, resorted to penal sanctions; civil law systems, in contrast, have traditionally punished infringements of copyright by lenient criminal sanctions. The increase in audio- and videotape piracy in recent years, however, has necessitated more stringent criminal sanctions in both systems; thus the distinction between civil and common law systems has been effectively removed.

108. Although some of the new laws are still confined to phonographic products, many are of a more general nature. Reform proposals providing more severe criminal sanctions for copyright infringements have been enacted in many countries. These efforts to achieve more effective

copyright protection are justified, since attacks against intellectual property deserve a criminal law response as much as do the more conventional attacks on corporeal property. The reluctance to criminalize copyright infringements, still evident in some countries, could be counteracted by adequate civil law provisions. The law can be structured to differentiate between less objectionable activities, such as private back-up copying, and more clearly criminal behaviour, which either causes economic damage or is regularly committed for gain.

Semiconductor products

109. Computer programs are not the only new economic values created by modern computer technology. As is evidenced by the miniaturization of computers and the development of fifth-generation computers, the technique of integrated circuits is becoming more and more sophisticated. The possibilities of copying the topography of semiconductor products give rise to demand for an effective protection of such products in order to stop unauthorized reproduction.

110. In most countries, it remains unclear to what extent the topography of semiconductor products is protected against reproductions by patent law, copyright law, registered designs, trade secret law and competition law. In the United States, special protection for computer chips was provided by the Semiconductor Chip Protection Act of 1984. 8 Many states followed this sui generis approach by enacting similar legislation.

111. However, criminal sanctions provided under this type of legislation differ from country to country. In contrast to the laws of Canada, Italy and the United States, the new Finnish, German, Japanese, Netherlands and Swedish laws include criminal sanctions, which among other things punish the infringement of a circuit layout right. Civil and penal sanctions for egregious infringements of circuit layout rights require serious consideration.

The protection of trade secrets

112. When information is acquired by stealing a corporeal carrier of information, such as a printout, tape or disk, the traditional penal provisions on theft, larceny or embezzlement are not problematic in application. However, the ability of data-processing and communication systems to copy data quickly, inconspicuously and, often, via telecommunication facilities has meant that most of these acts of traditional information carrier theft are replaced with acts of actual information acquisition. Therefore, the question arises, To what extent can or should the pure acquisition of incorporeal information be covered by these provisions? Most countries are reluctant to apply traditional provisions on theft and embezzlement to the unauthorized appropriation of secret information, because these provisions generally require that corporeal property be taken away with the intention of depriving the victim of use or control The acquisition of information (e.g. by

copying it or taking away a copy) does not necessarily deprive the original holder of the information. The data may still exist intact, or other copies my exist.

113. Additionally, in many countries the traditional laws of theft also require that the thing that is taken constitute property. However, legislators and the judiciary in many of these countries are reluctant to ascribe a property status to information, even confidential information. The issue of misappropriation of information raises a number of broader legal, social and economic issues. The conflict of interest between the free flow of information and the right to confidentiality must be taken into account, as must be the economic interests in certain kinds of information. Just as in the area of intellectual property law solutions in this area must also provide for an appropriate degree of flexibility to balance these competing interests. Traditional property law, with its emphasis on exclusivity to one owner, does not adequately account for the dynamics of information in an information society. Rather than relying on traditional theft provisions, special laws may need to be enacted. 2

114. As a result of problems in applying the general property law to cover trade secrets, in many countries the misappropriation of someone else's secret information is covered by special provisions on trade secrets law. These provisions protect trade secrets by prohibiting only certain condemnable acts of obtaining information, either by provisions of the penal code or by penal or civil provisions of statutes against unfair competition. These laws generally attempt to balance the competing interests.

115. Generally speaking, it can be said that criminal trade secret law and civil unfair competition law are less developed in common law countries, at least statutorily, and in Asian countries than in continental Europe. As far as future policy-making is concerned, the international trend towards trade secret protection should be encouraged. To achieve an international consensus, all legal systems could, either in their penal codes or in statutes against unfair competition, establish penal trade secret protection reinforced by adequate civil provisions on unfair competition.

C. The international harmonization of criminal law

116. In order to effectively address computer crime, concerted international cooperation is required. Such can only occur, however, if there is a common framework for understanding what the problem is and what solutions are being considered. To date, international harmonization of the legal categories and definition of computer crime has been proposed by the United Nations, by OECD and by the Council of Europe.

2. First initiatives of OECD

117. The first comprehensive international effort dealing with the criminal law problems of computer crime was initiated by OECD. From 1983 to 1985, an ad hoc committee of OECD

discussed the possibilities of an international harmonization of criminal laws in order to fight computer-related economic crime. In September 1985, the committee recommended that member countries consider the extent to which knowingly committed acts in the field of computer-related abuse should be criminalized and covered by national penal legislation.

118. In 1986, based on a comparative analysis of substantive law, OECD suggested that the following list of acts could constitute a common denominator for the different approaches being taken by member countries:

1. "The input, alteration, erasure and/or suppression of computer data and/or computer programs made willfully with the intent to commit an illegal transfer of funds or of another thing of value;

2. The input, alteration, erasure and/or suppression of computer data and/or computer programs made willfully with the intent to commit a forgery;

3. The input, alteration, erasure and/or suppression of computer data and/or computer programs, or other interference with computer systems, made willfully with the intent to hinder the functioning of a computer and/or telecommunication system;

4. The infringement of the exclusive right of the owner of a protected computer program with the intent to exploit commercially the program and put in on the market;

5. The access to or the interception of a computer and/or telecommunication system made knowingly and without the authorization of the person responsible for the system, either (i) by infringement of security measures or (ii) for other dishonest or harmful intentions". 9

2. The guidelines of the Council of Europe

119. From 1985 to 1989, the Select Committee of Experts on Computer-Related Crime of the Council of Europe discussed the legal problems of computer crime. The Select Committee and the European Committee on Crime Problems prepared Recommendation No. R(89)9, which was adopted by the Council on 13 September 1989. 10

120. This document "recommends the Governments of Member States to take into account, when reviewing their legislation or initiating new legislation, the report on computer-related crime... and in particular the guidelines for the national legislatures". The guidelines for national legislatures include a minimum list, which reflects the general consensus of the Committee regarding certain computer-related abuses that should be dealt with by criminal law, as well as an optional list, which describes acts that have already been penalized in some States, but on which an international consensus for criminalization could not be reached.

121. The minimum list of offences for which uniform criminal policy on legislation concerning computer-related crime had been achieved enumerates the following offences:

1. Computer fraud. The input, alteration, erasure or suppression of computer data or computer programs, or other interference with the course of data processing that influences the result of data

processing, thereby causing economic or possessory loss of property of another person with the intent of procuring an unlawful economic gain for himself or for another person;

2. Computer forgery. The input, alteration erasure or suppression of computer data or computer programs, or other interference with the course of data processing in a manner or under such conditions, as prescribed by national law, that it would constitute the offence of forgery if it had been committed with respect to a traditional object of such an offence;

3. Damage to computer data or computer programs. The erasure, damaging, deterioration or suppression of computer data or computer programs without right;

4. Computer sabotage. The input, alteration erasure or suppression of computer data or computer programs, or other interference with computer systems, with the intent to hinder the functioning of a computer or a telecommunications system;

5. Unauthorized access. The access without right to a computer system or network by infringing security measures;

6. Unauthorized interception. The interception, made without right and by technical means, of communications to, from and within a computer system or network;

7. Unauthorized reproduction of a protected computer program. The reproduction, distribution or communication to the public without right of a computer program which is protected by law;

8. Unauthorized reproduction of a topography. The reproduction without right of a topography protected by law, of a semiconductor product, or the commercial exploitation or the importation for that purpose, done without right, of a topography or of a semiconductor product manufactured by using the topography".

122. The optional list contains the following conduct:

1. Alteration of computer data or computer programs. The alteration of computer data or computer programs without right;

2. Computer espionage. The acquisition by improper means or the disclosure, transfer or use of a trade or commercial secret without right or any other legal justification, with intent either to cause economic loss to the person entitled to the secret or to obtain an unlawful economic advantage for oneself or a third person;

3. Unauthorized use of a computer. The use of a computer system or network without right, that either: (i) is made with the acceptance of significant risk of loss being caused to the person entitled to use the system or harm to the system or its functioning, or (ii) is made with the intent to cause loss to the person entitled to use the system or harm to the system or its functioning, or (iii) causes loss to the person entitled to use the system or harm to the system or its functioning;

4. Unauthorized use of a protected computer program. The use without right of a computer program which is protected by law and which has been reproduced without right, with the intent,

either to procure and unlawful economic gain for himself or for another person or to cause harm to the holder of the right".

3. Resolution of the General Assembly

123. In 1990, the legal aspects of computer crime were also discussed by the United Nations, particularly at the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, at Havana, as well as at the accompanying symposium on computer crime organized by the Foundation for Responsible Computing. The Eighth United Nations Congress adopted a resolution on computer-related crime, a portion of which was quoted in paragraph 18. 124. In its resolution 45/121, the General Assembly welcomed the instruments and resolutions adopted by the Eighth Congress and invited Governments to be guided by them in the formulation of appropriate legislation and policy directives in accordance with the economic, social, legal, cultural and political circumstances of each country.

4. The proposed resolution of the Association Internationale de Droit Pénal

125. The draft resolution of the AIDP Colloquium, held at Würzburg, 5-8 October 1992, contains a number of recommendations, including the following:

"3. To the extent that traditional criminal law is not sufficient, modification of existing, or the creation of new offences should be supported of other measures are not sufficient (principle of subsidiarity).

4. In the enactment of amendments and new provisions, emphasis should be put on precision and clarity. In areas where criminal law is only an annex to other areas of law (as in the area of copyright law), this requirement should also be applied to the substantive material or that other law.

5. In order to avoid overcriminalization, regard should be given to the scope to which criminal law extends in related areas. Extensions that range beyond these limits require careful examination and justification. In this respect, one important criterion in defining or restricting criminal liability is that offences in this area be limited primarily to intentional acts.

...

7. Having regard to the advances in information technology, the increase in related crime since the adoption of the 1989 recommendation of the Council of Europe, the significant value of intangibles in the information age, the desirability to promote further research and technological development and the high potential for harm, it is recommended that States should also consider, in accord with their legal traditions and culture and with reference to the applicability of their existing laws, punishing as crimes the conduct described in the ´optional list´, especially the alteration of computer data and computer espionage.

8. Furthermore, it is suggested that some of the definitions in the Council of Europe lists - such as the offence of unauthorized access - may need further clarification and refinement in the light of advances in information technology and changing perceptions of criminality. For the same reasons, other types of abuses that are not included expressly in the lists, such as trafficking in wrongfully obtained computer passwords and other information about means of obtaining unauthorized access to computer systems, and the distribution or viruses or similar programs, should also be considered as candidates for criminalization, in accord with national legal traditions and culture and with reference to the applicability of existing laws. In light of the high potential damage that can be caused by viruses, worms and other such programs that are meant, or are likely, to propagate into and damage, or otherwise interfere with, data, programs or the functioning of computer systems, it is recommended that more scientific discussion and research be devoted to this area. Special attention should be given to the use of criminal norms that penalize recklessness or the creation of dangerous risks, and to practical problems of enforcement. Consideration might also be given as to whether the resulting crime should be regarded as a form of sabotage offence.

9. In regard to the preceding recommendations, it is recognized that different legal cultures and traditions may resolve some of these issues in different ways while, nevertheless, still penalizing the essence of the particular abuse. States should be conscious of alternative approaches in other legal systems". 13

126. The draft resolution acknowledges the work of OECD and the Council of Europe and welcomes the guidelines adopted by the latter, which create a minimum list of criminal acts as well as an optional list of acts that should be penalized by national law. The draft resolution is expected to be adopted, with or without revisions, at a conference of AIDP to be held at Rio de Janeiro in 1994.

III. SUBSTANTIVE CRIMINAL LAW PROTECTING PRIVACY

A. Background

127. Unlike the legal rules concerning corporeal objects, information law does not only consider the economic interests of the proprietor or holder but also takes into account the interests of persons concerned with the content of information. Before the invention of computers, the legal protection of persons in regard to the content of information was limited. Few provisions existed in the criminal law other than those in relation to libel. Since the 1970s, however, new technologies have expanded the possibilities of collecting, storing, accessing, comparing, selecting, linking and transmitting data, thereby causing new threats to privacy. This has prompted many countries to enact new elements of administrative, civil and penal regulations, as discussed in paragraphs 128-

132. Various international measures, outlined in paragraphs 133-145, support this evolution by developing a common approach to privacy protection.

B. The development of national law

128. The penal provisions in privacy laws largely refer to the corresponding administrative provisions. Accordingly, first the administrative provisions are surveyed briefly and then the related questions of criminal law are dealt with.

1. Differing concepts of privacy laws

129. Special legislation against infringements of privacy have been past in most western legal systems. Moreover, the courts in most countries have also developed a civil action protecting privacy interests. An analysis of national laws demonstrates that various international actions have led to a considerable degree of uniformity among the general administrative and civil law regulations of national privacy laws. Most national privacy statutes include, for example, provisions addressing the limitation of data collection or the individual's right of access to his or her personal data. In spite of this tendency, considerable differences in general administrative and civil regulations remain. These differences concern the legislative rationale, the scope of application (especially with regard to legal persons and manually recorded data), the procedural requirements for commencing the processing of personal data and the substantive requirements for processing such data, as well as the respective control institutions.

130. The differences among the general administrative regulations are not only relevant for administrative law but to a significant extent also determine the existence of differences between criminal law provisions, which largely refer to these regulations. For example, one difference among criminal offences in various national privacy laws is found in the prohibition of the use of various types of data.

2. Differing acts covered by criminal law

131. The main difference among the penal privacy offences, however, derive not from their general scope of application but from the different illegal acts that they cover . These differences in penal coverage are mainly caused by a divergent evaluation of the criminal character of privacy infringements and the role that penal law should play in this field. In some countries, especially Canada, Japan and the United States , criminal law is not widely used for privacy protection. In other countries, the criminal law includes comprehensive lists of severe criminal offences that refer to many of the actions regulated by administrative law. Some legislation even punishes negligent acts. In Finland, the Committee on Informational Crimes and, in France, the Commission for the

Revision of the Penal Code intend to stress the importance of criminal sanctions of privacy legislations by implementing the most important infringements in their general penal codes.

132. The most important differences among the crimes against privacy in the various data protection laws emerge when the penal provisions are analysed in detail. Such a comparative analysis should differentiate four main categories of criminal privacy infringements, which are to be found particularly in European privacy laws:

1. The first main group of crimes against of privacy relates to infringements of substantive privacy rights and includes such acts as illegal disclosure, dissemination, obtaining of and/or access to data; unlawful use of data; illegal entering, modification and/or falsification of data with an intent to cause damage; collection, recording and/or storage of data, which is illegal for reasons of substantive policy; or storage of incorrect data. Detailed analysis of the respective criminal provisions indicates that these substantive infringements of privacy rights differ with regard not only to the data covered but also to the types of acts punished. They differ further according to the extent to which the described acts are permitted by law. Since the penal provisions either refer to the respective general provisions of the civil privacy laws or justify exceptions permitting the use of personal data by reference to general clauses, which are similar to those of the administrative provisions, all anomalies, inaccuracies and uncertainties in the field of administrative law can also be found within the corresponding penal provisions;

2. As a result of the uncertainties in the substantive provisions, many legal systems rely to a great extent on a second, and additional, group of offences and are directed towards enforcing various formal legal requirements or orders of supervisory agencies. These offences, included in most privacy laws, generally contain more precise descriptions of the prohibited conduct than do the substantive offences. However, these formal provisions also vary considerably among the various national laws. The main type of formal infraction covered in many states by penal law concerns infringement of the legal requirements for commencing the processing of personal data (e.g. registration, notification, application for registration, declaration or licensing). Additional, and considerably varying, offences that can be found in much of the European privacy legislation are infringement of certain regulations, prohibitions or decisions of the regulatory authorities; refusal to give information or release of false information to the regulatory authorities; refusal to grant access to property and refusal to permit inspections by regulatory authorities; obstruction of the execution of a warrant; failure to appoint a controller of data protection for a company; and failure to record the grounds or means for the dissemination of personal data;

3. A third type of criminal privacy infringement is infringement of access laws, e.g. the individual's rights to access information (freedom of information). With respect to a party's right of access, in many European countries it is an offence to give false information or not to inform the registered party or not to reply to a request;

4. Some countries go further and punish neglect of security measures with an administrative fine or even with a criminal sanction. This constitutes a fourth type of offence.

C. International harmonization

1. Harmonization of underlying administrative and civil law

133. In the field of administrative and civil privacy legislation, various international organizations have developed a common approach to privacy protection in order to prevent the proliferation of different concepts and national regulations that would impede the transborder flow of data. The main work in this field has so far been accomplished by OECD, the Council of Europe and the European Union.

The OECD guidelines

134. In 1977, OECD began to elaborate guidelines governing the protection of privacy and transborder flows of personal data. These guidelines were adopted by the Council of OECD in 1980 as a recommendation to the member States. The eight main points of the guidelines concern the principles of limitation on collection; data quality; specification of purpose; limitation of use; security and safeguards; openness; individual participation; and accountability.

Activities of the Council of Europe

135. In 1980, the Committee of Ministers of the Council of Europe, which had been considering privacy concerns since 1968, adopted the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. In contrast to the OECD guidelines, which are voluntary in nature, the Council of Europe Convention is a contractual commitment of the ratifying States and is legally binding. It formulates 10 basic principles representing minimum standards that must be incorporated in the legislation of the contracting States. Although similar to those of OECD, these principles are narrower and more specific.

136. Further initiatives were undertaken by the Committee of Experts on Data Protection of the Council of Europe. Since the opening for signature of the Convention, the Committee has pursued a sectoral approach to data protection issues aimed at elaborating guidelines, in the form of non-binding recommendations, addressed to the Governments of the member States.

Proposals of the European Union

137. The European Union started to harmonize privacy laws in 1976. A decisive breakthrough for European privacy protection was reached in September 1990, when the Commission of the European Communities submitted a draft package containing six proposals in the field of personal

data protection and information security. The package included the draft of a general directive on data protection applicable to all personal data files within the scope of European Union law. Within the context of the IMPACT2 program of the European Union, the Commission intends to elaborate, when necessary, the instruments concerning personal data protection in specific sectors of information services, mailing list services, credit ratings and solvency services.

Activities of the United Nations

138. In 1988, the Subcommission on the Prevention of Discrimination and the Protection of Minorities of the Commission on Human Rights elaborated draft guidelines for the regulation of computerized personal data files (E/CN.4/Sub.2/1988/22, annex I). In its resolution 45/95, the General Assembly adopted a revised version of these guidelines, which contain principles similar to those of the OECD guidelines and the Council of Europe Convention.

2. Harmonization of criminal law

139. In contrast to the progress achieved in administrative and civil privacy law, international harmonization in the field of criminal privacy law has still not really begun. The main initiative is being undertaken by the Council of Europe. The above-mentioned Convention of the Council of Europe contains, in article 10, a provision stating that "each party undertakes to establish appropriate sanctions and remedies for violation of ... the basic principles for data protection". However, this clause allows States to determine the nature of the sanctions and remedies (civil, administrative or criminal), as well as their scope of application.

140. Further studies to harmonize criminal privacy law were undertaken in the course of the work of the Select Committee of Experts on Computer-Related Crime of the Council of Europe, mentioned in paragraphs 119-122. The Committee recommended six basic principles that should be taken into account by member States when enacting legislation in the field of computer-related criminal privacy:

1. "The protection of privacy against offences caused by modern computer technology is of great importance. However, this protection should be based primarily on administrative and civil law regulations. Recourse to criminal law should be made only as a last resort. This means that criminal sanctions should be used only in cases of severe offences in which adequate regulation cannot be achieved by administrative or civil law measures (ultima ratio principle);

2. The respective criminal provisions must describe the forbidden acts precisely and should avoid vague general clauses. A precise description of illegal acts, without however resorting to a casuistic legislation technique, can easily be achieved, for example, for specific sensitive data. In cases in which precise descriptions of illegal acts are not possible, due to the necessity of a difficult balancing of interests (privacy versus freedom of information), criminal law should decline to

incriminate substantive infringements of privacy and adopt a formal approach, based on administrative requirements of notification of potentially harmful data-processing activities. Failure to comply with these notification requirements and to obey regulations of the data protection authorities could then be subject to sanctions. These formal offences are in accordance with the principle of culpability as long as they can be considered bans per se (Gefährdungsdelikte, délits-obstacles), which punish the endangering of privacy rights. In many areas, criminal privacy infringements, therefore, would presuppose both the infringement of formal requirements as well as the endangering of substantive privacy rights (principle of precision in the wording of criminal law);

3. The criminalized acts should be described as clearly as possible by the respective penal law provisions . Therefore, a too-extensive use of the referral technique (that is, the technique pursuant to which activities regulated outside the penal law provisions are criminalized by reference) makes criminal provisions unclear and incomprehensible and should be avoided. If implicit or explicit references of the criminal law are used , the criminal provision itself should at least give an adequate idea of the forbidden acts (clearness principle);

4. Different computer-related infringements of privacy should not be criminalized in one global provision . The principle of culpability requires a differentiation according to the interests affected, the acts committed and the status of the perpetrator, as well as of his intended aims and other mental elements (principle of differentiation);

5. In principle, computer-related infringements of privacy should only be punishable if the perpetrator acts with intent. Criminalization of negligent acts should be an exception requiring a special justification (principle of intent);

6. Minor computer-related offences against privacy should be punished only in accordance with Council of Europe Recommendation No.(87)18 on the simplification of criminal justice, on complaint of the victim or of the Privacy Protection Commissioner or of the Privacy Protection Authority (principle of complaint)".5

141. In future, further harmonization of criminal privacy law might be achieved along the lines outlined in the draft directive of the European Union. Chapter VII, article 23, of that draft directive, which concerns sanctions , demands that each member State provide in its laws the use of "sufficient sanctions" to guarantee the rules based on the directive.

142. The issue of privacy protection was also discussed at the AIDP Colloquium on Computer Crime and Other Crimes against Information Technology (see paragraphs 116-126). The discussion demonstrated significant differences of opinion as to the means by which and the degree to which protection should be afforded by administrative , civil, regulatory and criminal law. The draft resolution of the colloquium recommended, therefore, that "non-penal measures should be given priority, especially where the relations between the parties are governed by contract" and that

criminal provisions "should only be used where civil law or data protection law do not provide adequate legal remedies".

143. The Colloquium noted the basic principles, as advanced by the Council of Europe, that should be taken into account by States when enacting criminal legislation in this field. The draft resolution of the Colloquium proposes further that criminal provisions in the privacy area should in particular:

1. "Be used only in serious cases, especially those involving highly sensitive data or confidential information traditionally protected by law;
2. Be defined clearly and precisely rather than by the use of vague or general clauses (Generalklauseln), especially in relation to substantive privacy law;
3. Differentiate as between varying levels and requirements of culpability;
4. Display caution, in particular, as regarding matters of intent;
5. Permit the prosecutorial authorities to take into account, in respect of some types of offences, the wishes of the victim regarding the institution of prosecution".

144. The draft resolution also noted as follows:

"The significance of protecting privacy interests in the transformed information age should be recognized, but also balanced by the legitimate interests in the free flow and distribution of information within society. These interests include the right of citizens to access, by legal means consistent with international human rights, information about themselves which is held by others".

145. The Colloquium concluded that further study of this issue should be undertaken.

IV. PROCEDURAL LAW

A. Background

146. Computer-specific procedural law problems arise not only in the prosecution of computer-crime cases but also in many other fields of criminal investigation. This is especially illustrated by the prosecution of economic crimes , predominantly in the field of banking, where most of the relevant evidence is stored in automated data-processing systems. In the field of traditional crime, computer-stored evidence is already a significant issue, as is illustrated by cases of drug traffickers conducting their business using personal computers and international telecommunication systems. In future, new optical storage devices based on compact disc technology will further encourage the destruction of originals (if paper originals still exist) after the information has been recorded in automated data-processing systems. Owing to these new technical developments and to the growing use of computers in all areas of economic and social life, courts and prosecution authorities will depend to an increasing extent on evidence stored or processed by modern information technology.

147. The resulting replacement of visible and corporeal objects of proof by invisible and intangible evidence in the field of information technology not only creates practical problems but also opens up new legal issues: the coercive powers of prosecuting authorities, discussed in paragraphs 148-165; specific problems with personal data, discussed in paragraphs 166-170; and the admissibility of computer-generated evidence, discussed in paragraphs 171-175. The relevant problems are dealt with not only at the national level but also by various international organizations, as discussed in paragraphs 176-185.

B. The coercive powers of prosecuting authorities

148. In accordance with the practical requirements of investigations in the field of information technology and based on the various coercive powers existing in most legal systems, an analysis of the coercive powers of prosecuting authorities has to differentiate among search and seizure in automated information systems; duties of active cooperation; and wire-tapping of telecommunication systems and "eavesdropping" of computers.

1. Search and seizure in automated information systems - Problems of traditional law

149. Collecting data stored or processed in computer systems generally first requires entry to and search of the premises in which the computer system is installed (powers of search and entry of premises); it is then necessary that the data can be seized or captured (powers of seizure and retention).

150. With respect to the investigation of computer data permanently stored on a corporeal data carrier, the general limitation of the powers of search and seizure to the search and seizure of (corporeal) objects relevant to the proceedings or to finding the truth does not, in most countries, pose serious problems, since the right to seize and to inspect the corporeal data carrier or, in case of internal memories, the central processing unit also includes the right to inspect the data. In other words, there is no difference whether the data are fixed with ink on paper or by magnetic impulses in electronic data carriers. This conclusion is even more evident for provisions in which the powers of search and/or the powers of seizure are directed towards "anything" that would be admissible as evidence at a trial. The same evaluation also applies mutatis mutandis for powers of confiscation.

151. Application of the traditional powers of search and seizure might, however, cause problems in cases where data are not permanently stored in a corporeal data carrier. In these instances, it is questionable whether pure data or information can be regarded as an object in the sense of criminal procedural law. The same holds true if the legal principle of minimum coercion or of proportionality makes it unlawful to seize comprehensive data carriers, or complete computer installations, in order to gather only a small amount of data. Similarly, search and seizure of comprehensive data carriers could cause serious prejudice to business activities or infringe the

privacy rights of third parties. Uncertainties may also arise in cases in which data carriers (such as core-storage, fixed-disk devices or chips) cannot be taken away to be evaluated on a police computer but must be analysed using the computer system in question. In all these cases one might consider applying the powers of search not only to detect a computer installation and data but also to fix (especially to print) the relevant data on a separate data carrier and then seize this new object, which might be a diskette or a printout.

152. However, such a construction depends on the question of whether and to what degree the powers of search and seizure include the power to use technical equipment and (copyrightable) programs belonging to a witness or to an accused, in order to search and/or fix computer data. Only a few laws state that in the execution of search and seizure all necessary measures may be taken. Consequently, in many legal systems an effective search for pure data or information is not provided for by the law.

153. Special problems also arise with respect to search and seizure in computer networks. Here, it is questionable whether and to what extent the right to search and seize a specific computer installation includes the right to search databases that are accessible by this installation but that are situated in other premises. This question is of great practical importance since perpetrators increasingly store their data in computer systems located elsewhere in order to hinder prosecution. Specific problems of public international law arise with respect to search and seizure of foreign databases via international telecommunication systems. In these international systems, the direct penetration by prosecuting authorities of foreign data banks generally constitutes an infringement of the sovereignty of the State of storage (and often in a punishable offence); however, there might be some specific exceptions that could be developed internationally in which direct access to foreign data banks via telecommunication networks could be permissible and the lengthy procedure of mutual assistance avoided.

154. Problems of interpretation also arise with respect to extra safeguards for specific information. This is not only an issue with respect to the materials of professional legal advisers, doctors, journalists and other people who may , in some legal systems, be exempt from giving evidence. One of the latest disputes in this area is the question of how far the privileges of the press should also be applicable to electronic bulletin boards. Even more intricate questions arise with the application of safeguards and specific provisions to papers , documents and letters, especially in the fields of electronic mail and telecommunication systems. Owing to the rationale of these privileges , they should generally apply equally to paper-based and computer-stored material , especially as between traditional mail and electronic mail.

Law reform

155. In some countries attempts have been made to resolve these uncertainties and loopholes in the field of search and seizure of data and information by legislative amendments. In the United Kingdom, the general power of seizure provided by section 19 of the Police and Criminal Evidence Act of 1984 is directed to "anything which is on the premises" and, under certain conditions, provides the power "to require any information which is contained in a computer" (for the latter duty of active cooperation, see paragraphs 157-162). In Canada, section 14 of the Competition Act and similar provisions in the Environmental Protection Act and the Fisheries Act permit searching for "any data contained in or available to the computer system". Furthermore, section 3(1) of the legislation proposed by the Law Reform Commission of Canada with respect to search and seizure defines objects of seizure as "things, funds, and information" which are reasonably believed to be takings of an offence, evidence of an offence or contraband.

156. Such sui generis provisions for gathering data not only provide legal certainty and a basis for efficient investigations in an EDP environment but, with respect to legal policy, can also be based on the argument that copying data is often a less severe inhibition than the seizure of data carriers. Moreover, sui generis provisions have the advantage of being able to solve specific questions of search and seizure of data, such as compensation of costs for the use of EDP systems, subsequent erasure of copied data that are no longer required for the prosecution, or search and seizure in telecommunication networks.

2. Duties of active cooperation - The practical problems

157. The aforementioned powers of entry, search and seizure, and even a sui generis power of gathering data, do not, in many cases, guarantee a successful investigation, since the traditional authorities often lack the knowledge of computer hardware, operating systems and standard software necessary to access modern data-processing systems. The very complexity of modern information technology creates many problems regarding access to computer systems, which can be solved, but only partially, by better police training. This is mainly the case with respect to specific security software and encryption designed to prevent unauthorized access to information. Serious problems are also caused by the multitude of data stored in computer systems and by the limited time and financial resources available to prosecuting authorities for checking these data. Consequently, the duties of citizens to cooperate with prosecuting agencies become of much greater importance in computerized environments than in non-technical, "visible" areas.

158. The traditional legal systems of most countries include two instruments that might be used to achieve the cooperation necessary for gathering evidence in a computerized environment: the duty to surrender seizable objects of evidence and the duty to testify. In some countries, additional and more extensive provisions or reform proposals have been enacted or suggested.

Duties to surrender seizable objects

159. The duty to surrender seizable objects is often coupled with the powers of search an seizure. In many countries the holder of a seizable object is obliged to deliver it on request to the (judicial) authorities; however, some legal systems do not provide such an obligation, and in some countries the respective court orders are not enforceable. The duty to surrender seizable objects can help the investigating authorities, especially in selecting specific data carriers from among the many tapes and diskettes that are usually stored in a computer centre. However, the obligation to surrender seizable objects does not generally include the duty to print or deliver specific information stored on a data carrier. Consequently, in many countries the powers of seizure and the duties to surrender seizable objects can only support voluntary printing of specific information. Practice with respect to search and seizure in the field of banking shows that banks often voluntarily print out specific data in order to prevent the seizure of large volumes of data carriers. However, the threat of a comprehensive seizure and serious prejudice to business activities cannot be regarded as a satisfactory legal solution for the relevant problems.

Duties to testify

160. In many cases an important duty of active cooperation can be based on the duties to testify, i.e. the duty of (unsuspected) witnesses to "testify", to "tell the truth", to "answer questions" etc. This is especially the case in countries in which the traditional duties to testify contain the more extensive obligation that the witness refresh his or her knowledge of the case, e.g. by examining account books, letters, documents and objects that are available to the said witness without special inconvenience, and to make notes and bring them along to the court. However, in most legal systems the traditional duties to testify cannot be extended to efficient duties of cooperation , especially not to the printing out of specific information. The main reason for this conclusion is the fact that the duty to testify, and consequently the duty of witnesses to refresh their knowledge, refers only to knowledge they already had in mind and not to new information. A different conclusion would also confuse the roles of witnesses and experts. Furthermore, in many countries the witness must testify before a judge, and in some countries before the public prosecutor, but not before police conducting the investigation; in some legal systems, the duties to testify exist only at a later stage of the proceedings and not during the police investigation. Moreover, the requirement that a (written or oral) court summons be given to the witness in due time prior to the proceedings could make such proceedings ineffective.

Law reform

161. To make investigations in computerized environments more efficient, some countries have recently enacted or suggested new compulsory duties to produce specific information. According to the police and Criminal Evidence Act 1984 1of the United Kingdom, the constable "may require any information which is contained in a computer and is accessible from the premises to be produced in a form in which it can be taken away and in which it is visible and legible". In Canada, the Mutual Legal Assistance Act provides for an evidence gathering order addressed to a person "to make a copy of a record or to make a record from data and to bring the copy or record with him". However, with respect to data accessible via international telecommunication networks, these provisions leave open the question whether and to what degree a State, in accordance with international public law, has the right to oblige its citizens to gather evidence in foreign countries. Furthermore, other than in respect of recognized privileges, it is unclear under which conditions citizens have the right to deny cooperation.

162. The question whether or not such duties to produce and hand over computer printouts should be recommended de lege ferenda is difficult to judge and requires a differentiation between the duties of witnesses and the duties of defendants or suspected persons. With respect to (innocent) witnesses, there are good arguments for the introduction of such a duty. However, with respect to the defendant or suspect, there are equally good arguments that a duty of active cooperation should be rejected since this duty could impede the accused's right to remain silent and could infringe upon the privilege against self-incrimination. It is true that the wording of article 14(3)g of the International Covenant on Civil and Political Rights only guarantees that, in the determination of any criminal charge against a person, everyone shall be entitled to the minimum guarantee of "not to be compelled to testify against himself or to confess guilt". However, the reasons underlying this guarantee could justify a general privilege against any active self-incrimination.

3. Wire-tapping and "eavesdropping"

Problems of traditional law

163. Tapping telecommunication lines and eavesdropping on computer systems can assist criminal investigations, especially in cases where data are only transmitted and not permanently stored, where data merely cross a country or where permanent observation of telecommunications or computer activities is necessary. These investigative acts, however, constitute not only a highly efficient means of prosecution but also a very severe intrusion into the civil liberties of the person whose communications have been surveyed. This is primarily based on the fact that tapping telecommunication systems and eavesdropping on computers is, generally, a permanent and clandestine intrusion, whereas the above-mentioned powers of entry, search and seizure usually

constitute a single, "visible" interference with civil liberties. Consequently, in most countries the statutory requirements for telephone tapping and the recording of telecommunications are much more stringent than for other coercive measures.

164. The question whether the traditional powers of wire-tapping can be applied to tapping other telecommunication services and computer systems is answered differently in various countries. No computer-specific issues arise in legal systems in which the statutory law permits, for example, "surveillance of the telecommunication traffic including the recording of its content". On the other hand, computer-specific problems of interpretation exist, especially in countries that permit only "monitoring of conversations" or "surveillance and tapping of the telecommunication traffic on sound carriers". Such clauses are particularly problematic if an analogous application of coercive powers in criminal procedural law is not jurisprudentially permissible.

Law reform

165. To avoid problems of interpretation, some countries have already enacted or proposed new legislation that would make it possible to tap all kind of telecommunications under the same conditions as must be met for tapping telephone conversations. In Denmark, a new provision of the Administration of Justice Act was passed in 1985, according to which the police. under certain conditions , may "interfere in private communication by ... tapping telephone conversations or other similar telecommunication". In 1986, in the United States, the Electronic Communication Privacy Act extended legal protection and powers of wire-tapping from aural communication (covered by the Omnibus Crime Control and Safe Street Act of 1968) to electronic communication. Similarly, in the Federal Republic of Germany, an amendment to the Criminal Procedural Code in 1989 11extended the possible use of wire-tapping to public telecommunication networks. With respect to future policy-making, such clarifications are helpful since telecommunication between computers probably does not merit more protection than telecommunication between persons.

C. Specific problems with personal data

166. Potentially coercive powers for collecting evidence in the field of information technology, as analysed above, cover both personal and non-personal data. With respect to personal data, however, there are additional legal problems that mainly concern gathering, storing and linking personal data in the course of criminal proceedings. In this field of "privacy protection in criminal matters", legal requirements vary considerably among countries. Differences between various legal systems are found not only in substantive law requirements but also in the constitutional background, legal context and legislative technique of the relevant provisions.

167. An extensive discussion of the underlying constitutional implications regarding the gathering, storing and linking of personal data exists in only a few countries. For example, in the Federal

Republic of Germany, the Federal Constitutional Court, in its famous "census decision", recognized that the State's storage of personal data, especially in computer systems, could influence citizen's behaviour and endanger their general liberty of action and must therefore be considered as a violation of civil liberties ("right of informational self-determination"), which requires an express and precise legal basis. This legal balance must balance the interests of the individual and the right to privacy, on the one hand, and the interests of society in the suppression of criminal offences and the maintenance of public order, on the other hand. The new Constitution of Spain of 1978, the new revised Constitution of Portugal of 1982, the Constitution of the Netherlands of 1983 and the new Constitution of Brazil of 1988 even contain specific safeguards protecting their citizens' privacy against the incursions of modern computer technology. However, in many other countries the gathering and storing of personal date are not (yet) considered to be of constitutional relevance and are dealt with by the legislature in ordinary statutory (non-constitutional) law on a voluntary basis.

168. In regulating the legality of gathering, storing and linking personal data (either on a constitutional, compulsory basis or on an ordinary, voluntary legal basis), various legal systems place the relevant provisions in different contexts and laws. A few countries, such as Germany, intend to place most of the respective provisions within the purview of their criminal procedural law.. This legislative technique has the advantage that the criminal procedural code retains its monopoly over the application of criminal law and thus retains the exclusive enumeration of powers regulating the infringement of civil liberties in the course of criminal prosecution. However, most countries (uniquely or in part) regulate the legality of police files within their general data protection acts; in most cases the relevant provisions are applicable both to the enforcement activity of the police (prosecution of crimes) and to its preventive action (maintenance of public order). Some countries exclude police files, completely or partly, from their general data protection laws and/or create specific acts or decrees for all types of (law enforcement or preventive) police data. In a number of countries, additional specific laws concerning criminal records exist. However, there are also legal systems without any statutory legal provisions regulating the general use of personal data in the police sector.

169. Apart from these questions of placement and context of the relevant statutes, the legislative technique, content and control mechanisms of the relevant laws also vary. With respect to legislative technique, some countries, such as Germany, consider a more detailed and precise regulation necessary; other countries resort to more or less general clauses.

170. As far as the contents of the various laws are concerned, serious limitations rarely seem to be applicable to police files. In many countries, far-reaching and precise regulations concerning the deletion of entries exist only with respect to registers of criminal convictions.

D. Admissibility of computer-generated evidence

171. The admissibility of computer-generated evidence is not only important for the use of computer records in the criminal trial process but is also essential to define the extent of the above-described coercive investigatory powers, including those of mutual assistance. In most countries coercive powers are applicable only to material that would be admissible in evidence at a trial, if specific computer data or printouts could not be used as evidence; consequently, they could also not be searched and seized. In practice, the various legal problems are particularly crucial since computer printouts and computer data can easily be manipulated, a phenomenon that is illustratively described as the "second-hand nature" of computer printouts.

172. The admissibility in courts of evidence from computer records depends to a great extent on the underlying fundamental principles of evidence in the particular country. It is necessary to differentiate among varying legal systems, including but not limited to (a) civil law countries and (b) common law countries. Other legal systems, such as Islamic law, incorporate elements from one of these two primary types of systems.

1. Civil law countries

173. Civil law countries and many other countries operate according to the principle of free introduction and free evaluation of evidence (système de l'intime-conviction). In these countries the judge can, in principle, consider all kinds of evidence and then weigh the extent to which the court can rely on the evidence. Legal systems based on these principles do not, in general , hesitate to introduce computer records as evidence. Problems occur only when procedural provisions contain specific regulations for the proof of judicial acts or proof with legal documents.

2. Common law countries

174. Contrary to the legal situation in civil law countries, common law countries are characterized by an oral and adversarial procedure. In these countries a witness can only testify concerning his or her personal knowledge, thereby permitting the statements to the verified by cross-examination. Knowledge from secondary sources, such as other persons, books or records, is regarded as hearsay evidence and is, in principle, inadmissible. Additionally, the "best-evidence" rule generally requires that originals, rather than copies, be introduced as evidence before the court in order to lessen the chance of fraud and error. There are, however, several exceptions to the hearsay and best-evidence rules, such as the "business records exception" or the "photographic copies exception". The business records exception, for example, permits a business record created in the course of everyday commercial activity to be introduced as evidence even if there is no individual who can testify from personal knowledge. If certain prerequisites are met, copies of certain types of records may also be permitted. The questions whether computer files are "real evidence" and whether

computer printouts fall under one of the exceptions of the hearsay rule have been the subject of extensive debate. The courts in some common law countries have accepted computer printouts as falling within the business records exception. Other common law countries have elaborated new laws allowing computer records to be admitted as evidence if certain conditions are met.

3. Islamic law countries

175. Under Islamic law, computer crime falls within the area of taazir offences, which operates according to the same principles of evidence law as civilian systems: the free introduction and evaluation of evidence (système de l'intime-conviction). In adjudicating taazir offences the judge weighs the reliability of evidence, and thus computer records are generally admissible in the prosecution of computer crime.

E. International harmonization

176. In procedural law, international action has already commenced in all of the areas described above and has been concerned with (a) the field of coercive powers; (b) the legality of processing personal data in the course of criminal proceedings; and (c) the admissibility of computer-generated evidence in court proceedings.

1. Coercive powers in the field of information technology

177. One example of international harmonization of the above-mentioned coercive powers in information technology derives primarily from the guarantees of article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms. The European Court of Human Rights applied these guarantees especially in the area of wire-tapping. In the Klass case,the Court confirmed the legality of the German law on limitations of the secrecy of letters, post and telecommunication, which, under specific conditions, provides the authorities with the competence to supervise

V. CRIME PREVENTION IN THE COMPUTER ENVIRONMENT

A. Security in the electronic data-processing environment

186. Society increasingly relies on automated systems to carry out many essential functions in day-to-day life. If these systems are to be depended upon, it is essential that the persons responsible for their operation recognize the vulnerabilities to which they are subject and take steps to implement appropriate safeguards.

187. An EDP system can be considered as a group of assets of varying sensitivity related to the maintenance of tree basic requirements: confidentiality, integrity and availability.

188. EDP security, while a relatively recent discipline, is subject to a variety of interpretations. Historically, security measures have been applied to the protection of classified information from the threat of disclosure in a national security context. Recently, much attention has been directed to the issue of individual privacy as it relates to personal information stored in computerized data systems. Another consideration is data integrity in financial, scientific and process control applications. The security of computer installations themselves is of great concern to many organizations, owing to the significant financial investment involved.

189. Since all of these interpretations of EDP security may have significance to different users, a practical definition is needed to account for the wide range of concerns. For the purpose of this Manual, EDP security is defined as that state reached when automated systems, data and services are receiving appropriate protection against accidental and deliberate threats to confidentiality, integrity or availability.

190. Security, like insurance, is to a large extent applied risk management, defined as the attempt to archive a tolerable level of risk at the lowest possible cost. The goal is to reduce the risk exposure of the facility to an acceptable level, best achieved by a formal assessment of risk. This includes a number of components, such as the identification of EDP assets, values, threats and vulnerabilities and the financial impact of each threat-asset combination; estimation of the frequency of occurrence for each chosen threat-asset pair; and choice of safe-guards and implementation priorities for security measures. Safeguards should not only be cost-effective but should also provide a judicious balance between those designed to prevent threats, those to detect threats occurrences or security infractions and those to respond to the threats that inevitably occur. Risk analysis is a team function that must involve managers from user, application, systems and operations areas in the establishment of priorities and the allocation of funds for security measures. In some cases, where confidentiality is a specific concern, additional protection must be provided through the application of mandatory regulatory requirements. Government classified information is subject to such regulations.

B. Assets

191. Three general categories of assets in the computer environment can be targeted for protection, each posing a distinct protection problem given is unique sensitivities.

1. Software, data and information

192. Protection requirements for software, data and information are based on the need to preserve confidentiality, integrity and availability. Confidentiality, or the need to protect from disclosure, can be required because a system contains personal data, information proprietary to an organisation

or data related to national security. Even waste material may require protection up to the time of is destruction.

193. Software and data integrity are also requirements of all computer systems. Users of the system require assurance that unauthorized changes, deliberate or accidental, do not take place. The integrity of all software, utilities and applications must be above question, otherwise the results of manipulating the data will not be practicable.

194. To be of value, software and data must be available for use within an acceptable time-frame. The availability concern is important in both the long and short term. The properties of confidentiality, integrity and availability can also be applied to other information assets, such as system documentation, descriptive materials and procedural manuals, control forms, logs and records.

2. Data-processing services

195. In numerous cases the sensitivity of the information handled may not be as significant as the services performed. Service can be the most important asset requiring protection in cases where national security, the safety or livelihood of individual citizens, or essential services are dependent upon computer systems. Air traffic control, police information service, medical monitoring systems, electronic funds transfer systems and all services where processing is time-sensitive, in which availability is an important goal, are examples of this type of dependency.

3. Electronic data-processing equipment and facilities

196. The third category of assets requiring protection involves tangible property in the EDP environment, including computer equipment and supplies, the physical site facilities, machine rooms, media libraries, data preparation areas and terminal areas, as well as environmental services, such as power, air-conditioning and lightning.

197. Although these three categories represent the features of computer systems that security measures should target, the current limitations of computer security technology require that a much broader view of safe-guards be taken. Computer security is a weak-link phenomenon. To ensure that complete protection is provided to EDP assets, other established security areas, such as administrative, personnel, physical and communication-electronic security, must be taken into consideration. There is little point in emphasizing sophisticated systems features if more basic and perhaps more vulnerable areas are slighted. It also has been noted that, owing to the cost or unavailability of technical features in computer systems, physical or procedural safe-guards are sometimes practical alternatives.

C. Security measures

198. EDP security is considered to consist of seven essential components: administrative and organizational security; personnel security; physical security; communication-electronic security; hardware and software security; operations security; and contingency planning.

1. Administrative and organizational security

199. Administrative security involves the development of an overall security policy and the establishment of procedures for its implementation. While specific security administrative practices will vary considerably depending on the size and nature of the work performed by an organization, minimum requirements include the following:

1. The development of procedures to ensure that risks are identified;
2. The definition of individual security duties and the appropriate assignment of responsibilities;
3. The designation of restricted areas;
4. The establishment of authorization procedures;
5. The identification of external and contractual dependencies;
6. The preparation of contingency plans.

200. Second only to the necessity for the established policy and procedures for EDP security is the requirement for an effective organization to administer it. It is essential that senior management be aware of EDP security requirements and of the fact that a close working relationship must be cultivated between automated system management and the group responsible for overall security.

2. Personnel security

201. Personnel security includes specifying security requirements in job descriptions and ensuring that incumbents meet these requirements and are provided with adequate security motivation and training. It involves supervising access to and control over system resources through appropriate personnel identification and authorization measures. It further requires attention to hiring and employment termination procedures. External service or support personnel such as maintenance and cleaning staff or contract programmers who have unsupervised access to restricted areas should be subject to the same personnel security measures as regular employees.

3. Physical security

202. All EDP facilities should be provided with physical protection in order to ensure security commensurate with the sensitivity of the data being processed and the service being provided. The following factors should be borne in mind when physical security measures are chosen:

1. Site planning (e.g. location and layout, building construction, heating, lighting, fencing and shielding);

2. Control of access to restricted areas (e.g. perimeter security, visitor control, key and badge control, guard staffs and intrusion alarms)
3. Protection against physical damage (e.g. fire, flooding, explosion, wind, earthquake and physical attack);
4. Protection against power and environmental failures (e.g. air-conditioning, water-cooling, power-monitoring, un-interruptable power-sources and dust control);
5. Protection of EDP media and supplies (e.g. waste disposal, storage containers, transportation, postal procedures and packaging).
The close relationship between the physical, environmental and hardware aspects of EDP security makes coordination between computer system and traditional security staff essential, particularly during the planning and design stages of new systems and facilities.

4. Communications-electronic security

203. Telecommunication are almost invariably a fundamental component of automated systems, and their use has the effect of extending the geography of the security concern and of complicating service availability. As the communication facets multiply, so do the possibilities of crossed communication between lines, misrouting of information and the wire-tapping of, and monitoring of electromagnetic radiation from hardware. Some possible countermeasures for communications and electronic threats include electronic screening, filtering encryption and specially designed terminals. However, the inherent complexity of communications systems requires that each case be approached individually. As dependence on communications become greater, so too does the probability that the ability to provide the automated service could be lost because of a failure in the communication system.

5. Hardware and software security

204. Hardware security relates to those protective features implemented through the architectural characteristics of the data-processing equipment, as well as the support and control procedures necessary to maintain the operational integrity of those features.
205. Computer systems security features, whether implemented in hardware, software or micro-programmed firmware, can be addressed in five categories:
1. Identification mechanisms to identify authorized users;
2. Isolation features that ensure that users of the system are restricted from accessing devices, software and data to which they are not entitled;
3. Access control features that provide for selected sharing of system resources by removing or negating isolation measures for authorized cases;

4. Surveillance and detection measures, which assist in the detection of security violations, usually implemented by software;
5. Response techniques to counter the harm of security violations, such as redundant components and circuits, and error correction logic.

6. Operations security

206. Operations security relates to the policy and produces that are necessary to ensure that the required operational capability is always available and that security exposures within the environment are acceptable. Once an environment has been selected that presents minimal inherent weaknesses, the vulnerabilities within the environment should be reduced as much as is practicable. The most important step in this process is to ensure that responsibilities are clearly assigned. The concept of separation of duties and the concept of least privilege are helpful in this regard. In shared systems, the separation of duties concept means that no single individual can subvert controls on the system and the least privilege concept ensures that no one is granted a capability for which there is no well-substantiated operational necessity.

207. The considerations involved in establishing and maintaining an adequate security program are, briefly, as follows:

1. Identification of the EDP assets (data, software, hardware, media, services and supplies) requiring protection;
2. Establishment of the value of each of the assets;
3. Identification of the threat associated with each of the assets;
4. Identification of the vulnerability of the EDP system to these threats;
5. Assessment of the risk exposure associated with each asset (probability of frequency of occurrence multiplied by impact of occurrence);
6. Selection and implementation of security measures;
7. Audit and refinement of the EDP security program on a continuing basis.

208. It is generally recognized that absolute security is an unrealistic goal. An adversary with sufficient motivation, resources and ingenuity can compromise the most sophisticated security safeguards. An optimum security policy is one in which the cost of implementing protective mechanisms has been balanced against the reduction in risk achieved. Although security measures can be costly, experience has shown that adequate security is inexpensive compared to the potential consequence of failure to provide appropriate protection.

7. Contingency planning

209. Every EDP system has been developed to perform some type of service or to fulfill a role. The plans for achieving the goals associated with that role are, in most instances, based on normal

operating conditions. However no amount of precautionary work can preclude the occurrence of situations that produce unexpected disruptions in routing operations. Contingency planning is therefore a basic requirement in the EDP security program, regardless of the sensitivity of the information processed or the size of the installation providing the service.

D. Law enforcement and legal training

210. The dynamic nature of computer technology, compounded by specific considerations and complications in applying traditional laws to this new technology, dictate that the law enforcement, legal and judicial communities must develop new skills to be able to respond adequately to the challenge presented by computer crime. The growing sophistication of telecommunications systems and the high level of expertise of many system operators complicate significantly the task of regulatory and legal intervention.

211. Familiarity with electronic complexity is slowly spreading among the general population. It is a time when young people are comfortable with a new technology that intimidates their elders. Parents, investigators, lawyers and judges often feel a comparative level of incompetence in relation to "complicated" computer technology. In their recent book, Hafner and Markhoff contend that society is in a transition, in terms of general familiarity with computers and their use. Training in this area and familiarity with the concepts behind complex computer techniques such as trojan horses and salami slices are required before law enforces can operate adequately.

212. Until recently, computer-related crime was concentrated in the economic environment. The law enforcement community responded by training existing commercial crime or fraud experts in the specialized area of computer crime investigation. However, modern experience indicates that computer crime has progressed far beyond the economic environment and is evident in many areas of traditional criminal activity. For example, drug traffickers can utilize data banks to organize transactions and store records of their contacts. Sex offends have utilized computer bulletin boards to identify potential victims. A coordinated and concentrated effort must be made to provide investigators, prosecution authorities and the courts with the necessary technical means and expertise to adequately and properly investigate all types of computer crime. To adopt this approach will require a dedication to efficient training.

213. Few individuals possessing the necessary blend of experience and technical understanding in computer technology are employed in law enforcement. Teaching computer techniques to individuals in all sectors of the justice system will promote an appreciation of the complexities that have arisen in this new area of enforcement and will foster consistency in the application of criminal sanctions and procedures. For example, traditional search and seizure techniques are conducted in an environment where the evidence being sought is visible or otherwise tangible. In the electronic environment, however, courts and investigators alike are often unsure how to apply

traditional evidence procedures to intangible information. In addition, very few legislative or procedural guidelines exist. Proper training in clearly developed search and seizure techniques is required to ensure the preservation of evidence consistent with accepted principles of admissibility of evidence, while at the same time protecting the rights of all parties to the action.

214. An appropriate training program would, therefore, impart a thorough understanding in five areas.

1. The difference between a civil and a criminal wrong

215. Since not all computer-related abuses may constitute a criminal offense, it is necessary to be able to differentiate between infringements of the civil law and the criminal law, as well as to determine what are merely social nuisances. This is important for the purposes of establishing liability and respecting the rights of citizens, and it also permits scarce police resources to be concentrated on and allocated to conduct that is truly deserving of the criminal sanction.

2. The technology

216. To address computer crime, most police departments are allocating a greater proportion of resources to their economic or fraud investigation divisions, since many types of computer crime occur in the course of business transactions or affect financial assets. Accordingly, it is important for investigators to know about business transactions and about the use of computer in business.

217. To be able to understand fully the potential for criminal exploitation of computer technology, regardless of whether it is business-related, investigators must have a thorough understanding of that technology. Experience has demonstrated that the assistance of technical experts is not sufficient. The ideal situation is to have investigators with not only solid criminal investigation backgrounds but also supplementary technical knowledge. This is similar to the traditional approach, where many police forces ensure that their fraud investigators, although not necessarily accountants, possess a thorough understanding of financial and business record-keeping.

218. By extension, the administrators of the criminal justice system must also ensure that those who fulfill the prosecutorial and judicial duties possess enough technical knowledge to be able to properly prosecute and adjudicate computer crimes.

3. Proper means of obtaining and preserving evidence and of presenting is before the courts

219. Investigators have always been expected to be well trained in obtaining evidence, maintaining its continuity and integrity and presenting it to the prosecutorial authorities in a manner such that it may be considered by the courts. These processes presented little difficulty when the evidence was tangible and detectable by human senses. Computer technology, however, has introduced new challenges to the gathering and preservation of evidence. Investigators must be able to search for,

gather, analyse, maintain the continuity and integrity of, and present computer evidence for the purposes of judicial hearings. It must be done in a manner that is fair to the parties concerned and that does not risk damaging or modifying the original data. This requires a special knowledge of and the development of investigatory techniques that will be judicially acceptable. It also requires an understanding of the laws of evidence of the particular jurisdiction.

4. The intricacies of the international nature of the problem

220. National boundaries, which in the past may have hindered the activities of criminals, have effectively disappeared with the advent of modern telecommunications. In gathering evidence, investigators must be able to understand and deal with international issues, such as extradition and mutual assistance. The laws of evidence, criminal procedure and data protection of other jurisdictions must be considered when pursuing international investigations.

5. The rights and privileges of the accused and the victim

221. Investigators, prosecutors and others involved in the investigation and prosecution of computer crime must be fair to both the accused and the victim in order to ensure equitable application of the law. Additionally in dealing with international investigations, investigators should also understand the rights and privileges in the order jurisdiction to ensure the integrity and fairness of the investigation. Respect for the rights and privileges of all persons concerned will not only ensure the credibility of the investigators and others who present these matters before the courts, but it may also help to instill confidence in the citizenry that the criminal justice system can adequately and fairly deal with the challenges posed by the computer criminal.

E. Victim cooperation in reporting computer crime

222. In paragraph 30, the term "dark figure" was briefly discussed. All studies in this area have indicated that the true extent of computer-related crime in unknown, since most crimes are either not detected or are not reported to the responsible authorities. The inability or reluctance of victims to identify incidents of computer crime must be addressed.

223. International studies have examined the relation behind this reluctance, evident particularly in the financial sector, to report computer crime. Loss of consumer confidence in a particular business and in its management can lead to even greater economic loss that that caused by the crime itself. In addition, many managers fear personal repercussion if responsibility for the infiltration is placed at their door. Victims have complained about the inconvenience of lengthy criminal investigations and indeed have questioned the ability of authorities to investigate the crime. These concerns, however, must be balanced by the equally important consideration that, in the absence of detection and sanction of crime, offenders will be encouraged to commit further computer-related crimes.

224. Without the cooperation of victims of computer crime, efforts to suppress computer crime, can be only partially effective. Reporting incidents of crime to authorities and society at large is necessary to discourage criminal behaviour. In response to the concerns of the business community regarding consumer confidence, it is suggested that an open, proactive approach to computer crime in fact would instill public confidence in a company's commitment to preventing and detecting crime and to protecting the interests of its investors.

225. The accurate reporting of computer crimes provides an additional benefit. The more information the law-enforcement community has on new trends in computer crime, the better it can adapt existing methods of detection to respond to them. The experience and knowledge of those responsible for investigating and processing computer crimes would be immeasurably broadened.

226. Methods to encourage victim openness have been discussed by the Select Committee of Experts on Computer-Related Crime. The report of that Committee detailed various possible strategies, ranging from legislating cooperation to creating an independent body that would provide advice and assistance to victims. While no definitive solution was chosen, there was a consensus that reporting of crimes would promote public confidence in the ability of the law-enforcement and judicial communities to detect, investigate and prevent compute-related crime.

F. Developing a computer ethic

227. In contrast to the science of computers, which has only existed in this century, other sciences and disciplines have had a longer time in which to develop the ethical standards and principles that inform new developments. Codes of ethics in medicine, accounting, law and engineering, for example, are well established and a continuity of principles and ethics has been maintained as these codes are transferred from instructor to student.

228. The need for a similar, specialized ethic for computer technology is clear. Computer-specific ethical issues arise from the unique characteristics of computers and the roles they play. Computers are now the repositories of modern, negotiable assets, in addition to being a new form of asset in themselves. Computers also serve as the instrument of actions, so that the degree to which computer service providers and users should be responsible for the integrity of computer-output becomes an issue. Furthermore as technology advances into areas such as artificial intelligence, threatening to replace humans in the performance of some tasks, it takes on intimidating proportions.

229. The need for professionalism on the part of service providers in the computer industry, as well as on the part of systems personnel who support and maintain computer technology, is well recognized. Ethical codes are the natural consequence of realizing the commitment inherit in the safe use of computer technology in both the public and private sector.

230. There is a parallel need for professionalism on the part of users of computer systems, in terms of their responsibility to operate legally in full respect of the right orders. Users must be made aware of the risks of operation when systems are being used or installed; they have a responsibility to pursue and identify lapses in security. This will promote ethical conduct in the user community.

231. Education can play a pivotal role in the development of ethical standards in the computer service and user communities. Exposure to computers occurs at a very early age in many countries, often at the primary school level. This presents a valuable opportunity to introduce ethical standards that can be broadened as children progress through school and enter the workforce. Universities and institutes of higher learning should include computer ethics in the curriculum since ethical issues arise and have consequences in all areas of the computer environment.

232. In 1992, recognizing that with society's increasing dependence upon computer technology standards ensuring the availability and the intended operation of systems were required, OECD adopted guidelines for the security of information systems. As increased dependence results in increased vulnerability, standards to protect the security of information systems are just as important. The principles that OECD is promoting have broader application that the security of information systems; they are equally relevant for computer technology in general. Of primary importance among these principles is a statement of ethics that recognizes the rights and legitimate interests of others in the use and development of the new technologies (see paragraph 238).

233. The promotion of positive computer ethics requires initiatives from all sectors of society at the local, national and international levels. The ultimate benefit, however, will be felt by the global community.

G. International security of information systems

234. Lack of international coordination and cooperation can have detrimental effects on national and international economies, on trade and on participation in social, cultural and politic life. International understanding of, and domestic implementation of measures that are required to enhance the security of information systems and facilitate the international exchange of data and commerce are important. Confidence that countries are abiding by security principles promotes confidence in international trade and commerce.

235. It has been noted throughout this Manual that the present measures, practices, procedures and institutions may not adequately meet the challenges posed. There is a need for clarity, predictability, certainly and uniformity of rights and obligations, of enforcement of rights, and of recourse and redress for the violation of rights relating to information systems and their security.

236. The OECD guidelines for the security of information systems were developed to provide a foundation on which countries and the private sector acting singly and in concert may construct a framework for the security of information systems. The framework includes laws code s of

conduct, technical measures, management and user practices and public education and awareness activities. The guidelines are intended to serve as a benchmark against which Governments, the public sector, the private sector and society may measure their progress.

237. The guidelines are addressed to the information systems. They are intended to accomplish the following:

1. Promote cooperation between the public and private sectors in the development and implementation of such measures, practices and procedures;
2. Foster confidence in information systems and the manner in which they are provided and used;
3. Facilitate development and use of information systems, nationally and internationally;
4. Promote international cooperation in achieving security of information systems".

238. guidelines are based on nine principles:

"1. Accountability principle

The responsibilities and accountability of owners, providers and users of information systems and other parties concerned with the security of information systems should be explicit.

2. Awareness principle

In order to foster confidence in information systems, owners, providers and users and other parties should readily be able, consistent with maintaining security, to gain appropriate knowledge of and be informed about the existence and general extant of measures, practices and procedures for the security of information systems.

3. Ethics principle

Information systems and the security of information systems should be provided and used in such a manner that the rights and legitimate interests of others are respected.

4. Multidisciplinary principles

Measures, practices and procedures for the security of information systems should take account of and address all relevant considerations and viewpoints, including technical, administrative, organizational, operational, commercial, educational and legal considerations and viewpoints.

5. Proportionality principle

Security levels, costs, measures, practices and procedures should be appropriate and proportionate to the value of and degree of reliance on the information system and to be severity, probability and extent of potential harm, as the requirements for security vary depending on the information system.

6. Integration principle

Measures, practices and procedures for the security of information systems should be coordinated and integrated with each other and other measures, practice and procedures of the organization so as to create a coherent system of security.

7. Timelines principle

Public and private parties, at both the national and international levels, should act in a timely and coordinated manner to prevent and to respond to branches of security of information systems.

8. Reassessment principle

The security of information systems should be reassessed periodically, as information systems and the requirements for their security vary over time.

9. Democracy principle

The security of information systems should be compatible with the legitimate use and flow of data and information in a democratic society".

VI. INTERNATIONAL COOPERATION

A. General aspects

239. As modern society is heavily information-dependent, computer-related crimes are easily committed on an international scale. International access to information and the mobility of data are fundamental to the working of our economic systems. Distance, time and space have ceased to be obstacles in commercial transactions. There is no longer any need for the physical presence of human agents. As the manipulation and storage of data take place within the dimension of international telecommunication networks, the usual border controls are bypassed. International instruments containing principles of the transborder flow of data, such as those by the United Nations or OECD, focus clearly on the principle of free flow of information, tempered by concerns to protect the confidentiality and integrity of the transmitted information, particularly in the case of sensitive data. Given the utility of paperless commercial transactions in international commerce and the rapidly improving sophistication of electronic communications, the volume of cross-boarder computer has increased significantly.

240. Currently, whole sectors of economy, such as banking and international aviation, rely heavily or even exclusively on international telecommunication networks. With the continuing development of standards and norms for electronic data interchange (EDI), such as that under the auspices of the United Nation Electronic Data Interchange for Administration, Commerce and Transportation (UN/EDIFACT), the use of EDI will increase substantially in the decade to come.

241. The international element in the commission of computer crime create new problems and challenges for the law. Systems may be accessed in one country, the date manipulate in another and the consequences felt in a third country. Hackers can operate physically operate in one country, move electronically across the world from one network to another and easily access databases on a different continent. The result of this ability is that different sovereignties, jurisdictions, laws and rules will come into play. More than in any other transnational crime, the speed, mobility,

flexibility, significance and value of electronic transactions profoundly challenge the existing rules of international crime law.

242. There are a number of complex issues to confront, given the multiplicity of countries potentially involved in a crime. How can it be determined which country the crime was actually committed? Who should have jurisdiction to prescribe rules of conduct or of adjudication? In crimes involving multinational contacts, there will be frequently be conflicts of jurisdiction. Countering computer crimes committed from a distance and having and increasing range of international targets (such as country of commission of the crime, the number of actors and victims involved, and the range of potential consequences) will require a well-developed network of inter-State cooperation to attain effective investigation and prosecution. In the light of the technicalities of international interaction, cooperation between nations in criminal matters is crucial.

243. These issues have to be addressed by all countries, whether they be producers, users or consumers of the new information technologies, since these technologies ate becoming an integral part of economic, social and culture development.

244. In seeking solutions to the above problems, the international community should strive for the following:

1. Maximizing cooperation between nations in order to address, firstly, the potential for enormous economic losses and, secondly, the general threat to privacy and other fundamental values that near-instantaneous cross-border electronic transactions may create;

2. Worldwide protection so as to avoid "data paradises" or computer crimes havens where computer criminals can find refuge or launch there attacks;

3. A lawfully structured cooperation scheme, taking into account and balancing the necessities of international trade and relations on the one hand and the rights and freedoms of the individual on the other hand.

B. The jurisdiction issue

1. The territoriality principle

245. There are a number of problems related to the issue of jurisdiction. In every computer crime, the determination of the locus delicti (the location of the offence) will affect the ability of a particular country to sanction the crime. Will the sanction arise by virtue of territorial jurisdiction and domestic law, or must extraterritorial principles apply?

246. Today, it is technologically possible for an operator to punch a keyboard in country A so as to modify data stored in country B, even the operator does not know that the data are stored there, to have the modified data transferred over a telecommunications network through several other countries, and to cause an outcome in country C. On the basis of the physical act, the technical

modification, the transmission of the falsified data and the consequences, three or perhaps more countries will have been involved and may have a claim to jurisdictional competency.

247. Depending on which elements or stages of the crime are given priority, several countries in the above scenario could, within their full sovereignty, declare the incident as having occurred on their territory, thus invoking the principle of territorial jurisdiction in order to prosecute and sanction. This raises a potential jurisdictional conflict, as well as the question of the appropriate arbitration of these equal claim for jurisdiction, the applicability of the non bis in idem rule,and the impact of the lex mitior rule.

248. The recurring threat of computer viruses worms in another striking example of transnationality. If a virus infects the system in one location, the infection can spread with destructive rapidity and affect programs throughout the international network. What criteria should apply in determining which country may act? Once again, several choices are available: the country in which the virus was introduced, all countries in which software or databases were affected and all countries in which results were felt. It is possible that it may not manifest itself far away from the country of origin. It is also possible that it may not manifest itself until considerable time has passed, when retracing the technological path of the of the original offender has become difficult, as, for example, in cases of the so-called time-bomb virus. What, then, determines the competency to prosecute and sanction? Can it be the best evidence rule or the first-come, first-served principle, or do the traditional solutions discussed below still stand firm?

249. The primacy of the principle of territoriality is generally accepted in sphere of criminal jurisdiction. The principle is based on mutual respect of sovereign equality between States and is linked with the principle of non-intervention in the affairs and exclusive domain of other States. Even in the exceptional event that a country might apply extraterritorial jurisdiction for a sake of protecting its own vital interests, the primacy of the extraterritorial principle is not altered.

250. The ubiquity doctrine is often referred to in determining the place of commission. The offence will be considered to have been committed in its entirety within a country's jurisdiction if one of the constitutive elements of the offence, or the ultimate result, occurred within that country's borders. Jurisdiction is equally applicable to co-perpetrators and accomplices.

251. Common law countries also use the effects doctrine in addition to focusing on the physical act. This doctrine locates crimes in the territory in which the crime is intended to produce, or actually does produce, its effects. Thus, where various elements or effects of a crime may occur in more than one country, the two doctrines of territorial jurisdiction may lead to concurrent, legitimate jurisdictional claims.

252. These positive conflicts of jurisdiction, while at first glance not very problematic in determining the appropriate judicial response, do contain some inherent risks. The most

fundamental problem is the general refusal, particularly in civil law systems, to apply the double jeopardy rule. Thus, the accused is submitted to a multitude of prosecutions for the same act.

253. Equally important is the manner of classification of the multiple acts potentially involved in a pattern of computer crimes. In particular, in cases of repeated data manipulation, data espionage or unauthorized access, it is unclear whether the acts should be considered as separate crimes or as a single act by application of the principle of international connexity, by which a single prosecution for the whole transaction would be justified.

254. States should, therefore, endeavour to negotiate agreements on the positive conflicts issue. These agreements should address the following issues:

1. An explicit priority of jurisdictional criteria: for example, of location of act over location of effect, of the place of physical detainment of the suspect over in absentia proceedings or extradition;

2. A mechanism for consultation between the States concerned in order to agree upon either the priority of jurisdiction over the offence or the division of the offence into separate acts;

3. Cooperation in the investigation, prosecution and punishment of international computer offences, including the admissibility of evidence lawfully gathered in the other countries, and the recognition of punishment effectively served in other jurisdictions. This would prevent unreasonable hardship to the accused, otherwise possible by an inflexible interpretation of the territoriality principle.

2. Other base of jurisdiction

255. The issue of international computer crime also requires an analysis of the principles of extraterritorial jurisdiction. State practice discerns the following theoretical grounds:

1. The active nationality principle, which is based on the nationality of the accused. The principle, when applied in conjunction with the territoriality principle, may result in parallel concurrent jurisdictions, creating a situation of double jeopardy. The use of the active nationality principle is therefore generally confined to serious offences;

2. The passive personality principle, which is based on the nationality of the victims. This principle has been highly criticized, since it could subject a national of State A, although acting lawfully in State A, to punishment in State B for acts done in State A to a national of State B, if the acts were unlawful in State B and State B were to apply the principle. On practice, therefore, this principle is seldom used;

3. The protective principle, which is based on the protection of the vital interests of a State. By this principle, a State may exercise jurisdiction over foreigners who commit acts that are considered to be a threat to national security. Given the potential for abuse of this principle if security is

interpreted too broadly, the protective principle is not highly favoured; in practice, therefore, it is often linked to other doctrines, such as the personality principle or the effects doctrine;

4. The universality principle, based on the protection of universal values. It is usually effected on the basis of express treaty provisions but is otherwise rarely used. It is generally held that this principle should apply only in cases where the crime is serious, where the State that would have jurisdiction over the offence, based on the usual jurisdictional principles, is unable or unwilling to prosecute.

256. Other than the basic policy considerations as to whether a State should apply one or more of these bases of jurisdiction, it is unlikely that application of these principles of extraterritorial jurisdiction to information technology offences will create specific problems. Nevertheless, the characteristics of transnational computer crime do have the potential to involve an increasing number of States, thereby creating a jurisdiction network in which the ordering of the subsequent priorities is required.

257. There are no rules of international law, other than the principles of comity and non-intervention, that impose express limitations on the freedom of sovereign States in establishing extraterritorial criminal jurisdiction. Where there is strong international solidarity by way of customary or conventional international law, jurisdiction over important offences may be decided by the principle of universality, in addition to the applicability of other grounds of jurisdiction. No such conventions exist yet in relation to computer crime. Eventually, however, as has been the case in other major international crimes, international conventions will regulate this area.

258. A spirit of moderation might be expected from States in exercising these jurisdictional principles, in order to encourage international cooperation and to avoid significant conflicts of jurisdiction with other States. In that spirit, the passive personality principle, although sometimes used to protect the economic interests of nationals (natural or legal persons), is highly disputed, while universality is best limited to express treaty provisions. The protective principle may be relevant for certain types of computer offences, because it grants jurisdiction to a State over offences committed outside its territory, in the defence of fundamental (vital) interests.

259. There exists very little consensus on what constitutes vital interests. No doubt a sovereign State might consider attacks on data or telecommunication infrastructures, when related to basic government activities (police data, military data, State security systems etc.), to fall within its purview. However, a tendency may arise to consider certain economic interests, naturally involving a significant amount of transborder data flow, as a vital concern of the State. Nevertheless, caution is needed in regard to such extensions, since they can affect adversely the legitimate flow of information and data, as well as other economic and social interests. Therefore, the State concerned should be expected to take due account of the principles of cooperation, comity and reasonableness, which should govern State action in exercising extraterritorial jurisdiction.

260. Even if very few specific computer-related concerns seem apparent, the general issues in extraterritorial jurisdiction remain valid: the need for harmonized legislation (see paragraphs 268-273), the settlement of concurrent jurisdictional claims, the international validity of the non bis idem principle and the development of agreements on mutual cooperation and the transfer of criminal proceedings (see paragraphs 279-280).

C. Transborder search of computer data banks

261. One very specific transborder situation in relation to computer-related offences deserves particular attention. Within the international economic environment, in particular within multinational corporate structures, data are often stored centrally in one country (e.g. where headquarters are located), with on-line access available to company partners (e.g. subsidiary corporations) operating in the territory of other countries.

262. Criminal investigations in such situations are presented with the problem of how to retrieve the data, as potential evidence, that are stored abroad, when investigating by means of on-line access to that data. The question arises whether the investigating authorities may penetrate the database by direct access, without the intervention, knowledge or agreement of the State in which the data are located. Urgent situations compelling the preservation of evidence may require that data be made readily available or, at least, that they be seized and blocked, thereby securing their evidential value. A suspect with sufficient speed and expertise in the access to and the functioning of the system could otherwise interfere with the data and make them unavailable by, for example, erasing them or transmitting them to another data bank.

263. Traditional means for cooperation between States in criminal cases do exist, in the form of conventional mutual assistance agreements, particularly the procedure of the letters rogatory. This procedure, however, by which a State is requested to undertake an investigation on its own territory on behalf of the investigating State, is highly time-consuming. The investigation of crime in the computer environment requires quicker, more efficient action. Another problem arises when a person, natural or legal, is compelled by the investigating State to produce data located in another State, whether or not they are available by on-line access, even though under the law of the State of storage that person is obliged to secrecy.

264. There is no unanimity today on the solution to these problems. However, the view that the deliberate investigation of on-line data constitutes a violation of the sovereignty of the other State is probably correct, whether it is done by the investigating authorities from the premises of the suspect or from their own terminals. In fact, such access might even be considered in the other State as a form of computer crime, such as unauthorized access.

265. The only explicit rule in international public law relevant to this situation seems to be the non-intervention principle, which historically has been applied only when foreign agents have operated

physically on a State's territory. Nevertheless, the direct penetration of data banks appears very similar to acts of physical intervention by official foreign agents. The analogy is strengthened if the acts of penetration also constitute an offence in the other State. However, some people will probably resist the analogy and accept the legality of this penetration.

266. There is a definite need to address these questions, which are indeed not hypothetical ones, and to find solutions that balance the requirement of quick action with the appropriate respect for the sovereign rights of the other State in matters of police or investigatory action within its territory. States could, therefore, strive to conclude agreements that make direct penetration acceptable only as an exception. Any exception should, in addition, be subject to a number of stringent conditions, such as the following:

1. The freezing of data, by which any further operation on the data is rendered impossible, would be permissible only for preserving the data for evidentiary purposes;
2. The use of this evidence in the investigating State would be subject to the explicit consent of the State where the evidence was stored;
3. The right to penetrate data banks directly would be limited to serious offences only;
4. Sufficient indication must exist that the usual method of mutual assistance would, for lack of rapidity, compromise the search for evidence;
5. Upon commencement of the investigation, a duty would be imposed to immediately inform the authorities of the State being investigated.

267. The problem of on-line transborder searches of computerized data has not been adequately addressed so far. By virtue of not being cooperative acts, such actions do not fall within the traditional category of mutual assistance in criminal matters. However, the appropriate solution is not to view States as having a complete unilateral freedom to act, provided there is no violation of the non-intervention principle by physical interference. This potential area of conflict between States could be solved by a solution based on the principles mentioned above.

D. Mutual assistance in transborder computer-related crime

268. As discussed above, transnational computer crime can be efficiently addressed only if the countries involved agree to provide maximum cooperation in countering it. This cooperation is usually organized by multi- or bilateral conventions may given rise to a number of problems of which States should be aware.

269. First, as for other forms of international cooperation, the requirement of dual criminality may be an issue. Refusal of assistance could be based on the ground that the act in relation to which the request is made is not an offence in the territory of the requested State. Thus there is a clear need to make the substantive criminal law of computer crime correspond from State to State.

270. Even if the dual criminality rule is not an aspect of all incidents of mutual assistance, it is often a requirement in cases of search and seizure, which is a particularly important means of assistance where data are concerned. Double criminality, furthermore, is basic to other common cooperation modes, such as extradition, or other schemes for solving jurisdictional conflicts as discussed above. Unless domestic criminal legislation, as it develops, moves beyond expressions of sovereignty to espousing common principles as agreed among nations, conflicts will not be avoided. Efforts by States to harmonize their domestic laws will prevent conflicts of jurisdiction and, at minimum, will lay the basic groundwork for cooperation.

271. It is, therefore, imperative that States undertake action to achieve this aim. Such action may range from the undertaking of consultations among States prior to enacting domestic legislation; solutions for harmonization, such as recommended guidelines for national legislation; and the elaboration of a convention of substantive law that defines computer crime under international law, including the governing principles in jurisdiction and cooperation.

272. Secondly, a form of mutual assistance rendered to requesting States is the search and seizure of data banks or carriers that store or transmit information. The target of request is not the carrier itself but the intangible specific data. If seizure remains applicable only to physical objects, the carrier is still at issue. The technical storage capacity of such data banks and carriers often far exceeds the volume of content requested by the investigating State. Explicit rules should be elaborated in relation to the surplus of information a data bank or carrier might contain, which would allow the execution of letters rogatorys upon only the targeted data. Notions such as relevance, proportionality and defined purpose should necessarily be included.

273. A final concern relates to potential grounds of refusal, which almost uniformly include the protection of the essential interests of the requested party. Data that relate to the privacy of nationals, including, for example, financial or medical information, could be considered sufficiently sensitive by a State, in its role of protecting its citizens, to be an essential interest. Many computer-related investigations may concern tax fraud or violations of customs, import and export rules, equally subject to the essential public interest qualification. Again, it is to be expected that States interpret their treaty obligations in a practical manner, in a spirit of cooperation and international comity.

E. Extradition

274. Given the potential for multiple territorial and extraterritorial jurisdictions, resolving the resulting jurisdictional conflicts will often require an agreement between States. It is therefore possible that the effective exercise of an agreed jurisdiction will involve extradition, since the State of physical location of the suspect may not necessarily be the appropriate forum for prosecuting the crime.

275. The terms of traditional extradition treaties will remain applicable. Computer crimes do not appear to raise any specific difficulties, provided the requirements of the extradition law and/or treaty are met. The most important issues are the requirement, again, of double criminality, i.e. the impugned conduct would be an offence punishable under the law of both the requesting and the requested State, and the fulfilling of any other conditions that would include computer crime within the category of extraditable offences. This could be accomplished either by setting sanctions for the open formula, e.g. a maximum punishment of a certain number of months, or by including computer crime in the enumerated list of extradition crimes appended to the extradition treaty in question.

276. Both conditions require careful attention in the computer crime area. The first condition highlights once again the absolute need to legislate the substantive law in each State as consistently as possible, thus avoiding loopholes or conflicting interpretations of the requirements of criminality. Currently, there is insufficient international discussion in the definition of computer crime, or at least on the constitutive elements of the most significant criminal behaviour. The efforts of OECD, the Council of Europe and the United Nations have not yet produced conclusive results. Nevertheless, the reports of these bodies contain sufficient indicators to allow States to formulate criminal laws that are consistent with the criminal laws of partner States.

277. The second condition, the extraditable character of the offence, requires an attentive legislative drafting policy. In particular, offences such as unauthorized access to computers or telecommunications facilities are often characterized as minor offences, and penalty scales may not meet the minimum threshold standards of extraditable crimes. Unfortunately, experience shows that transborder hacking cases are common, significantly affecting important transnational economic networks. It might be advisable to consider serious penalties, at least in cases where the hacking affects the international relations of the victim, whether the victim is a legal or physical person or a State. Disregarding the use of extradition or other cooperation methods could seriously hinder the efficiency of the cooperative response to this important and disturbing phenomenon.

278. Other important concerns, not specific to networking but potentially magnified by it, relate to grounds of refusal where the offence for which extradition is requested is, under the law of the requested State, viewed as having been committed in whole or in part within the territory of that State. A second problematic scenario is possible if the invoked ground for jurisdiction is an extraterritorial one but the law of the requested State does not provide such jurisdiction in similar cases. These situations might also create positive or negative conflicts of jurisdiction. The creation of channels of consultation or negotiation on order to solve such conflicts is highly recommended.

F. Transfer of proceedings in criminal matters

279. As mentioned above, the exercise of jurisdiction in transborder cases involves the possibility of competing claims, which may eventually lead to multiple prosecutions and bring about friction between States. The technique of transfer of proceedings offers a rather effective mechanism to solve this problem in a harmonious way. By creating agreements by which one State can waive its jurisdiction rights on favour of another State, conflicting claims can be resolved. The reason for such an initiative, beyond avoidance of jurisdictional conflicts, are the effective administration of penal justice, the interests of the victim and the reintegration of the offender into society. In case where multiple proceedings are pending in two or more States, a provision can be made for compulsory consultation to reach a settlement.

280. Few conventions of this type are force today. The European Convention for the Transfer of Proceedings in Criminal Matters (1972), for example received a limited number of ratifications. However, the United Nations Model Treaty on the Transfer of Proceedings in Criminal Matters (General Assembly resolution 45/118, annex) represents an excellent basis for more effective international cooperation and deserves greater attention. The basic issues, e.g. the issues of double criminality and non bis in idem, remain similar to those in the other cooperation techniques, but again, any problems can be overcome. In the interests of the administration of criminal justice, which includes effective truth-finding and locating the most important or best items of evidence, agreements in this field may very well solve recurring, conflicting claims of jurisdiction while serving the interests of efficiency.

G. Concluding remarks and suggestions

281. In coping with the increase in transborder computer-related transactions, it is clear that a set of solutions elaborated by the international community represents an effective response. The problems predictable in confrontations among different States, whether common to all transborder crime situations or specific to computer crimes, require well-regulated solutions. Whether the problems are related to multiple jurisdiction conflicts, of a positive or negative nature, or to the requirements of mutual cooperation agreements, it is suggested that States should elaborate explicit rules to solve them.

282. Problems of concurrent jurisdiction based on the principle of territoriality are likely to be the most difficult to solve. Criminal law and jurisdictional questions are still integrated in national policy, and the implementation of that policy remains exclusively in the hands of the sovereign State.

283. Rather than seeking a solution through a conventional classification of priorities, a more effective action might be to develop a mechanism for mutual consultation and for allocating responsibilities on a case-by-case basis. A procedure for settling jurisdictional disputes by a body

of experts knowledgeable in both jurisdictional issues and computer crime could also by developed. This could provide a speedy and flexible alternative to existing dispute-resolution mechanism, such as the Council of Europe Convention on Peaceful Settlements of Disputes.

284. It appears to be generally accepted that claims of extraterritorial jurisdiction are subsidiary to primary territoriality claims. Conflicts of extraterritorial jurisdiction should preferably also be settled by cooperative mutual consultation.

285. In the administration of criminal justice in a multi-sovereign environment, different cooperation techniques can be of relevance. Traditional techniques such as extradition or mutual assistance are generally applicable, provided that the basic requirements of double criminality and conditions for extradition are met. States must, therefore, operate with criminal laws that are as consistent as possible. Laws will be consistent only if there has been cooperation with international institutions such as the United Nations, the Council of Europe, the Organization of American States, the British Commonwealth of Nations, OECD and similar groups. The imposition of penalties sufficient to classify international computer crimes as serious offences is also required.

286. In the search and seizure of data, the mass storage of information in data banks and its transmission through carriers may necessitate additional safeguards, with regard to the criteria for limiting acceptable purpose of search and seizure and for determining relevance in the selection of the data.

287. Many key issues could be properly addressed by the more extensive use of, and consequent greater confidence in, a mechanism for transferring criminal proceedings. It would be advisable to develop conventional agreements that offer cooperative avoidance of conflict, mutual assistance and effective administration of justice.

288. Finally, and more specifically, the legality of direct access to computerized data stored abroad, for evidentiary purposes, should be examined to determine the appropriate balance between, on the one hand, preservation of evidence and efficient prosecution, and on the other hand, respect of exclusive sovereign territorial rights. The basis for a valid solution could be found by combining the notion of a right to immediate access to information for the purpose of freezing and conservation, with the requirement that clearance be given by the other State before the frozen data could be used as evidence. Few if any transborder problems in computer crimes will resist solution by appropriate, balanced legal rules. What is fundamental is the political willingness, in a spirit of international cooperation, to tackle a crime that has no frontiers.

VII. CONCLUSION

289. This Manual has attempted to provide a broad overview of the newest forms of computer and computer-related crime. It has exposed the history, extent and complexities of this phenomenon.

The complexities, intrinsic to the technology itself and to the vagaries of human nature, are exacerbated by the inadequacies of current law. The Manual has canvassed the various solutions that have been suggested and proposed some reform initiatives in the legal area. Pertinent issues for security in the electronic environment have been explored. In addition, the use of non-penal methods to combat this problem has been noted.

290. Many groups of experts in the computer and crime-enforcement fields have discussed, and continue to discuss, these issues. The discussions suggest that the phenomenon of computer crime has existed for some time and will not go away. Computer technology today is where automotive technology was in 1905. Significant developments lie ahead. Equally, we have not yet seen the full extent of computer-related crime.

291. Countries must be cognizant of the problem and realize its implications for their own social and economic development. Action must be taken at the national level to address the problem. This first step is not enough, however: computer-related crime is not merely a national problem, but an international one.

292. Given the international scope of telecommunications and computer communications, the transborder nature of many computer crimes and the acknowledged barriers within current forms of international cooperation, a concerted international effort is required to address the problem effectively. Attempts to define computer crime, or at least achieve common conceptions of what is comprises, and to harmonize the procedural processes for sanctioning it have a number of benefits:

1. A growing commonality of technology permits the transnational expansion of large-scale computer networks. This in turn increases the vulnerability of these networks and creates opportunities for their misuse on a transnational basis. Yet, concerted international cooperation can occur only if there is a common understanding of what a computer crime is or should be;

2. The expansion of international trade and commerce raises a concomitant need for laws that will adequately safeguard economic interests and facilitate, stabilize and secure economic activities. Likewise, the increasing computerization of data on the personal characteristics, attributes and socio-economic status of individuals, combined with a growing concern for privacy, engenders a corresponding need for legal protection, not only nationally but internationally;

3. International legal harmonization increases the ability of transnational business and other computer users to predict the legal consequences of criminal misuse of computer systems. Predictability leads to confidence and stability on the international investment market;

4. To the extent that criminal law establishes positive norms of conduct and serves to educate and deter, harmonization of the criminal law facilitates the creation of international norms of conduct for computer usage;

5. Harmonization can help to avert market restrictions and national barriers to the free flow of information and the transfer of technology. Business and Governments may otherwise refrain from

exporting computer programs, data or technology to, or from establishing complex computer interconnections with, countries that do not have an effective system of legal protection;

6. The harmonization of laws, including criminal laws, could promote equal conditions for competition. The inadequate legal protection of computer programs, technology or trade secrets in some countries could cause some companies to operate there in a manner that would be considered by other countries to be unfair competition;

7. Better harmonization can prevent some countries from becoming havens from which international computer crime could be committed with impunity;

8. Harmonization facilitates law enforcement by the agencies of different countries because it provides a common understanding of what types of conduct constitute crime and, in particular, computer-related crime.

9. The harmonization of substantive law facilitates the extradition of alleged or fugitive offenders. Extradition treaties generally require dual criminality, that is, the conduct must be considered to be a crime under the laws of both countries and, sometimes, must be the same type of crime. Accordingly, harmonization of the concept and even the definition of crime can be crucial to the ability to extradite;

10. Harmonization facilitates mutual legal assistance, that is, the use of legally controlled investigatory powers, such as search and seizure, examination of witnesses, electronic surveillance etc., by one country for the benefit of another country. In some mutual assistance treaties, dual criminality is also required before one country will use its judicial or law-enforcement mechanisms to aid another country. Even where dual criminality is not a prerequisite, a common conceptualization of what constitutes a crime assists the law-enforcement and judicial authorities of the country in undertaking investigations within its own territory on behalf of a foreign country;

11. The harmonization of offences facilitates the harmonization of procedural law with respect to investigatory powers.

293. Much remains to be accomplished to achieve international cooperation. Most of the international work so far has been done in just a few regions of the world. The challenge for the future is to expand that cooperation to other portions of the international community. The potential for computer crime is as vast and extensive as the interconnections of worldwide telecommunications networks. All regions of the world, both developed and developing countries, must become involved in order to stifle this new form of criminality. Computer technologies will be increasingly important for developing countries attempting to achieve economic sufficiency. The implementation of security and crime-prevention procedures should be an integral aspect of technological progress in these countries, as should their cooperation in international computer-crime matters.

294. Cooperation in addressing computer-related crime must be developed and improved at both the national and international levels. At the national level, working groups could be established to address the relevant issues. These groups could draw their members from various disciplines and fields, including government, industry and learned societies. They could commence by examining the experience acquired in the field, including the material set forth in this Manual, and by conducting a similar analysis of their own national situations and laws. They could also consider adopting the following measures:

1. Reviewing the present state of legislation in light of the issues raised in this Manual, assessing the substantive and procedural adequacy of their legal and administrative infrastructures and recommending appropriate solutions;

2. Cooperating in the exchange of experience and information about legislation and judicial and law-enforcement procedures applicable to computer crime. This would foster international cooperation and the understanding of common problems;

3. Undertaking a review of sentencing legislation, policies and practices with a view to developing more effective penal sentencing provisions. International cooperation in sentencing reform would ensure the uniform treatment of computer-crime offenders and could prevent computer offenders from relocating to jurisdictions where computer misuse might be treated more leniently;

4. Ensuring periodic reviews and reform of laws, policies and practices in order to incorporate changes arising from technological developments and trends in computer crime;

5. Inviting educational institutions, associations of hardware and software manufactures and the data processing industry to add courses on the legal and ethical aspects of computers to their educational and training curricula, with a view to preventing the misuse of computers and creating ethical standards for the respective sectors;

6. Developing a mechanism to educate potential victims of computer crime and to expose the real extent of computer crime. The active involvement of victims should be encouraged in developing prevention programs and victim assistance programs that are commensurate with the scope of the problem;

7. In view of international character of data-processing and information technology, sharing security standards and procedural techniques among all sectors of the industry, both nationally and internationally;

8. In consultation with groups in other countries, and in order to keep abreast of advances in modern computer crime, consolidating and facilitating law enforcement efforts, including the development of and training in innovative techniques for investigative and prosecutorial personnel;

9. Implementing voluntary security measures by computer users in the private sector;

10. Imposing obligatory security measures in certain sensitive sectors;

11. Encouraging the creation and implementation of national computer security legislation, policies and guidelines;

12. Encouraging management and senior executives to commit their organizations to security and crime prevention;

13. Incorporating and promoting the use of security measures in the information technology industry;

14. Developing and promoting computer ethics in all sectors of society, but especially in educational institutions and professional societies;

15. Developing professional standards in the data-processing industry, including the option of disciplinary measures;

16. Educating the public about the prevalence of computer crime and the need to promote computer ethics, standards and security measures;

17. Promoting victim cooperation in reporting computer crime;

18. Training and educating personnel in the investigative, prosecutorial and judicial systems.

295. At the international level, further activities could be undertaken, including the following:

1. Within regional groups or associations, conducting comparative analyses of substantive and procedural law relating to computer crime;

2. Attempting to harmonize substantive and procedural law among the States of a region by developing guidelines, model law or agreements;

3. When negotiating or reviewing treaties on extradition, mutual assistance or transfer of proceedings, whether bilateral or multilateral, addressing the following issues, taking into account human rights, including privacy rights, and the sovereignty of States:

4. Ensuring a jurisdictional base for the prosecution of transborder, computer-related crime and enacting mechanisms for resolving jurisdictional conflicts;

1. Imposing obligations to extradite or prosecute offenders;

2. Facilitating mutual assistance, particularly regarding synchronized law enforcement, transborder search and seizure and the interception of communications.

296. To ensure that human rights principles, privacy rights and international legal principles are effectively balanced, model treaties on criminal matters, such as those developed by the United Nations, can provide valuable guidelines. The implementation of security and crime prevention measures should be concomitant with technological development. The time to act is now.

ANEXO B

MANUAL PRÁTICO DE INVESTIGAÇÃO

MANUAL PRÁTICO DE INVESTIGAÇÃO

MINISTÉRIO PÚBLICO FEDERAL

PROCURADORIA DA REPÚBLICA NO ESTADO DE SP

GRUPO DE COMBATE AOS CRIMES CIBERNÉTICOS

CRIMES CIBERNÉTICOS

MANUAL PRÁTICO DE INVESTIGAÇÃO

ABRIL DE 2006

REDAÇÃO: Adriana Shimabukuro Kurokawa (técnica em informática – PRSP), Sergio Gardenghi Suiama, Ana Carolina Previtalli Nascimento, Karen Louise Jeanette Kahn e Eduardo Barragan Serôa da Motta (Procuradores da República)

REVISÃO TÉCNICA: Thiago Tavares Nunes de Oliveira, Carla Elaine Freitas, Thiago Oliveira Castro Vieira e Moisés Araújo Machado (Safernet Brasil)

REVISÃO FINAL: Sergio Gardenghi Suiama e Adriana Shimabukuro Kurokawa

GRUPO DE CRIMES CIBERNÉTICOS DA PR-SP: Ana Letícia Absy, Anamara Osório Silva de Sordi, Karen Louise Jeanette Kahn, Sergio Gardenghi Suiama e Thaméa Danelon Valiengo (Procuradores da República), Adriana Shimabukuro Kurokawa (consultora técnica), Fernando Jesus Conceição e Ipólito Francisco Jorge.

PROCURADORA CHEFE: Adriana Zawada Melo

AGRADECIMENTOS: ao Comitê Gestor da Internet no Brasil, a António Alberto Valente Tavares, a Thiago Tavares Nunes de Oliveira e equipe do Safernet Brasil, a Anderson e Roseane Miranda (do *hotline* censura.com.br*)*, a Suely Freitas da Silva e aos ex-estagiários da PR-SP Patrícia Cotrim e Marcelo Chiara Teixeira.

PROCURADORIA DA REPÚBLICA NO ESTADO DE SÃO PAULO

Rua Peixoto Gomide, 768 – Cerqueira César

CEP 01409-904 – São Paulo – SP

Telefone: (11) 3269-5000

Home-page: www.prsp.mpf.gov.br

ÍNDICE

1. APRESENTAÇÃO.

Este manual nasceu de uma necessidade: em meados de 2002, um grupo de Procuradores da República decidiu pedir à Associação Brasileira Multiprofissional de Proteção à Infância e à Adolescência – ABRAPIA que as notícias de *sites* contendo fotografias ou imagens de pornografia infantil fossem encaminhadas diretamente ao Ministério Público Federal para que pudéssemos investigar, de maneira eficaz, essa conduta criminosa. Recebemos daquela organização não-governamental dezenas de endereços de *sites* sediados no Brasil e no exterior, e, naquele momento, percebemos nossa total ignorância a respeito dos meandros da criminalidade cibernética; um mundo quase inacessível para quem, como nós, nasceu no tempo das máquinas de escrever e não sabia nem mesmo o que era um *browser*. Bem, segundo um antigo provérbio latino, a necessidade é a mãe da invenção. O número de investigações relacionadas a crimes cibernéticos é crescente, e é razoável supor que, à medida que novos usuários ingressem na rede e mais pessoas passem a ter o domínio das estruturas básicas do sistema, surjam formas de criminalidade informática para as quais não temos nenhum conhecimento. Foi preciso, então, começar um processo de formação, do qual este manual é apenas um primeiro modesto resultado. Nosso objetivo com a publicação é dividir com os profissionais do direito que participam de algum modo da atividade de persecução penal (delegados, membros do Ministério Público, juízes e auxiliares da Justiça) os conhecimentos que o grupo de combate aos crimes cibernéticos da PR-SP acumulou até agora, apresentando os procedimentos básicos de coleta, preservação da integridade e análise das provas e de identificação dos autores desses crimes. Como os assuntos aqui tratados dizem respeito a técnicas de investigação, é desnecessário lembrar a inconveniência de divulgação mais ampla do manual. O tema da criminalidade cibernética é por demais extenso e as novas tecnologias que surgem a cada dia desafiam os conhecimentos acumulados no presente. Por isso, nossas pretensões com o manual são bastante modestas e se dirigem, principalmente, ao combate dos principais crimes praticados por intermédio da rede mundial de computadores de competência da Justiça Federal brasileira, notadamente a pornografia infantil e os chamados "crimes de ódio" (*hate crimes*). Temos plena convicção de que a efetividade da aplicação da lei penal em relação a esses crimes depende da aquisição de conhecimentos mínimos de informática pelos operadores do direito. Depende, também, de uma postura menos burocrática de nossa parte, já que o tempo da Internet é muitíssimo mais rápido do que o tempo dos órgãos envolvidos na persecução penal. Basta lembrar, a propósito, que a maioria dos provedores de acesso à Internet no Brasil guarda as informações necessárias à investigação dos crimes cibernéticos por apenas três ou quatro meses, em razão do grande espaço de memória exigido para o armazenamento dessas informações. Agradecemos muitíssimo o Comitê Gestor da Internet no Brasil, nas pessoas de Demi Getschko e Hartmut Richard Glaser e o presidente da Associação Brasileira dos Provedores de Acesso, Serviços e Informações da Rede Internet – ABRANET, António Alberto Valente Tavares, pelo apoio e patrocínio da publicação

desta obra. Agradecemos também as Procuradoras-Chefes da Procuradoria da República em São Paulo Elizabeth Mitiko Kobayashi e Adriana Zawada Melo, por terem determinado o suporte necessário às iniciativas desenvolvidas pelo grupo. Aqueles que começam a trabalhar com o assunto cedo percebem as imensas limitações que encontramos para combater a disseminação, na rede mundial de computadores, da pornografia infantil, do racismo, e de outros crimes com alto potencial lesivo. O caráter transnacional do delito, a extrema volatilidade das evidências e o despreparo do sistema de justiça para lidar com essa forma de criminalidade são os principais fatores de insucesso das investigações. Temos consciência de todos esses problemas, e achamos que é hora de compartilhar conhecimentos e multiplicar o número de profissionais preparados para enfrentar a questão. Esperamos que a leitura do manual seja de alguma forma útil. E, desde já, colocamo-nos inteiramente à disposição dos colegas para ajudar no que for preciso. Mãos à obra!

2. COMO FUNCIONA A INTERNET?

No ano de 1962, em pleno auge da Guerra Fria, um grupo de pesquisadores americanos vinculados a uma instituição militar começou a imaginar um sistema imune a bombardeios, que fosse capaz de interligar muitos computadores, permitindo o intercâmbio e o compartilhamento de dados entre eles. Sete anos mais tarde, a primeira versão desse sistema ficou pronta: chamava-se ARPAnet (nome derivado de *Advanced Research Projects Agency* ou Agência de Projetos de Pesquisa Avançada), e sua principal característica era não possuir um comando central, de modo que, em caso de destruição de um ou mais computadores, todos os outros equipamentos ligados ao sistema continuariam operando. O nome "Internet" surgiu décadas mais tarde, quando a tecnologia desenvolvida passou a ser usada para ligar universidades americanas entre si, e depois também institutos de pesquisa sediados em outros países. A idéia central, porém, permaneceu a mesma: uma espécie de *associação mundial de computadores, todos interligados por meio de um conjunto de regras padronizadas que especificam o formato, a sincronização e a verificação de erros em comunicação de dados*. Esse conjunto de regras recebeu a denominação de **protocolo**. A exploração comercial do serviço começou no início da década de 90 e se desenvolveu graças à invenção da *World Wide Web*, um enorme pacote de informações, em formato de texto ou mídia (imagens e arquivos de áudio e vídeo), organizadas de forma a que o usuário possa percorrer as páginas na rede (isto é, "navegar"), a partir de seqüências associativas (*links*) entre blocos vinculados por remissões. Do início da década de 90 até o presente, o número de usuários da Internet explodiu. Em 1990, havia cerca de 2 milhões de pessoas conectadas à rede em todo o mundo. Doze anos mais tarde, esse número passou para 604 milhões (cf. tabela 1). No Brasil, estima-se que o número de usuários da Internet seja de 14,3 milhões.

Tabela 1: Número de usuários da Internet no mundo:

País Usuários da Internet Data da Informação

1 Estados Unidos 159,000,000 2002

2 China 59,100,000 2002

3 Japão 57,200,000 2002

4 Alemanha 34,000,000 2002

5 Coréia do Sul 26,270,000 2002

6 Reino Unido 25,000,000 2002

7 Itália 19,900,000 2002

8 França 18,716,000 2002

9 Índia 16,580,000 2002

10 Canadá 16,110,000 2002

11 Brasil 14,300,000 2002

12 México 10,033,000 2002

13 Austrália 9,472,000 2002

14 Polônia 8,880,000 2002

15 Taiwan 8,590,000 2002

16 Holanda 8,200,000 2002

17 Indonésia 8,000,000 2002

18 Malásia 7,841,000 2002

19 Espanha 7,388,000 2001

Mundo 604,111,719

Fonte: The Cia's World Factbook

Em geral, as informações na *Web* estão agrupadas em *sites*, que são coleções de páginas a respeito de um determinado assunto. Há, hoje, aproximadamente 800 milhões de *sites* publicados na rede. Todos eles podem ser acessados por intermédio de programas de navegação (*browsers*) como o *Internet Explorer,* o *Netscape* ou o *Mozilla Firefox*. O "endereço" que digitamos nesses programas de navegação para acessar algum *site* (por exemplo, www.stf.gov.br) é chamado de **URL**, abreviação de *Uniform Resource Locator*, ou "*Localizador Uniforme de Recursos*". Os endereços da *Web* seguem uma estrutura ordenada, composta por **domínios**. No URL do Supremo Tribunal Federal, por exemplo, após a sigla www, há o nome do *site* (".stf"), um sufixo que indica o tipo de organização (no caso, ".gov"), e duas letras finais para designar o país de origem (".br"). Essas três partes que compõem o endereço eletrônico receberam, respectivamente, a denominação de "nomes de domínio" ou *domain names* (como "google", "yahoo", "uol", "globo")1; "domínios de nível superior" (".gov", ".com", ".edu", ".org" etc.); e "domínios de países" (.br, .fr., .it, .pt etc.). *Sites*

sediados nos Estados Unidos não possuem a extensão final porque, no princípio, a *Web* estava restrita àquele país e não se julgou necessário acrescentar o domínio específico. Os URLs que digitamos nos programas de navegação precisam ser "traduzidos" para um endereço numérico, denominado **"endereço IP"**. Dissemos mais acima que as comunicações entre os computadores conectados à rede são feitas por intermédio de regras padronizadas, chamadas de "protocolos". Pois bem, a abreviação "IP" refere-se justamente a esses protocolos da Internet. Cada *site* ou página que acessamos está hospedado em um computador permanentemente ligado à rede, chamado de *servidor*, o qual é identificado apenas pelo endereço numérico IP. Por exemplo, o URL da Procuradoria da República em São Paulo (www.prsp.mpf.gov.br) é identificada na rede pelo endereço IP 200.142.34.3, que é um número único em toda a rede mundial. A "tradução" dos nomes de 1 No Brasil, o registro dos nomes de domínio é responsabilidade do Núcleo de Informação e Coordenação do Ponto BR - NIC.br, segundo a resolução n.º 001/2005 disponível em <http://www.cgi.br/regulamentacao/resolucao2005-01.htm>. Acesso em 01.03.2006 domínio para um endereço IP é feita por meio de um computador chamado servidor DNS (sigla de *Domain Name System – Sistema de Nomes de Domínios*). Como é sabido, para que um usuário possa "navegar" nas páginas da Internet, e também receber e enviar e-mails, trocar arquivos de áudio ou vídeo, participar de grupos de discussão ou conversar com outras pessoas em *chats*, é preciso que esteja conectado à rede. A conexão é feita por intermédio de um **modem**, ligado a uma linha telefônica ou a um cabo. As concessionárias de telefone comercializam linhas especiais para a Internet, popularmente conhecidas como "banda larga", que utilizam sistemas ADSL (a*symetric digital subscriber* line) ou ISDN (*integrated services digital network*). A conexão com a Internet depende ainda da assinatura de um **provedor de acesso** como UOL, Globo, IG, Terra, AOL, USP, Procuradoria da República. A regulação estatal da atividade desses provedores é mínima, o que dificulta as investigações criminais desenvolvidas no Brasil e, conseqüentemente, contribui para a impunidade de alguns crimes cibernéticos. Para reduzir o problema, as Procuradorias da República de alguns Estados vêm celebrando "termos de compromisso" (anexo III) com os provedores, pelos quais estes se obrigam a preservar os dados dos usuários pelo prazo mínimo de seis meses e a informar a polícia e o Ministério Público, tão logo tomem conhecimento de algum crime cometido em suas páginas. Quando o usuário faz a conexão à rede, recebe um número – o *Internet Protocol* (IP) já referido. Esse número, *durante o tempo de conexão*, pertence exclusivamente ao usuário, pois é graças a ele que o internauta pode ser "encontrado" na rede. **A identificação do IP é o primeiro e mais importante passo para a investigação de um crime cibernético, como veremos adiante**. Convém, desde logo, lembrar que o investigador deve ainda identificar a **hora exata da conexão e o fuso horário do sistema**, pois um número IP pertence ao usuário apenas durante o período em que ele está conectado; depois, o número é atribuído a outro internauta, aleatoriamente.

3. OS CRIMES CIBERNÉTICOS

Muitas coisas podem ser feitas pela Internet. Podemos pagar contas, trocar mensagens, participar de salas de bate-papo, "baixar" arquivos de música, imagem ou texto, comprar produtos, solicitar serviços, acessar *sites* contendo informações sobre todos os assuntos do conhecimento humano. Em todas essas atividades há o risco de encontrar alguém que se aproveita da velocidade e da escala em que as trocas de informações ocorrem na rede para cometer crimes. A "Convenção sobre a Cibercriminalidade", adotada pelo Conselho da Europa em 20012 (anexo V), e aberta à assinatura por todos os países do globo, obriga os Estados a tipificar as seguintes condutas: 1. Infrações contra a confidencialidade, integridade e disponibilidade dos dados e sistemas informáticos: a) acesso doloso e ilegal a um sistema de informática; b) interceptação ilegal de dados ou comunicações telemáticas; c) atentado à integridade dos dados (conduta própria de um subgrupo *hacker*, conhecido como *cracker*); d) atentado à integridade de um sistema; e) produção, comercialização, obtenção ou posse de aplicativos ou códigos de acesso que permitam a prática dos crimes acima indicados; 2. "Infrações informáticas": a) falsificação de dados; b) estelionatos eletrônicos (v.g., os *phishing scams*); 3. I nfrações relativas ao conteúdo: a) pornografia infantil (produção, oferta, procura, transmissão e posse de fotografias ou imagens realistas de menores ou de pessoas que aparecem como menores, em comportamento sexual explícito); b) racismo e xenofobia (difusão de imagens, idéias ou teorias que preconizem ou incentivem o ódio, a discriminação ou a violência contra uma pessoa ou contra um grupo de pessoas, em razão da raça, religião, cor, ascendência, origem nacional ou étnica; injúria e 2 Disponível no site: http://conventions.coe.int/Treaty/FR/Treaties/Html/185.htm. ameaça qualificadas pela motivação racista ou xenófoba; negação, minimização grosseira, aprovação ou justificação do genocídio ou outros crimes contra a humanidade)3; 4. Atentado à propriedade intelectual e aos direitos que lhe são conexos. No Brasil, o projeto de lei n.º 84/99, de autoria do deputado Luiz Piauhylino, buscou dar um tratamento mais sistemático aos crimes cibernéticos. Um substitutivo da proposta foi aprovado pela Câmara dos Deputados em novembro de 2003 e atualmente aguarda a manifestação do Senado. Nossa legislação, porém, não apresenta muitas lacunas em matéria de crimes cibernéticos, havendo, inclusive, tipos penais específicos relativos a essa modalidade de delitos: a) No capítulo dos crimes contra a administração pública, o art. 313-A do Código Penal sanciona a conduta de "inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano"; b) O art. 313-B contém a hipótese de "modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente"; c) A divulgação, sem justa causa, de informações sigilosas ou reservadas contidas ou não nos sistemas de informações ou banco de dados da Administração Pública é sancionada pelo

art. 153, § 1o-A; d) Ao servidor que viola o sigilo funcional, permitindo ou facilitando, "mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública", ou que se utiliza, indevidamente, do acesso restrito, há a incidência das penas previstas no art. 325 do Código Penal; e) A Lei 10.764, de 12 de novembro de 2003, modificou a redação do art. 241 do Estatuto da Criança e do Adolescente para explicitar a possibilidade do crime de 3 A repressão aos crimes de racismo e xenofobia praticados por intermédio de um sistema de informática está prevista, na verdade, no Protocolo Adicional à "Convenção sobre a Cibercriminalidade", de 30 de janeiro de 2003 (disponível no site: http://conventions.coe.int/Treaty/FR/Treaties/Html/189.htm). pornografia infanto-juvenil ser praticado pela rede mundial de computadores. Além disso, previu a responsabilidade criminal daquele que "assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens produzidas" ou "assegura, por qualquer meio, o acesso, na rede mundial de computadores ou internet, das fotografias, cenas ou imagens de pedofilia" (cf. item seguinte); f) Além dos tipos penais que fazem menção explícita à informática, há outros em relação aos quais é possível haver a subsunção de condutas ilícitas executadas por meio da internet: o *cracker*, por exemplo, pode estar incurso no crime de dano, descrito no art. 163 do Código Penal. A prática ou incitação do racismo é reprimida pelo art. 20, *caput* e § 2º, da Lei 7.716/89. O *phishing scam* subsume-se perfeitamente ao delito de estelionato.

3.1. Breves comentários aos crimes do art. 241 do ECA.

É sabido que o desenvolvimento das comunicações e da transmissão de dados à distância tem trazido incontáveis vantagens à humanidade. Os avanços tecnológicos ocorridos nos últimos anos tornaram a Internet uma ferramenta muito versátil e cada vez mais popular, de sorte que, num futuro não muito distante, computadores conectados à rede poderão substituir o papel e outros suportes de dados, como os CDs. Conseqüentemente, nossas vidas serão cada vez mais influenciadas pela tecnologia, revolucionando a percepção e a prática de atividades corriqueiras, tais como a leitura de um jornal, o envio de correspondências ou a audição de uma música. Lamentavelmente, porém, as inovações da Internet vêm acompanhadas de todas as conseqüências do "mau uso" da tecnologia. O notável crescimento da rede mundial de computadores não criou muitas novas condutas antijurídicas, mas amplificou de forma extraordinária o dano causado pelas ofensas já conhecidas: um panfleto racista, no início do século passado, por exemplo, poderia ser lido, no máximo, por algumas centenas de pessoas; na Internet, porém, o mesmo conteúdo está disponível a mais de meio bilhão de pessoas e pode ser encontrado em poucos segundos. O mesmo ocorre em relação à pornografia infantil. O relativo anonimato propiciado pela Internet favoreceu a produção e a distribuição de fotos e vídeos abjetos de crianças e adolescentes em cenas de sexo explícito. Possibilitou, também, que adultos assediem livremente crianças em salas de bate-papo

virtuais, ou encontrem outros adultos portadores da mesma patologia em sites de pornografia ou comunidades de relacionamento. O número de sites de pornografia infantil cresce a cada ano no mundo. Apenas no segundo semestre de 2004, mais de 5000 páginas de pornografia foram denunciadas ao *hotline* mantido pela *Association of Sites Advocating Child Protection* (http://www.asacp.org). Fonte: ASACP (www.asacp.org) No Brasil, algumas organizações da sociedade civil recebem denúncias de pornografia infantil na Internet e as retransmitem para os órgãos envolvidos na persecução penal. A Procuradoria da República em São Paulo mantém convênio com os *hotlines* Safernet Brasil (www.safernet.org.br) e www.censura.com.br e temos obtidos bons resultados com essas parcerias. A conduta de produzir ou distribuir fotografias ou imagens de pornografia infantil está tipificada no art. 241 do Estatuto da Criança e do Adolescente (Lei Federal 8.069/90), cuja redação original prescrevia: Art. 241. Fotografar ou publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente.Pena: reclusão de 1 (um) a 4 (quatro) anos. A despeito de inovador, tal preceito foi considerado tímido para a proteção do bem jurídico, razão pela qual foram apresentadas diversas propostas de alteração legislativa, com o objetivo de assegurar maior efetividade à repressão ao crime de pedofilia. O projeto de lei n.º 3.383/97, por exemplo, tipificava a disponibilidade de acesso de crianças e adolescentes a material com descrição ou ilustração de sexo explícito, pornografia ou violência em rede de computadores. Apesar das infindáveis polêmicas sobre qual das propostas melhor adaptaria a lei penal à criminalidade cibernética de hoje, em especial ao crime de pornografia infantil praticado através da rede mundial de computadores, optou-se por modificar o já existente tipo penal do art. 241, da Lei nº 8.069/90. Isso foi feito pela Lei Federal nº 10.764, de 12 de novembro de 2003, que conferiu ao artigo a seguinte redação: Art. 241. *Apresentar, produzir, vender, fornecer, divulgar, ou publicar, por qualquer meio de comunicação, inclusive rede mundial de computadores ou internet, fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente. Pena – reclusão de 2 (dois) a 6 (seis) anos, e multa. § 1º Incorre na mesma pena quem: I – agencia, autoriza, facilita ou, de qualquer modo, intermedeia a participação de criança ou adolescente em produção referida neste artigo;II – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens produzidas na forma do caput deste artigo; III – assegura, por qualquer meio, o acesso, na rede mundial de computadores ou internet, das fotografias, cenas ou imagens produzidas na forma do* caput *deste artigo. § 2º A pena é de reclusão de 3 (três) a 8 (oito) anos: I – se o agente comete o crime prevalecendo-se do exercício de cargo ou função; II – se o agente comete o crime com o fim de obter para si ou para outrem vantagem patrimonial"*. Com a alteração legislativa, como se vê, o art. 241 do ECA passou a prever expressamente o crime de divulgação e publicação, pela Internet, de imagens e fotografias de crianças e adolescentes em cenas de sexo explícito. É relevante indagar, nesse passo, se o tipo penal abrange também a divulgação de desenhos hiper-realistas de crianças em situação sexual, ou

se a proteção criminal abrange tão somente a transmissão ou publicação de filmes ou fotografias envolvendo crianças "reais". Nos debates parlamentares houve a rejeição de emenda apresentada pelo Deputado Antonio Carlos Biscaia (PT-RJ), que previa a repressão a *"qualquer representação, por qualquer meio, de criança ou adolescente no desempenho de atividades sexuais explícitas ou simuladas"*. Por outro lado, a cabeça do artigo refere-se não apenas a fotografias, mas também a "imagens". Assim, pensamos que desenhos, montagens e composições que retratem crianças em cena de sexo explícito podem, em tese, configurar o crime. É importante mencionar, ainda, que o art. 241, § 1º, do ECA tornou possível a responsabilização criminal dos administradores de provedores de acesso e de hospedagem de páginas, quando estes, dolosamente, *assegurem os meios ou serviços para o acesso ou armazenamento* na rede das fotografias, cenas ou imagens produzidas na forma do caput do artigo. O crime não admite forma culposa, de modo que é preciso comprovar que o responsável pelo provedor tinha ciência da existência de material com tais características em seu sistema informático. A observação é importante porque há provedores de hospedagem gratuita – como o hpG, mantido pelo IG – que armazenam milhares de páginas, não sendo razoável supor que os responsáveis pelo serviço tenham, *a priori*, conhecimento de eventuais páginas criminosas mantidas no provedor. Todavia, uma vez cientes da existência da página, os responsáveis pelo provedor têm o dever de informar a polícia ou o Ministério Público sobre o fato, pena de responderem pelo delito tipificado no art. 241, § 1º, incisos II ou III, do Estatuto da Criança e do Adolescente. Não temos, até o momento, conhecimento de acórdãos que versem sobre as modificações introduzidas pela Lei Federal nº 10.764/03. O Supremo Tribunal Federal, em dois julgados, entendeu que qualquer instrumento hábil a tornar público o material proibido está incluído na compreensão do verbo "publicar", inclusive a Internet (cf. a jurisprudência compilada no anexo I deste manual). A objetividade jurídica do tipo é a integridade física, a liberdade sexual, a dignidade e a honra da criança ou adolescente. Entendemos que o crime é de perigo, havendo, portanto, a incidência do delito, ainda quando não se saiba a identidade da criança ou do jovem retratado. Sujeito ativo do crime tipificado no *caput* do artigo é qualquer pessoa. As condutas descritas nos incisos II e III do § 1º, e no inciso I do § 2º, por sua vez, são delitos próprios, na medida em que só podem ser praticados por determinadas pessoas (aqueles que asseguraram o armazenamento das fotografias ou imagens na Internet e o acesso do criminoso à rede). Em muitos casos, quando a vítima é púbere, não é possível dizer, com a certeza exigida para o ajuizamento da denúncia, que houve a divulgação de imagem de menor de 18 anos. Nesses casos, temos optado por arquivar o procedimento, sem prejuízo do disposto no art. 18 do Código de Processo Penal. O momento da consumação do crime enseja, certamente, muitas dúvidas na doutrina. Entendemos que se o agente mantiver a fotografia ou imagem em uma determinada página eletrônica, o crime será *permanente*. Em contrapartida, se o criminoso remeter a fotografia ou imagem para um destinatário específico, o crime será instantâneo.

4. A INVESTIGAÇÃO DOS CRIMES CIBERNÉTICOS.

Quando recebemos a notícia de um crime cibernético, a primeira providência a tomar é a **identificação do meio usado**: trata-se de a) um *website?*; b) um e-mail?; c) programas de troca de arquivos eletrônicos (do tipo *Kazaa*)?; d) arquivos ou mensagens ofensivas trocados em programas de mensagem instantânea (do tipo *MSN Messenger* ou *ICQ*)?; e) arquivos ou mensagens ofensivas trocados em salas de bate-papo (*chats*)?; f) grupos de discussão (como *yahoo groups*)?; ou g) comunidades virtuais como o *Orkut*? As características de cada um desses meios são diferentes e, por isso, as medidas a serem tomadas são igualmente distintas. De modo geral, podemos dizer que as evidências dos crimes cibernéticos apresentam as seguintes características: a) possuem formato complexo (arquivos, fotos, dados digitalizados etc.); b) são voláteis, i.e., podem ser apagadas, alteradas ou perdidas facilmente; c) costumam estar misturadas a uma grande quantidade de dados legítimos, demandando, por isso, uma análise apurada pelos técnicos e peritos que participam da persecução penal. Como já dito, uma das mais importantes evidências que podemos coletar é o chamado **número IP** (*Internet Protocol*). O número IP é uma identificação que todos os computadores que acessam a Internet possuem; ele aparece no formato A.B.C.D, onde A, B, C e D são números que variam de 0 a 255 (por exemplo, 200.158.4.65). O IP deve estar acompanhado da data, hora exata da conexão ou comunicação e o fuso horário do sistema. Por exemplo: Received: from mailserver.uol.com.br ([**200.143.23.48**]) by mc1- f23.hotmail.com with Microsoft SMTPSVC(6.0.3790.211); **TUE, 1 FEB 2005 05:41:12 (-0800)** Como a Internet é uma rede *mundial* de computadores, os registros indicam a hora local (05:41:12, no exemplo) e a referência à hora GMT (no caso -08:00). Às vezes, é feita apenas a menção à hora GMT (por exemplo, "Tue, 09 Mar 2004 00:24:28 GMT").

Nos pedidos feitos aos provedores de acesso e às companhias telefônicas, é imprescindível que haja, no mínimo, a menção a esses três indicadores: a) o número IP; b) a data da comunicação; e c) o horário indicando o fuso horário utilizado – GMT ou UTC. Sem eles, não será possível fazer a quebra do sigilo de dados telemáticos.

A ilustração abaixo busca representar o caminho básico percorrido pela investigação de um crime cibernético: **Observação importante: antes de tomar qualquer providência a respeito de uma notícia recebida, recomendamos vivamente que o investigador providencie a proteção de seu computador contra ataques digitais.** Há, hoje, mais de 100 mil vírus catalogados pelas empresas de segurança. E não são apenas eles que provocam danos e comprometem a segurança do computador. Há ainda "pragas" como *worms*, *spywares* e "cavalos de Tróia". "*Cavalos de Tróia*" ou *trojans* - à semelhança da invenção mitológica - são programas aparentemente inofensivos que contêm códigos maliciosos capazes de destruir dados armazenados, enviar informações sigilosas e até mesmo permitir que o *cracker* tenha acesso ao computador. *Vírus* são *malwares (softwares* maliciosos) criados com o objetivo de danificar arquivos armazenados no disco rígido

(especialmente arquivos críticos para o funcionamento do sistema), tornando o sistema inoperante. *Worms* são como os vírus, mas têm a capacidade de se propagar para outros computadores. Normalmente, os *worms* geram um aumento considerável no tráfego de dados, prejudicando o acesso aos serviços de rede. Os *worms* constumam se propagar buscando vulnerabilidades em sistemas e em e-mails. Para evitar que seu computador seja danificado, é muito importante manter os programas de proteção permanentemente atualizados e nunca abrir e-mails enviados por remetentes estranhos, sobretudo se estiverem acompanhados de arquivos com extensão ".exe", ".src", ".bat" e ".pif". *Spywares* são programas espiões, usados geralmente com fins comerciais. São instalados quando o usuário recebe algum e-mail, baixa algum arquivo ou navega pela Internet. Uma vez executados, passam a monitorar as páginas acessadas e o que é digitado pelo usuário. As conseqüências de um programa-espião incluem a lentidão no acesso à Internet, a mudança da página inicial do *browser* e a proliferação daquelas pequenas janelas, conhecidas como "*pop-ups*". Nos últimos anos têm ocorrido a proliferação de redes de computadores infectados, conhecidos como *botnets.* Essas redes são criadas para furtar dados, enviar *spams* em larga quantidade, trocar programas piratas e, principalmente, obter vantagens financeiras. Tudo começa com o recebimento de um e-mail falso, supostamente remetido por uma instituição conhecida, como um banco ou órgão governamental (TRE, Receita Federal, Polícia Federal...). Os e-mails contêm arquivos maliciosos anexados ou acessados quando o usuário seleciona um determinado link inserido no texto da correspondência. Aberto o arquivo, um robô (*bot*) é instalado no computador do usuário. Através da Internet, o robô conecta o computador a uma rede (*botnets*) controlada por um *cracker.* Este cibercriminoso pode remotamente controlar as máquinas dos usuários vinculados à rede, obtendo dados como senhas e números de cartões e furtando arquivos pessoais e dados internos do sistema. Essas redes vem evoluindo de forma tão intensa que as operações são realizadas automaticamente, sem a necessidade de intervenção do *cracker*. As vantagens financeiras obtidas pelo *cracker* incluem: venda dos dados de cartão de crédito; aluguel de *botnets* para a realização de ataques DDoS (*Distributed Denial of Service*). Trata-se do envio de muitas requisições simultâneas a um determinado serviço, com o objetivo de torná-lo inoperante. Há registros de *botnets* contendo mais de um milhão e meio de máquinas. Se apenas 10% das máquinas dessa rede, enviarem uma requisição a um serviço ao mesmo tempo, o sistema certamente entrará em colapso; venda de *proxys* abertos, para facilitar a comunicação entre criminosos e o envio de spam; venda de seriais de programas proprietários; roubo de dados pessoais, para pedir posterior resgate a vítima; realização de subtração de valores de contas bancárias de suas vítimas. A proliferação desses robôs é causada pela sua capacidade de buscar novas máquinas para infectar. Ou seja, basta que apenas um computador seja infectado para que os outros computadores da rede fiquem potencialmente vulneráveis. No site www.download.com é possível encontrar antivírus, anti*spywares* (*Ad-Aware* e *Spybot* são dois deles), *firewalls* (veja Zone

Alarm ou OutPost) e outros programas que aumentam a segurança do computador. Muitos desses programas são gratuitos. **Recomendamos que: a) o usuário faça periodicamente a atualização dos programas de seu computador (especialmente do *Windows*); b) instale, em seu micro, um *firewall* (programa que dificulta a invasão de cr*ackers*) e filtros *anti-spam*; c) evite abrir e-mails desconhecidos, especialmente quando façam referência a *links* ou tragam anexados programas ou arquivos; d) crie um e-mail específico para trabalhar com investigações, de preferência vinculado a um provedor estrangeiro (*G-Mail*, *Hotmail, Yahoo* etc.); e) utilize, preferencialmente, uma máquina exclusiva para investigação, evitando o uso de computadores com dados pessoais e de trabalho.** O site http://www.virustotal.com/flash/index_en.html disponibiliza um serviço pelo qual é possível submeter um arquivo suspeito à avaliação. Apresentamos, em seguida, os principais meios eletrônicos sobre os quais podem recair a investigação criminal, e as providências iniciais necessárias à coleta da prova:

4.1. WEBSITES:

4.1.1. Evidências necessárias:

Não é suficiente o endereço URL (exemplo: www.usp.br) para iniciar uma investigação, pois, como dissemos, as evidências nos crimes eletrônicos são voláteis, i.e., podem ser apagadas, alteradas ou perdidas facilmente. Assim, se a *notitia criminis* não estiver acompanhada da página impressa, é preciso, antes de mais nada, providenciar a impressão do *site* ou, melhor ainda, o *download* de seu conteúdo (ver item seguinte).

4.1.2. Salvando o conteúdo inteiro do *site.* Existem aplicativos – por exemplo, o *HTTrack*4 - que permitem o *download* de *sites* inteiros, incluindo textos e fotos publicadas. Utilizar estes aplicativos é um artifício interessante para casos onde o volume de dados é grande. Após o *download*, os arquivos podem ser encaminhados para o órgão competente através de e-mails, disquetes e, se possível, em mídia não-regravável (CD-R). Abaixo apresentamos uma tela do software *HTTrack* fazendo o *download* de um site: O HTTrack, além de permitir o *download* parcial ou total do *site*, também gera um arquivo de *log* (hts_log) registrando a data, hora e endereço do *site* salvo. Essas informações servirão para definir o tempo do crime. Para sistemas Unix e assemelhados (ex: GNU/Linux), o utilitário apropriado para se copiar o conteúdo de um site é o software livre *wget*5. Assim como o HTTrack, esse programa também gera um arquivo de *log*, 4 Gratuitamente disponível no site http://www.httrack.com 5 Página do wget: http://www.gnu.org/software/wget/ além de permitir diversas configurações que auxiliam na investigação. Um exemplo de *download* dos arquivos *.jpg*6 de um site com o wget: investigador@mpf-sp:~$ wget -r -A.jpg http://www.prsp.mpf.gov.br/ --06:13:32--

http://www.prsp.mpf.gov.br/ => `www.prsp.mpf.gov.br/index.html' Resolvendo www.prsp.mpf.gov.br... 200.142.58.20 Connecting to www.prsp.mpf.gov.br|200.142.58.20|:80... conectado! HTTP requisição enviada, aguardando resposta... 200 OK Tamanho: 22,171 (22K) [text/html] 100%[==========>] 22,171 60.93K/s 06:13:53 (60.83 KB/s) - `www.prsp.mpf.gov.br/index.html' saved [22171/22171] Um front-end (interface gráfica) para o wget é o programa *gwget:*

4.1.3. Salvando e garantindo a integridade dos dados (procedimentoideal):

No curso do processo penal, a autenticidade das evidências colhidas pode ser impugnada pela defesa. Para evitar esse tipo de problema, nos casos onde não é possível gravar os arquivos em mídia não-regravável, é importante a utilização de um aplicativo que garanta a integridade dos dados. O MD5Sum7 é um aplicativo de verificação da integridade dos dados; 6 JPG é um formato de compressão de imagem muito comum na *Web* e bastante utilizado na distribuição de pornografia infantil. 7 Pode ser baixado gratuitamente no site: www.md5summer.org. na prática ele garante que os dados que foram gravados no momento da produção da prova não sofreram nenhum tipo de adulteração em todo o trâmite do processo. Tecnicamente, ao criarmos uma cópia de algum arquivo, criamos também sua assinatura baseada no arquivo original. Esta assinatura, em forma de um arquivo, acompanhará a cópia e permitirá que a qualquer momento o destinatário verifique se o arquivo recebido é idêntico ao original.

Como utilizar o *MD5Sum*?

1. Compacte seus arquivos para gerar somente um arquivo .ZIP (é mais fácil gerar a assinatura de um só arquivo do que de todos); 2. Rode o programa MD5Sum para esta cópia gerada; 3. Mande a cópia de seu arquivo zipado, junto com este arquivo adicional criado (assinatura) com extensão .MD5. 4. Com este arquivo (assinatura) o receptor de seu arquivo poderá a qualquer momento rodar o MD5Sum no arquivo recebido e comparar as assinaturas, se forem iguais, o arquivo é autêntico. Abaixo uma tela do MD5Sum criando uma assinatura de um arquivo:

4.1.4. Outras softwares que auxiliam a investigação.

Além dos utilitários que auxiliam na cópia parcial ou integral do *site* investigado existem outras ferramentas capazes de facilitar o trabalho do investigador. Navegadores em modo texto, a exemplo do LYNX8, facilitam a identificação de *links* internos e externos do site investigado. Para identificarmos todos os links contidos na página inicial da Procuradoria da República em São Paulo, utilizamos o comando: lynx --dump www.prsp.mpf.gov.br que retorna o seguinte resultado:

1. LYNXIMGMAP:http://www.prsp.mpf.gov.br/#banner
2. http://www.prsp.mpf.gov.br/

3. http://www.prsp.mpf.gov.br/acessibilidade/acessibilidade.htm
4. LYNXIMGMAP:http://www.prsp.mpf.gov.br/#Map
5. http://www.prsp.mpf.gov.br/digidenuncia.htm
6. http://www.prsp.mpf.gov.br/atuacao/atuacao.htm
7. LYNXIMGMAP:http://www.prsp.mpf.gov.br/#licitacao
8. LYNXIMGMAP:http://www.prsp.mpf.gov.br/#contas
9. http://producao.prsp.mpf.gov.br/news/internews/news_noticias.php
10. http://www.prsp.mpf.gov.br/noticiasindice.htm
11. http://www.prsp.mpf.gov.br/prdc/
12. http://www2.pgr.mpf.gov.br/concurso/concurso-de-procuradores/index_html
13. http://www.pgr.mpf.gov.br/pgr/concursos/servidor/index.htm
14. http://www.prsp.mpf.gov.br/outroslinks/concursos/estagiario.htm
15. http://www.prsp.mpf.gov.br/outroslinks/informes/clipping.htm
16. http://www.prsp.mpf.gov.br/outroslinks/informes/notdefic.htm
17. http://www.prsp.mpf.gov.br/outroslinks/informes/informes.htm
18. http://www.prsp.mpf.gov.br/abnt/abnt.htm
19. http://producao.prsp.mpf.gov.br/plantao/plantaocapital.pdf
20. http://producao.prsp.mpf.gov.br/plantao/plantaointerior.pdf
21. http://producao.prsp.mpf.gov.br/plantao/plantaojuizes.pdf
22. http://producao.prsp.mpf.gov.br//consultaprocessual/consproc_consulta_rapida.php
23. http://www.prsp.mpf.gov.br/acessibilidade/acessibilidade.htm
24. http://www.prsp.mpf.gov.br/
25. http://www.prsp.mpf.gov.br/repensando.pdf
26. http://www.prsp.mpf.gov.br/Templates/procuradoria/organograma/prdc.htm
27. http://www.prsp.mpf.gov.br/audp/audp.htm
28. http://www.prsp.mpf.gov.br/credenc.htm
29. http://www.prsp.mpf.gov.br/procuradoria/municipios.htm

Outra ferramenta bastante útil é um acessório do navegador Mozilla-Firefox, disponível gratuitamente no endereço https://addons.mozilla.org/extensions/moreinfo.php?id=590&application=firefo x. A extensão mostra, na barra de *status* do navegador, o número IP do *site* visitado, e fornece ainda uma série de ferramentas para tratar a informação. 8 http://lynx.browser.org/ Com apenas um clique é possível obter informações importantes, como o país onde a página está sediada e a empresa responsável por sua hospedagem.

4.1.5. Pesquisa de domínios (localizando o responsável por um *site*).

Depois de preservar a prova, o passo seguinte é a identificação do servidor que hospeda a página. Há ferramentas de busca na Internet que fazem esse serviço. É preciso apenas verificar se o *site* é nacional (ou seja, se as letras finais do nome do domínio são "br") ou estrangeiro.

4.1.5.1. Domínios nacionais (".br").

Os sites que ficam sobre a administração do NIC.br são facilmente identificados pela terminação ".br" e podem ser pesquisados pelo site do http://www.registro.br O resultado desta pesquisa pode trazer informações importantes como o nome do responsável administrativo pelo domínio, o contato de incidentes de segurança (responsável pelo Setor de Tecnologia de Informação) e o provedor de *backbone* (empresa que detêm blocos de endereços IPs). Abaixo uma tela contendo o resultado de pesquisa de um *site*:

4.1.5.2. Domínios estrangeiros.

A pesquisa de sites estrangeiros pode ser feita por diversos serviços de WHOIS, dentre eles http://www.arin.net/; http://www.internic.net/whois.html; http://lacnic.net/ e http://www.netoworksolutions.com. Outro serviço muito bom para investigações de sites estrangeiros leva o nome do cínico detetive de Dashiell Hammett: http://www.samspade.org. Veja abaixo um resultado de busca no WHOIS: Caso o site esteja hospedado no exterior, a competência da Justiça e da Polícia brasileiras só estará justificada (e executável) se houver algum vínculo com brasileiros. Por exemplo, há hoje *sites* racistas e nazistas feitos por brasileiros hospedados em provedores na Argentina e nos EUA. Nesse caso, entendemos que é possível a persecução penal no Brasil, remanescendo o problema da identificação da autoria. Se não houver vínculo algum do *site* com o Brasil (ou seja, ele não está hospedado em provedores nacionais e não há indícios da participação de brasileiros no delito) recomendamos que a notícia do fato criminoso seja encaminhada à INTERPOL. Ou, melhor, comunicada a um dos *hotlines* associados à INHOPE - International Association of Internet Hotlines (www.inhope.org), pois a associação filiada se encarregará de informar rapidamente a polícia local.

Dica:

Alguns *sites*, mesmo hospedados em provedores externos, trazem *links* do tipo "contato" ou "webmaster", com a indicação de um endereço de e-mail. Vale a pena pesquisar este e-mail, pois às vezes ele pode indicar algum responsável pelo conteúdo do *site*.

4.1.6. Quebra do sigilo de dados telemáticos.

Feita a identificação do provedor que hospeda a página, qual a etapa seguinte? Depende: a) se o hospedeiro é um provedor conhecido, que hospeda, gratuita ou mediante remuneração, *sites* de

terceiros (por exemplo, “HPG”, “Geocities”, “Terra”); b) se a página está registrada em nome de uma empresa não conhecida. Nessa última hipótese, seria preciso analisar o caso concreto, e verificar se é possível requerer a quebra do sigilo de dados telemáticos sem que o autor da página tome conhecimento disso. Se o provedor que hospeda a página for conhecido (e brasileiro), o investigador deverá requerer, judicialmente (ver modelo no anexo III), a quebra de sigilo de dados telemáticos, para que o hospedeiro forneça uma cópia, em mídia não-regravável (CD-R), das páginas investigadas e também os *logs*, isto é, os registros de criação e alteração da página. É no *log* que encontramos as três informações que nos são necessárias para prosseguir: a) o número IP; b) a data e a hora da comunicação; e c) a referência ao horário, incluído o fuso horário GMT ou UTC. No caso de páginas da Internet, é comum o provedor fornecer uma lista de IP’s e datas. Esta lista indica todas as vezes em que a página foi modificada. Como é possível que mais de um computador tenha sido usado para alterar o conteúdo da página, aconselhamos que o investigador selecione quatro ou cinco “linhas” da lista para, em seguida, formular outro requerimento judicial, desta vez à operadora de telefonia ou cabo.

4.1.7. Localizando o “dono” de um IP.

Como dissemos, o número IP é uma identificação que todos os computadores que acessam a Internet possuem. Essa identificação pode ser estática (i.e., pertence a uma pessoa determinada, por um certo período de tempo) ou dinâmica (aleatoriamente atribuídas a um usuário). Organizações como empresas e universidades normalmente possuem uma faixa de IP’s próprios, e a identificação do usuário depende da política interna de conexão da instituição. Para usuários domésticos, o mais comum é o IP dinâmico, fornecido por uma operadora de comunicação, normalmente, provedores de acesso (UOL, Globo, IG etc.). As informações de quem usava o endereço IP em um determinado dia e horário devem ser buscadas nas operadoras de comunicação. Como, então, saber a qual instituição pedir as informações? É simples: basta repetir as pesquisas mencionadas no item 4.1.5. Por exemplo: a qual empresa pertence o IP 200.153.238.195? Os números IP iniciados com “200” pertencem, geralmente, a concessionárias brasileiras. Digitando o número 200.153.238.195 no *site* www.registro.br9 (no campo “procure um nome de domínio”) descobrimos que o usuário conectou-se à Internet por meio de uma linha fornecida pela Telecomunicações de São Paulo S.A. – TELESP. O próprio *site* já fornece o nome do responsável e o endereço para onde o ofício judicial deverá ser encaminhado. Localizado o provedor de acesso, que pode ser um provedor de Internet, uma organização particular ou uma companhia telefônica, a autoridade policial ou o Ministério Público deverá requerer ao juiz (ver modelo no anexo III) **novo pedido de quebra do sigilo de dados telemáticos**, desta vez para que o provedor de acesso informe as informações do usuário vinculado ao IP, em uma determinada data e horário. A concessionária deverá responder à ordem judicial fornecendo as informações necessárias para a identificação do indivíduo usuário do

IP no momento solicitado, inclusive o endereço físico. De posse dessas informações, o investigador poderá, se entender cabível, requerer a expedição de um mandado judicial, para a busca e apreensão do computador, de disquetes e de outros materiais.9 Outro *site* que possui diversas ferramentas para a localização de responsáveis por um IP
está localizado no endereço http://www.network-tools.com.

Cyber-Cafés, Lan-Houses, Wireless...

É muito comum encontrar *cyber-cafés* e *lan-houses* instalados nas cidades brasileiras. A maioria não mantêm nenhum registro de usuários, o que praticamente impede a investigação de eventuais crimes por eles cometidos, já que não é possível identificá-los. Em algumas cidades e Estados há leis que obrigam esses estabelecimentos a manter um cadastro de seus usuários; é preciso admitir, porém, que o grau de eficácia dessas normas é muito pequeno. Outro problema sério que deverá ser enfrentado nos próximos anos é o uso crescente de sistemas de transmissão sem fio (*Wireless* ou *Wi-Fi*). A tecnologia permite a conexão entre equipamentos de forma simples e fácil, pois os dados são transmitidos através de ondas eletromagnéticas. A maioria dos *notebooks* comercializados nos últimos meses já vem com a facilidade. Apesar das muitas vantagens do sistema (mobilidade, flexibilidade, custo reduzido, instalação simples...), há duas desvantagens que facilitam a prática de crimes: a) a vulnerabilidade a acessos não autorizados; e b) a dificuldade de identificação do computador que acessou a rede, através desse sistema: com efeito, qualquer pessoa que estiver na área de abrangência das ondas emitidas pelo ponto de acesso poderá praticar, anonimamente, toda a sorte de delitos. Considerando que as redes sem fio já estão funcionando em aeroportos, faculdades e cafés nas grandes cidades brasileiras, será preciso encontrar rapidamente formas de tornar o sistema mais seguro. Mais uma vez lembramos que nos requerimentos endereçados aos provedores e concessionárias de acesso deve haver referência expressa: a) ao número IP; b) à data e a hora da comunicação; e c) ao horário GMT.

4.2. E-MAILS.

4.2.1. Evidências necessárias.

Quando a evidência investigada for um *e-mail* (por exemplo, uma mensagem que contenha arquivos com pornografia infantil anexados) é preciso não apenas preservar o conteúdo da mensagem, como também **identificar o cabeçalho do *e-mail*,** ou seja, a parte do e-mail que informa os dados do remetente e do destinatário da mensagem. O objetivo é aquele já mencionado: descobrir o número do IP, a data e a hora da transmissão e a referência à hora GMT. Com a disseminação de vírus que alteram o remetente e com a falha de diversos aplicativos de *e-mails*, os quais permitem o preenchimento do campo "de" (remetente) sem autenticação, nem sempre o

endereço que consta no campo remetente, realmente mostra o verdadeiro autor da mensagem. Daí a importância do cabeçalho do *e-mail* numa denúncia que envolva algum tipo correio eletrônico.

4.2.2. Localizando o cabeçalho do *e-mail*.

Em aplicativos como o *Outlook* ou *Outlook Express*, o cabeçalho de um *e-mail* pode ser acessado abrindo a mensagem e clicando *Alt + Enter*. Outra opção é clicar, com o botão direito do *mouse*, em cima da mensagem recebida e selecionar "Opções". Na parte de baixo da janela aberta, há uma série de informações, agrupadas no título "Cabeçalho de Internet". No *groupwise* (aplicativo utilizado no Ministério Público Federal), podemos localizar o cabeçalho de um *e-mail* abrindo a mensagem e clicando no Menu Arquivo – Anexos – Ver . Selecione o arquivo MIME.822. Nos acessos feitos via Internet – como nos sistemas WEBMAIL e WEBACESS – os provedores costumam trazer opções no MENU que permitem editar e imprimir cabeçalhos de e-mails. Algumas dessas opções aparecem com o título "ver código fonte da mensagem" ou "verificar código completo", ou ainda "mensagem em formato texto". Caso não existam estas opções, basta encaminhar o e-mail para uma outra conta, e usar o Outlook para editar o cabeçalho de e-mail.

4.2.3. Analisando o cabeçalho de um e-mail.

A análise do cabeçalho de um *e-mail* é bastante complexa, mas é graças a ela que é possível identificar o remetente da mensagem. É comum um cabeçalho possuir várias linhas que começam com a palavra "*received*". A palavra marca por quantas estações (ou servidores) a mensagem passou antes de chegar ao destinatário. O parágrafo que interessa é sempre o **último "*received*"10**; é ele quem indica a primeira máquina que originou a mensagem, isto é, o computador do remetente.. Abaixo um exemplo de cabeçalho de e-mail com endereço falso (típico de estação infectada com vírus), mas contendo o IP verdadeiro do remetente. Observe também a data e o horário (incluindo o fuso horário) que o e-mail foi encaminhado: 10 Os "*received"* estão em ordem decrescente, ou seja, o primeiro "*received"* mostrará a máquina mais recente por onde sua mensagem passou. Um outro exemplo de cabeçalho de *e-mail*, que mostra o endereço eletrônico, a data e o horário (apenas GMT):

4.2.4. Localizando o "dono" de um e-mail:

O número IP encontrado deve pertencer a uma operadora de telefonia. Para saber a qual concessionária pertence o número, o investigador deverá executar o procedimento descrito no item 4.1.7. deste manual. Se o número IP pertencer a um provedor de acesso, a providência necessária é aquela do item 4.1.6. Se não foi possível localizar o número IP que originou a mensagem, mas há o endereço eletrônico do remetente (exemplo: joaodasilva@terra.com.br), a autoridade policial ou o membro do Ministério Público podem requerer judicialmente a quebra do sigilo de dados

telemáticos para que o provedor do e-mail (no exemplo, o Terra) forneça o número IP da máquina que autenticou esta conta, na data e horário do e-mail remetido (ver modelo anexo). Caso queiram uma abrangência maior, poderão pedir a relação de todos os IPs gerados no momento de autenticação da conta, num determinado período (um mês, por exemplo). Se o provedor do e-mail não estiver sediado no Brasil (exemplos: xxxxxxxx@*hotmail.com* ou xxxxxxxx@*yahoo.com*), o investigador encontrará dificuldades para obter as informações necessárias ao prosseguimento das investigações. O provedor de *e-mails Hotmail*, um dos mais populares do mundo, é mantido pela *Microsoft*. A empresa possui uma filial brasileira, sediada em São Paulo e, em reunião com o Ministério Público Federal de São Paulo, disse que, "a título de colaboração", encaminha as ordens judiciais de quebra de sigilo de dados telemáticos à sua matriz americana, para atendimento. Nem sempre, porém, esse atendimento é feito com presteza. Além disso, a empresa não faz interceptações de dados telemáticos (o "grampo" de e-mails), pois alega que a legislação americana não autoriza essa medida. Sugerimos que as ordens judiciais de quebra de sigilo de dados telemáticos continuem a ser enviadas às filiais nacionais desses provedores.

4.2.5. Interceptação de e-mails.

Medida muito útil para identificar os autores de um delito cibernético e também para comprovar a materialidade delitiva, a interceptação de dados telemáticos está prevista na Lei 9.296/96. Os requisitos, prazo e procedimento da interceptação de dados telemáticos são os mesmos aplicáveis à interceptação das comunicações telefônicas. Sugerimos que o Ministério Público ou a autoridade policial requeiram a criação de uma "conta-espelho", isto é, uma conta de *e-mail* que contenha todas as correspondências eletrônicas recebidas e enviadas pelo usuário investigado. Com essa providência, a autoridade responsável pela investigação poderá monitorar, em tempo real, as comunicações eletrônicas feitas pelo usuário investigado. Sugerimos, ainda, que o provedor seja compelido a entregar, ao final da interceptação, uma mídia não-regravável
(CD-R) contendo todos os e-mails recebidos e enviados, eventuais arquivos anexados e todos os *logs* gerados no período (ver modelo anexo).

"Pescando" o criminoso com um e-mail "isca".

Quando dispomos apenas de um endereço eletrônico fornecido por um provedor estrangeiro, a identificação do usuário pode ser muito difícil. Um expediente simples, mas algumas vezes eficiente, é o envio de um *e-mail* "isca" ao usuário que se pretende identificar. O objetivo da isca é obter uma resposta eletrônica do investigado, pois será a partir dela que a identificação do usuário poderá ser feita (ver item 4.2). Numa investigação de um crime de racismo, por exemplo, o investigador poderá se mostrar interessado nas idéias divulgadas pelo autor da mensagem racista, e solicitar dele mais informações. É óbvio que a linha telefônica usada para enviar o e-mail isca não

pode pertencer a um órgão envolvido na persecução penal (pois o destinatário tem, como vimos, condições de identificar o provedor e a concessionária de telefonia usados pelo remetente); e também é evidente que o e-mail "isca", do remetente deve ser criado com essa finalidade específica e pertencer, de preferência, a um provedor estrangeiro (o próprio *Hotmail*, por exemplo), para dificultar a identificação.

4.3. SOFTWARES P2P (*KAZAA*, *E-MULE*, *E-DONKEY* ETC).

As conexões "peer-to-peer" (ponto-a-ponto) não possuem um provedor central de conexão: elas utilizam diversos servidores independentes e espalhados pela rede. Os arquivos trocados ficam armazenados nas estações dos usuários que participam da "rede", os servidores apenas fazem a "ponte" entre a pessoa que disponibiliza o arquivo e aquela que o quer baixar. A estrutura garante a anonimidade dos usuários e servidores que participam da troca. A tecnologia P2P é usada nos aplicativos *Kazaa*, *GnuTella*, *e-Donkey*, *AudioGalaxy*, *Morpheus* e *BitTorrent*, dentre outros, para trocar arquivos de música (MP3), vídeo e imagem. As gravadoras alegam que a prática viola direitos autorais. Há a possibilidade de troca de qualquer tipo de arquivos, inclusive filmes e imagens contendo pornografia infantil.

Novas versões do Kazaa impedem rastreamento

Novas versões independentes do Kazaa, software de compartilhamento de arquivos, impedem o rastreamento de seus *downloads*. As versões são o Kazaa Lite 2.4.0 e o Kazaa K+++ 2.4.0 e prometem bloquear qualquer tipo de tentativa de rastreamento de seus *downloads*. Os autores criaram opções para desabilitar funções que permitem que um usuário veja todos os arquivos pertencentes a outros, sem contar que não salvam o histórico das pesquisas realizadas. A autenticação de um usuário é feita por servidores gerenciados, normalmente, por comunidades anônimas, sediadas em países que não adotam legislações rígidas de uso da Internet. Os registros dos *logs* gerados, por serem imensos, não são armazenados. Além disso, na prática, quando um servidor P2P é fechado, outros rapidamente são criados, em qualquer parte do mundo. Abaixo uma tela do software KAZAA, disponibilizando e procurando novos arquivos: Infelizmente, o rastreamento das trocas de arquivos entre usuários desses sistemas é bastante difícil. Uma alternativa pode ser a identificação de um arquivo disponível em um computador de um usuário. O processo pode ser demorado, pois as indicações normalmente são vagas (como o simples nome do arquivo ou algumas palavras-chave pelas quais ele pode ser encontrado). É preciso, ademais, aguardar que o usuário denunciado faça a conexão à rede e disponibilize o arquivo para todos. Uma vez localizado, o arquivo deve ser baixado para um computador onde possa ser analisado. Uma vez constatado o delito pode-se utilizar os dados colhidos durante a transferência para localizar o usuário e identificar seu IP (e ainda ter a hora da conexão já que o arquivo foi baixado em ambiente

controlado). Algumas redes P2P são construídas de forma a garantir o anonimato do usuário, o que praticamente impede a identificação do criminoso sem que haja a colaboração do servidor.

4.4. MENSAGENS INSTANTÂNEAS (ICQ, MSN MESSENGER ETC.).

Os programas de mensagens instantâneas surgiram em 1996, com o ICQ, aplicativo criado pela empresa israelense *Mirabilis*. A idéia básica era (e ainda é) tornar mais ágil a comunicação entre os usuários da rede. A vantagem desses programas, em relação aos aplicativos de *e-mail*, é que eles permitem saber se um interlocutor qualquer está *online* e, com isso, trocar mensagens em tempo real. Depois do ICQ, outros programas semelhantes surgiram. O provedor americano *America Online* criou o AIM (*AOL Instant Messenger*), mas depois acabou comprando a *Mirabilis*, fabricante do ICQ. A Microsoft e o Yahoo também lançaram seus produtos. Feita a assinatura do serviço (gratuita), o usuário recebe um código que o identificará dentro da rede de usuários daquele programa de mensagens instantâneas. O código pode ser um número, um apelido ou um endereço de e-mail, dependendo do programa usado. Depois de instalado o programa e configurada a conta, o usuário está apto a se comunicar com outras pessoas que assinam o mesmo serviço, desde que previamente cadastradas pelo usuário. Quando um usuário tenta se comunicar com um contato de sua lista, o programa avisa o destinatário (por meio de um som ou de ícone) de que existe uma mensagem para ele. Uma janela, então, é aberta, e os interlocutores iniciam o diálogo.

4.4.1. Evidências necessárias.

Se a notícia do fato criminoso fizer referência a esses programas, o denunciante deverá providenciar a impressão ou salvar os dados de algum conversa ou do conteúdo da mensagem, e também dos dados dos interlocutores (números identificadores, apelidos ou *e-mail*), e ainda anotar a data e horário da comunicação. Abaixo uma tela do MSN Messenger com uma tela de *chat* aberta:

4.4.2. Localizando o interlocutor de um “instant messenger”.

Antes de qualquer coisa é preciso verificar a forma como o aplicativo faz a autenticação na rede. Se for o ICQ, há um número, chamado UIN (*Universal Internet Number*). O *MSN* e o *Yahoo Messenger* utilizam um endereço de e-mail para fazer a autenticação na rede. Para localizar o e-mail de um usuário do MSN Messenger, selecione o nome ou apelido do mesmo, clique com o botão invertido do mouse e localize a opção “propriedades”. Será aberta uma janela contendo o e-mail e dados do usuários do MSN.

De posse do UIN (ou do e-mail de autenticação) é preciso entrar em contato com o provedor do programa (o ICQ é mantido pela *American OnLine*; o MSN, pela *Microsoft*, o *Yahoo Messenger*, pela *Yahoo*) e solicitar o IP usado na data e horário anotados. Com o IP em mãos, localiza-se o

provedor (ou operadora de telefonia) e solicita-se a ele os dados do usuário. O procedimento é o mesmo que aquele descrito nos itens 4.1.6 e 4.1.711.. Existem ferramentas de rastreamento e localização de IP's em aplicativos de Mensagens Instantâneas, mas os mesmos só podem ser usados quando a conversa está ocorrendo em tempo real, ou seja, é necessário estar com uma conexão ativa com o suspeito durante esta coleta de informação. 11 Sobre a Microsoft, ver a observação do último parágrafo do item 4.2.4.

4.5. **SALAS DE BATE-PAPO (*CHATS*).**

As salas de bate-papo são uma outra forma de conversar com alguém, em tempo real, pela Internet. Os aplicativos mais novos permitem a criação de "salas virtuais", nas quais os usuários podem trocar mensagens e arquivos. Essas "salas" ficam hospedadas na própria *web*, diversamente do que ocorre com os programas de *messenger*. Não é necessário, por isso, fazer o *download* de aplicativos específicos: basta que o usuário forneça seu nome ou apelido (*nickname*). Temos recebido notícias de adultos que usam as salas de batepapo disponibilizadas pelos grandes provedores nacionais para atrair e seduzir crianças, ou, então, para trocar fotos e vídeos contendo pornografia infantil. Para combater esse tipo de crime, a polícia inglesa desenvolveu um programa de detecção de pedófilos em salas de *chat*, apelidado justamente de "*chatnannie*". O programa usa recursos da inteligência artificial para "entrar" em uma sala de bate-papos e dar a impressão de que a conversa se realiza com uma criança; ao mesmo tempo, o aplicativo analisa as respostas e o comportamento do interlocutor e informa as autoridades policiais, caso haja alguma conversa "suspeita".

4.5.1. Evidências necessárias.

Quando o usuário tomar conhecimento de um delito eletrônico praticado em uma sala de bate-papo, deverá salvar ou imprimir o conteúdo da conversa, e também anotar todos os dados disponíveis sobre o *chat*, tais como o *site* onde o serviço funciona, o nome de sala, os *nicknames* usados e a data e a hora em que houve a conversa. Nos *chats* que permitem a troca direta de imagens, recomendamos que o usuário capture os dados da imagem, clicando em cima dela com o botão invertido do mouse e escolhendo a opção "propriedades". Imprima ou salve esta tela e anexe-a aos outros dados coletados. Apresentamos, abaixo, uma tela que contém os dados de uma imagem trocada num *chat*:

4.5.2. Identificando o autor de uma mensagem em um *chat*.

Provedores nacionais com maior estrutura de armazenamento, costumam manter *logs* dos *chats* ocorridos em seu domínio. De posse do apelido do investigado e da data e do horário em que ocorreu a conversa, a autoridade policial ou o Ministério Público deverá requerer judicialmente a quebra do sigilo de dados telemáticos, para que o provedor forneça o IP gerado quando do acesso

do investigado na sala de bate-papo. O procedimento é o mesmo que aquele descrito nos itens 4.1.6 e 4.1.7.

4.6. LISTAS DE DISCUSSÃO.

As listas (ou grupos) de discussão – hospedadas, por exemplo, no "Yahoo! Groups" ou no "Grupos.com.br" - utilizam o e-mail para a troca demensagens entre os integrantes de um determinado grupo temático. Existem milhares de listas hospedadas na Internet, sobre os mais variados assuntos, alguns deles criminosos (grupos nazistas, por exemplo). Para participar de um grupo, o usuário deverá assinar a lista e acompanhar a discussão apenas como leitor ou contribuindo com comentários. Alguns grupos são moderados, isto é, contam com uma pessoa que decide quem participará da lista e quais as mensagens poderão ser publicadas. Como o meio utilizado por essas listas para a troca de mensagens é o endereço eletrônico, a investigação deve seguir os passos descritos no item 4.2., ou seja, o usuário deverá localizar o cabeçalho de email do responsável por alguma mensagem e deste localizar o IP de origem da mensagem.

4.7. ORKUT.

O ORKUT (www.orkut.com) é uma comunidade virtual de relacionamentos, criada em 22 de janeiro de 2004 e mantida pela empresa GOOGLE. Possui atualmente mais de 13 milhões de membros, sendo 72% deles brasileiros. Comparando com os dados fornecidos pelo Comitê Gestor da Internet no Brasil12, podemos concluir que de cada 10 internautas brasileiros, 3,1 estão cadastrados no Orkut. Apesar da empresa mantenedora do serviço proibir o cadastro de menores de idade, há dezenas de milhares de crianças e adolescentes inscritos na comunidade de relacionamentos. Infelizmente o ORKUT vem abrigando centenas de subcomunidades criminosas, nas quais é possível comercializar drogas, divulgar idéias intolerantes e encontrar pornografia infantil. A maioria das notícias que temos recebido referem-se a comunidades racistas e nazistas. Até julho de 2005, a empresa americana Google não possuía filial no Brasil, o que dificultava imensamente a identificação de usuários criminosos. Após diversos "convites" não atendidos, o representante legal da empresa finalmente resolveu colaborar, e desde março de 2006 temos encaminhado à Justiça Federal pedidos de quebra de sigilo de dados telemáticos, para a obtenção dos dados cadastrais, logs de acesso, e cópias em papel e em meio magnético dos perfis e comunidades investigados. Também propusemos à empresa a assinatura de um termo de compromisso semelhante ao já celebrado com os provedores de acesso.

4.7.1. Evidências necessárias.

12 Segundo o CGI-BR cerca de 32,2 milhões de brasileiros com mais de 16 anos tem acesso a internet. http://www.nic.br/indicadores/usuarios/tab02-05.htm Os crimes no serviço Orkut podem ser praticados nas comunidades virtuais e nas páginas contendo os perfis dos usuários. São exemplos da segunda situação a publicação de perfis falsos, com conteúdo difamatório, e a veiculação, nos álbuns associados aos perfis, de imagens e fotografias de crianças em cenas sexuais. As comunidades virtuais são usadas para reunir usuários com as mesmas preferências, sejam elas lícitas ou ilícitas. A cada dia, são criadas centenas de novas comunidades temáticas, muitas delas com o fim de disseminar a intolerância, em todas as suas manifestações. Quando o usuário tomar conhecimento de uma conduta criminosa praticada em ambientes do serviço Orkut, deverá salvar ou imprimir o conteúdo da comunidade, mensagem ou imagem ofensiva, e também da página inicial do usuário responsável por aquele conteúdo.

4.7.2. Identificando o autor de um crime praticado no Orkut.

De posse das evidências acima referidas, o investigador deverá requerer judicialmente a quebra do sigilo de dados telemáticos, para que a empresa GOOGLE BRASIL, responsável pelo serviço, forneça os logs de acesso, e cópias em papel e em meio magnético dos perfis e comunidades investigados (os dados da empresa estão no anexo II). O procedimento é o mesmo que o descrito nos itens 4.1.6 e 4.1.7.

4.8. PROXY.

Até agora, tratamos das operações usuais de acesso à Internet, mas é necessário dizer que nem sempre o usuário realiza a conexão direta com o website, cliente de e-mail, salas de bate-papo e os demais serviços disponíveis na rede mundial. Com efeito, o usuário pode optar por utilizar um método de acesso indireto, que funciona da seguinte maneira: o usuário se conecta a um servidor específico, que lhe serve de "ponte" para acessar o verdadeiro conteúdo desejado. O servidor conectado utiliza um IP próprio e "esconde" o IP original do usuário, de forma que toda mensagem que chega no servidor é redirecionada a usuário e toda mensagem que parte do usuário é identificada apenas pelo IP do servidor. Este tipo de serviço chama-se *Proxy*. Para nós, o maior problema é que há na Internet13 servidores Proxy que garantem ao usuário o anonimato do IP de acesso, e ainda muitos programas gratuitos para fazer as configurações necessárias à utilização dessa forma de acesso indireto à rede. Há ainda a possibilidade do usuário se utilizar de múltiplos servidores Proxy, de forma a dificultar ainda mais o 13 Uma lista deles pode ser obtida nos endereços www.publicproxyservers.com e www.stayinvisible.com – horário do acesso 22:41 27/02/06 -3:00 GMT. rastreamento.

De todo o modo, a identificação do usuário depende da colaboração dos servidores Proxy envolvidos. Abaixo, a tela de um serviço Proxy que promete anonimato ao usuário:

A real função dos servidores de Proxy

Os servidores Proxy não se prestam, apenas à prática de crimes. A maioria deles busca legitimamente "esconder" o IP do usuário, a fim de protegê-lo contra técnicas maliciosas de invasão, roubo de dados e envio de spams. O Proxy serve também para negar ao usuário o acesso a listas de IPs bloqueados (é o que ocorre na maioria das máquinas ligadas à rede MPF) e para armazenar cópia de sites, de forma a facilitar o acesso pelo internauta.

5. COMPETÊNCIA JURISDICIONAL NOS CRIMES CIBERNÉTICOS.

Como vimos no item 3, são muitas as condutas delituosas que podem ser praticadas por meio da Internet. É preciso, então, definir quais os tipos penais estão sujeitos ao processamento e julgamento pela Justiça Federal. Nos termos do artigo 109, inciso IV, da Constituição brasileira, compete aos juízes federais processar e julgar os crimes cometidos em detrimento de bens, serviços ou interesses da União, suas entidades autárquicas ou empresas públicas. Assim, é competência da Justiça Federal julgar os crimes eletrônicos praticados contra os entes da Administração Federal indicados nesse inciso. Podemos citar, a título exemplificativo, o estelionato eletrônico14, o dano ou a falsificação de dados constantes em sistemas informatizados mantidos por órgão ou entes da administração pública federal. Quanto à hipótese prevista no inciso V do artigo 109 da Constituição, ou seja, os crimes previstos em tratado ou convenção internacional, quando iniciada a execução no país o resultado tenha ou devesse ter ocorrido no estrangeiro, vale lembrar que as condutas tipificadas no artigo 241 do Estatuto da Criança e do Adolescente e também o crime de racismo (tipificado na Lei 7.716/89) têm previsão em convenções internacionais de direitos humanos. Como a consumação delitiva normalmente ultrapassa as fronteiras nacionais quando os dois crimes são praticados através da Internet, a competência para julgá-los pertence à Justiça Federal. No que tange à pornografia infantil, o Decreto Legislativo nº 28, de 24.09.90, e o Decreto Presidencial nº 99.710, de 21.11.90, incorporaram ao direito pátrio a *Convenção da ONU sobre os Direitos da Criança*. A Convenção obriga os Estados-Partes, dentre outras medidas, a: a) dar proteção legal à criança contra atentados à sua honra e à sua reputação (art. 16); b) tomar todas as medidas que forem necessárias para proteger a criança contra todas as formas de exploração e violência sexual, inclusive para impedir que seja explorada em espetáculos ou materiais pornográficos (art. 34). Ressalte-se que referida Convenção prevê expressamente o comprometimento dos Estados em adotar medidas de natureza legislativa para a proteção dos direitos da criança (art. 4º). A competência da Justiça Federal para processar e julgar a divulgação na Internet de material pornográfico envolvendo crianças e adolescentes já foi reconhecida por

quatro Tribunais Regionais Federais (1ª, 3ª, 4ª e 5ª Regiões) brasileiros. As ementas dos acórdãos estão no anexo I deste manual. Esses acórdãos reconheceram presente o requisito da extraterritorialidade, uma vez que a visualização de imagens de pornografia 14 Recebemos, uma vez, a notícia de que uma advogada transmitia, pela Internet, declarações de imposto de renda ideologicamente falsas, com o objetivo de receber, em nome de "laranjas", restituições indevidas de imposto de renda. Trata-se de um caso evidente de estelionato eletrônico, praticado contra a Receita Federal. infantil publicadas na Internet pode, virtualmente, ocorrer em qualquer país do mundo. Também está sujeito à competência da Justiça Federal o crime de racismo, tipificado na Lei Federal n.º 7.716/89, já que a discriminação racial é prática vedada pela *Convenção sobre a eliminação de todas as formas de discriminação racial*, ratificada pelo Brasil em 1968 e vigente no território nacional a partir da edição do Decreto Presidencial n.º 65.810, de 8.12.1969. A Convenção obriga os Estados-partes a: *a)* não encorajar, defender ou apoiar a discriminação racial praticada por uma pessoa ou uma organização qualquer (art. 2º, § 1º, "b"); b) tomar todas as medidas apropriadas, inclusive, se as circunstâncias o exigirem, medidas de natureza legislativa, para proibir e pôr fim à discriminação racial praticada por quaisquer pessoas, grupo ou organização (art. 2º, § 1º, "d"); c) declarar, como delitos puníveis por lei, qualquer difusão de idéias baseadas na superioridade ou ódio raciais, qualquer incitamento à discriminação racial, assim como quaisquer atos de violência ou provocação a tais atos, dirigidos contra qualquer raça ou qualquer grupo de pessoas de outra cor ou de outra origem étnica, como também qualquer assistência prestada a atividades racistas, inclusive seu financiamento (art. 4º, "a"). Portanto, os chamados "crimes de ódio", quando praticados por meio da Internet, também são da atribuição da Justiça Federal. Outros delitos não abrangidos pelas hipóteses acima mencionadas – por exemplo, os crimes contra a honra de particular, praticados através da rede - deverão ser investigados e processados no âmbito das Justiças Estaduais, já que o simples fato do crime ter sido cometido por meio da Internet não é suficiente para justificar a competência da Justiça Federal.

6. A RESPONSABILIDADE DOS PROVEDORES.

A legislação brasileira sobre a responsabilidade dos provedores no enfrentamento aos crimes cibernéticos é manifestamente deficiente, uma vez que não há, em nosso ordenamento, a definição clara dos deveres das empresas que mantém serviços de acesso e hospedagem de páginas em matéria criminal. Em países mais empenhados no combate à essa modalidade delitiva - como por exemplo Holanda, Suécia, Austrália e Canadá – os governos estão exigindo dos provedores que informem a polícia ou o Ministério Público tão logo tomem conhecimento de crimes cometidos no uso dos serviços de Internet, e também que preservem as evidências necessárias à investigação criminal, por um prazo mínimo estabelecido por lei. Como já vimos, a identificação de um criminoso cibernético depende, em grande medida, da identificação do endereço IP do computador

por ele utilizado. Um provedor de acesso normalmente controla uma gama de centenas ou milhares de endereços de IP, os quais são atribuídos aos assinantes, durante o período de conexão. Os números de IP são normalmente dinâmicos, ou seja, cada vez que um usuário faz a conexão à rede por meio de um provedor de acesso, seu computador é aleatoriamente vinculado a um endereço de IP, disponibilizado pelo provedor. O computador do usuário retém o endereço de IP pela duração da conexão, impedindo que o mesmo protocolo seja atribuído a outro assinante, no mesmo período. Quando, porém, o usuário encerra a conexão, o protocolo torna-se novamente disponível para ser atribuído a outro assinante. Assim, um endereço de IP de dado usuário normalmente difere a cada vez que ele se conecta por meio de algum provedor, e um dado endereço de IP poder estar associado a centenas ou milhares de diferentes usuários por um período de semanas ou meses. Para que seja possível identificar qual usuário estava ligado a determinado endereço de IP, num determinado dia e hora, os provedores de acesso e também de hospedagem devem manter um banco de dados eletrônico, uma lista de cada endereço de IP utilizado, juntamente com a correspondente data, horário e região de conexão. A *International Association of Prosecutors* recomenda que os provedores mantenham os *logs* de acesso pelo prazo mínimo de um ano, de forma que, quando forem formalmente requisitados, tenham disponível a informação de interesse do órgão solicitante, inclusive para instruir os casos envolvendo cooperação internacional, em cujo âmbito as investigações demandam maior tempo para sua conclusão. É indispensável que os provedores proporcionem, ainda, a educação necessária ao uso responsável da Internet. É cada vez mais precoce o uso, pelas crianças, da rede mundial de computadores, sendo certo que elas estão muito expostas ao assédio de criminosos. Considerando, ainda, que a repressão penal é insuficiente para coibir as práticas nocivas mais comuns da Internet, é imprescindível que os provedores assumam a responsabilidade de informar corretamente os consumidores de seus serviços acerca dos mecanismos de proteção contra ações danosas. Como já foi dito, a Lei 10.764/03 previu explicitamente a responsabilidade criminal dos administradores e empregados de pro*vedores, quando estes: a) assegurarem os meios ou serviços para o armazenamento das fotografias ou imagens de crianças ou adolescentes em cena de sexo explícito; b) assegurarem, por qualquer meio, o acesso, na rede mundial de computadores ou Internet, das fotografias, de tais cenas ou imagens.* À míngua de uma legislação mais abrangente, algumas unidades do Ministério Público Federal – incluindo a nossa - têm celebrado "termos de compromisso" com os provedores locais, objetivando fazer com que eles: a) divulguem campanhas contra a pornografia infantil e contra os crimes de ódio; b) orientem o público sobre a utilização não criminosa de salas de bate-papo, grupos e fóruns de discussão, *blogs*, páginas pessoais e outros serviços disponibilizados ao usuário; c) insiram, nos instrumentos de adesão ao serviço, cláusula que preveja a rescisão do contratual na hipótese do usuário valer-se do provedor para veicular fotografias e imagens de pornografia infantil, ou idéias preconceituosas quanto à origem, raça, etnia, sexo, orientação sexual, cor, idade,

crença religiosa ou outras formas de discriminação; d) mantenham *link* pelo qual os usuários possam noticiar ao provedor signatário as condutas referidas neste termo, quando praticadas em ambiente, página, grupo de discussão, álbum eletrônico, ou outro serviço prestado pelo próprio provedor; e) informem imediatamente ao Ministério Público Federal, quando tomem conhecimento de que abrigam pornografia infantil ou conteúdo manifestamente discriminatório, assegurada a proteção ao sigilo dos dados telemáticos; f) preservem e armazenem, pelo prazo mínimo de 6 (seis) meses, o registro de *logs* de acesso discado e, quando possível, também os IPs originários dos usuários dos serviços de *web page*, salas de bate-papo, *fotologs*, fóruns de discussão *on-line* e outros. g) solicitem e mantenham os dados cadastrais informados por seus assinantes de acesso; h) exijam que os novos usuários informem o número de algum documento validável de identificação, como por exemplo o número do RG ou do CPF. Como se vê, o objetivo do termo é comprometer os provedores no combate aos crimes de pornografia infantil e racismo, quando cometidos através da Internet. Inclusive sob o aspecto ético, a responsabilidade dos provedores em zelar pela não disseminação de tais práticas é algo incontestável, visto que, uma vez hospedando conteúdos de pornografia infantil, os provedores contribuem, em muito, para o convencimento do público em geral, inclusive crianças, muitas delas já usuárias da Internet, de que a pornografia infantil e a exploração sexual de crianças e adolescentes é algo natural, divertido e prazeroso. Nesse sentido, a cooperação entre os Provedores de Acesso à Internet e as autoridades responsáveis pelo combate à pedofilia e ao racismo é indispensável para o bom êxito das investigações e da persecução penal. De outra forma, provedores que, uma vez obrigados judicialmente a fornecer determinada informação ou proceder à determinada conduta, deliberadamente deixarem de fazê-lo devem ser sancionados na forma como a legislação estabelecer, na medida em que se tornam partícipes e assistentes na disseminação da pornografia infantil. Por fim, cumpre observar que, em razão da Internet ser um sistema que pode ser acessado internacionalmente, os esforços para o combate à exploração sexual e às práticas de racismo devem igualmente ser amplos no seu escopo, envolvendo não apenas os órgãos encarregados da persecução e aplicação da lei penal, como também a cooperação de outros segmentos do setor público e privado.

ANEXO I:

JURISPRUDÊNCIA RECOLHIDA

1. Art. 241 do ECA. Crime praticado pela Internet. Competência da Justiça Federal:

· "PENAL E PROCESSUAL PENAL. HABEAS CORPUS.

TRANCAMENTO DE AÇÃO PENAL. COMPETÊNCIA DA JUSTIÇA FEDERAL. DENEGAÇÃO DA ORDEM.

1. A divulgação de fotos pornográficas de menores na internet é crime previsto em convenção internacional, o que firma a competência da Justiça Federal para o seu processamento,

independentemente do resultado ter ou não ocorrido no estrangeiro (artigo 109, v, da Constituição Federal). 2. Denegação da ordem". (TRF – 5a Região – HC 2002.05.00.013765-0 – Rel. Des. Ricardo César Mandarino Barretto – j. 25.06.02 – DJU 03.10.02, p. 600). · "PENAL. ESTATUTO DA CRIANÇA E DO ADOLESCENTE (LEI 8.069/90). ARTIGO 241. COMPETÊNCIA DA JUSTIÇA FEDERAL. ART. 109, V, DA CF/88. CONVENÇÃO DOS DIREITOS DA CRIANÇA. DECRETO LEGISLATIVO Nº 28/90 E DECRETO Nº 99.710/90. (...) DIVULGAÇÃO DE IMAGENS PORNOGRÁFICAS DE MENORES PELA INTERNET. (...) 1. O Congresso Nacional, através do Decreto Legislativo nº 28, de 24.09.90, bem como o Governo Federal, por força do Decreto nº 99.710, de 21.11.90, incorporaram ao direito pátrio os preceitos contidos na Convenção Sobre os Direitos da Criança, que prevê, entre outras coisas, que os Estados Partes darão proteção legal à criança contra atentados à sua honra e a sua reputação (art. 16), bem como tomarão as medidas que foram necessárias para impedir a exploração da criança em espetáculos ou materiais pornográficos (art. 34). 2. A Justiça Federal é competente para o processamento e julgamento da causa, aplicando-se à hipótese o disposto no art. 109, V, da CF/88, pois o delito praticado (art. 241 do ECA) encontra previsão no citado tratado, bem como sua execução teve início no País. Quanto ao resultado, levando-se em conta que o meio de divulgação utilizado foi a rede mundial de computadores (INTERNET), as fotos podem ter alcançado todos os países que tem conexão com a rede, ou seja, praticamente todo o planeta. 3. Tendo o réu se conformado com a decisão que lhe negou a suspensão do processo, não é possível, já em fase recursal, quando toda a instrução probatória já foi realizada, bem como todos os atos processuais, se falar em suspender o processo. Preliminar não conhecida por se tratar de questão preclusa. 4. Comprovadas a materialidade e a autoria dodelito pelo farto conjunto probatório, é de ser reconhecida a responsabilidade penal do réu pelo cometimento do ilícito previsto no art. 241 do Estatuto da Criança e do Adolescente, pois o mesmo utilizava-se de seu site na Internet para divulgar pornografia infantil,através da publicação de fotos pornográficas envolvendo crianças, que eram enviadas a ele por correio eletrônico (e-mail)". (TRF – 4ª Região – ACR 2002.04.01.03.3189-7 – Rel. Juiz José Luiz B. Germano da Silva – j. 29.04.03 – DJU 21.05.03, p. 806). · CONSTITUCIONAL. PROCESSUAL PENAL. CONDENAÇÃO PELOS DELITOS DOS ARTIGOS 241 DA LEI Nº 8.069/1990 E 218 DO CÓDIGO PENAL. "HABEAS CORPUS". TESE DE INCOMPETÊNCIA DA JUSTIÇA FEDERAL. ARTIGO 109-V, DA CONSTITUIÇÃO FEDERAL. INCONSISTÊNCIA. 1 – Ao contrário do que afirma o impetrante, a denúncia atribui ao paciente dolo direto na realização do tipo, sendo certo que, ao consumar o crime, publicando, na Internet, fotografias, contendo cenas pornográficas de sexo explícito, envolvendo crianças e adolescentes, deu causa ao resultado da publicação legalmente vedada, dentro e fora dos limites do território nacional, justificando a incidência do artigo 109-V, da Constituição Federal, sem espaço para, na espécie, cogitar-se de situação de mero exaurimento do delito, quando o que se tem é sua

efetiva concretização, dentro e fora do País. 2 – Irrelevância de precedente do Colendo STF para balizar o deslinde da causa. 3 – Ordem denegada". (TRF – 1a Região – Rel. Juiz Hilton Queiroz – HC 2001.01.00.029296-8/GO – j. 28.11.01). · "O Decreto Legislativo n.º 28, de 24.09.90 e o Decreto n.º 99.710, de 21.11.90 incorporaram ao direito pátrio os preceitos contidos na Convenção Sobre os Direitos da Criança que prevê que os Estados darão proteção legal à criança contra toda forma de exploração, inclusive abuso sexual (art. 19), bem como tomarão as medidas que forem necessárias para impedir a exploração da criança em espetáculos ou materiais pornográficos (art. 34). Assim estando o delito praticado (artigo 241 do Estatuto da Criança e do Adolescente) previsto no citado tratado aplica-se à hipótese o disposto no artigo 109, V, da Constituição Federal. (...) Além disso, não obstante a execução ter se iniciado no Brasil, o resultado produziu efeitos extraterritoriais, em razão da divulgação de fotos pornográficas de menores pela rede mundial de computadores (Internet) que alcança todos os países a ela conectados. (...) Consoante ainda observado pelo *Parquet* Federal *"...em conformidade com o art. 21, inciso XI, da Constituição Federal Brasileira, a exploração de serviços de telecomunicação é de competência exclusiva da União, do qual se infere o interesse da União nos delitos praticados por meio da Internet, sendo, portanto, a competência da Justiça Federal resguardada também com fundamento no art. 109, inc. I da Constituição Federal"* (fl. 49). (TRF – 3a Região – RESE 2003.61.81.000927-6 – Rel. Des. Vesna Kolmar – j. 30.11.04).

2. Art. 241 do ECA. Crime praticado pela Internet. Tipicidade.

· "Crime de Computador: publicação de cena de sexo infanto-juvenil (E.C.A., art. 241), mediante inserção em rede BBS/Internet de computadores, atribuída a menores: tipicidade: prova pericial necessária à demonstração da autoria: HC deferido em parte. 1. O tipo cogitado - na modalidade de "publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente" - ao contrário do que sucede por exemplo aos da Lei de Imprensa, no tocante ao processo da publicação incriminada - é uma norma aberta: basta-lhe à realização do núcleo da ação punível a idoneidade técnica do veículo utilizado à difusão da imagem para número indeterminado de pessoas, que parece indiscutível na inserção de fotos obscenas em rede BBS/Internet de computador. 2. Não se trata no caso, pois, de colmatar lacuna da lei incriminadora por analogia: uma vez que se compreenda na decisão típica da conduta criminada, o meio técnico empregado para realizá- la pode até ser de invenção posterior à edição da lei penal: a invenção da pólvora não reclamou redefinição do homicídio para tornar explícito que nela se compreendia a morte dada a outrem mediante arma de fogo. 3. Se a solução da controvérsia de fato sobre a autoria da inserção incriminada pende de informações técnicas de telemática que ainda pairam acima do conhecimento do homem comum, impõe-se a realização de prova pericial" (STF – 1a Turma - HC 76.689/PB – Rel. Min. Sepúlveda Pertence – j. 22.09.98 – DJU 06.11.98, p. 03). · "O cerne da questão em

debate é saber se a conduta praticada pelo paciente na vigência da antiga redação do art. 241 do Estatuto da Criança e do Adolescente corresponde ao núcleo do tipo, o verbo "publicar". (...) Sustenta o impetrante que o paciente, ao trocar arquivos pela internet, o fez em uma sala de bate-paporeservadíssima (acesso restrito) e com apenas uma pessoa, o que não corresponderia ao verbo "publicar" exigido pelo tipo. Assim não me parece. O verbo constante do tipo do art. 241 do ECA está intimamente ligado à divulgação e reprodução das imagens de conteúdo sexual ou pornográfico envolvendo crianças e adolescentes, no sentido de torná-las públicas. Qualquer meio hábil a viabilizar a divulgação dessas imagens ao público em geral corresponde ao que o legislador almejou com a utilização do verbo "publicar". Neste sentido, já dizia Nélson Hungria que publicar significa "tornar público, permitir o acesso ao público, no sentido de um conjunto de pessoas, pouco importando o processo de publicação" (Comentários ao Código Penal. Rio de Janeiro: Forense, 1958. Vol. VII. p. 340). Não resta dúvida de que a internet é um veículo de comunicação apto a tornar público o conteúdo pedófilo das fotos encontradas, o que já demonstraria, em tese, a tipicidade da conduta. Ademais, a denúncia formulada foi clara em registrar que qualquer pessoa que acessasse o servidor de arquivos criado pelo paciente teria à disposição esse material (...). Por outro lado, a discussão referente ao advento da Lei 10.764/2003 não foi ventilada - e muito menos apreciada - no recurso em habeas corpus interposto no Superior Tribunal de Justiça, motivo por que não conheço do writ nessa parte, para evitar supressão de instância. Evidente que à época da redação do dispositivo original (1990), o legislador não teria como prever o surgimento dessa nova tecnologia, daí por que já se decidiu ser o tipo do art. 241 aberto. Não foi outra a razão de a doutrina e a jurisprudência terem assinalado que qualquer instrumento hábil a tornar público o material proibido estaria incluído na compreensão do verbo "publicar". Por isso não se pode falar em interpretação prejudicial ao paciente nem em aplicação da analogia *in malam partem*". (STF – 2a Turma - HC 84561/PR - Rel. Min. Joaquim Barbosa – j. 5.10.2004 – DJU 26.11.04).

3. Interceptação de conversa em sala de bate-papo. Ausência de proteção constitucional ao sigilo.

· "A conversa realizada em 'sala de bate papo' da Internet, não está amparada pelo sigilo das comunicações, pois o ambiente virtual é de acesso irrestrito e destinado a conversas informais. (...) Dos documentos acostados é verificado que a INTERPOL interceptou conversa do acusado em 'sala de bate-papo' na Internet, momento em que foi noticiado a transmissão de imagens pornográficas envolvendo crianças e adolescentes. Esta conduta funcionou como elemento condutor da instauração do referido inquérito policial. (...) Acertada a decisão do e. Tribunal Regional Federal da 3ª Região que sobre o tema entendeu não haver o sigilo das comunicações, uma vez que a conversa fora realizada em 'sala de bate papo' da internet, em que se caracteriza, em

'ambiente virtual de acesso irrestrito e destinado a conversas informais'" (STJ – 6ª Turma – RHC 18.116-SP – Rel. Min. Hélio Quaglia Barbosa – j. 16.02.06).

ANEXO II:

PEÇAS PROCESSUAIS

1. Pedido de busca e apreensão de computadores. Crime de racismo praticado pela rede.

EXCELENTÍSSIMO SENHOR JUIZ FEDERAL DA 1ª VARA CRIMINAL FEDERAL DA SUBSEÇÃO JUDICIÁRIA DE SÃO PAULO.

Autos n.º XXXX (URGENTE)

O **MINISTÉRIO PÚBLICO FEDERAL**, pelo Procurador da República infra-assinado, vem respeitosamente à presença de Vossa Excelência requerer, com fundamento no art. 240 e ss. do Código de Processo Penal, a expedição de **MANDADO DE BUSCA E APREENSÃO** nos seguintes termos: Em 04 de junho último, a Comissão de Defesa do Consumidor, Meio Ambiente e Minorias da Câmara dos Deputados encaminhou ofício ao Diretor Geral do Departamento de Polícia Federal noticiando que o sítio h ttp:// w ww.kkkk.net/brazil contém textos e símbolos que incentivam a discriminação e o preconceito de raça e cor (fls. 04). Instaurou-se o presente inquérito policial para apurar a conduta em questão, que está subsumida no art. 20, *caput* e § 2o, da Lei Federal n.º 7.716/89. O sítio, consoante atesta o documento de fls. 06, é mantido por um provedor situado nos EUA. Uma parte de seu conteúdo pode ser vista a fls. 07-09. Há nele a menção a um **endereço eletrônico (**xxxxxx@hotmail.com**)**, e a uma **caixa postal** no Brasil (CP XXXX, CEP XXXXXX). Há também a referência a uma organização denominada "***Imperial Klans of Brazil – Knights of the Ku Klux Klan***". Como é sabido, a "*Ku Klux Klan*" é uma nefasta organização criminosa criada no sul dos Estados Unidos logo após a Guerra Civil Americana. Pregava a superioridade da "raça" branca e foi responsável pela **morte de mais de mil e quinhentas pessoas**. Covardes que eram, seus membros trajavam capuzes para ocultar suas verdadeiras identidades. A organização sobrevive, atualmente, graças ao fanatismo e à intolerância de uma minoria, pouco esclarecida. Pois bem. Uma "mensagem-isca" foi enviada ao endereço eletrônico constante do sítio (X XXXX @ hotmail.com). Uma pessoa, que se autodenominou "**BROTHER MARCOS 33/6**", respondeu o e-mail e, com isso, foi possível localizar o endereço IP usado pelo usuário no ato da resposta. O número obtido foi 200.171.77.132, e o acesso à rede mundial de computadores ocorreu no dia 24 de junho de 2003, às 13:33:47 (GMT). Em atendimento a pedido formulado pelo Ministério Público Federal, este juízo ordenou a quebra do sigilo de dados telemáticos do número IP 200.171.77.132 e, com isso, foi possível identificar o **endereço a partir de onde foi feita a conexão com a rede mundial de computadores**. O endereço é **Rua XXXXXXX, 21**. O nome do assinante da linha é a empresa **XXXXXXXX**, de propriedade de **YYYYYYY** e XXXXXXXXXX. A Polícia Federal apurou, também, que o destinatário da Caixa Postal n.º XXXX é **XXXXXXXX**, e

o endereço fornecido é **Rua XXXXXX, 86**. **XXXXXXXX de fato reside nesse último endereço, consoante atestam os documentos ora anexados. Nesse mesmo endereço está instalada a linha telefônica n.º (11) 5522-3378, de propriedade de YYYYYYY**, consoante atesta a anexa informação, fornecida no sítio da companhia telefônica. **Há, portanto, indícios suficientes que YYYYYYYY e XXXXXXXXX mantêm algum tipo de relacionamento, e que um deles é o responsável pela publicação da página.** O sítio contendo o conteúdo racista ainda está publicado na rede. Há nele outras páginas que ainda não haviam sido juntadas aos autos. Nelas, as mensagens de racismo são ainda mais evidentes. "**Acaso o senso comum nos diz que somos 100% perfeitamente iguais?**" ("Doesn't common sense tell us that we are all 100% perfectly equal?"), perguntam os membros dessa organização em uma das páginas ora anexadas. "**Olhe dentro dos olhos de uma criança *branca* e lembre-se dos motivos da criação deste grupo**", composto por "**arianos (homens brancos honráveis)**". O objetivo do grupo é a "**defesa dos direitos da raça branca**15". "Queremos entender porque que os outros (*sic*) seres podem ter 15 Celso Lafer, em parecer juntado aos autos do *habeas corpus* n.º 82.424-2, julgado pelo Supremo Tribunal Federal em setembro de 2003, lembra que a divisão dos seres humanos em raças é absolutamente insustentável do ponto de vista científico. "O avanço do conhecimento se incumbiu de mostrar que não há fundamento biológico em qualquer subdivisão racial da espécie humana e que os critérios das diferenças visíveis, a começar pela cor da pele, são apenas juízos de aparência. As diferenças genéticas individuais entre duas pessoas brancas são maiores que a diferença genética média entre brancos e negros e não custa lembrar que a integridade genética da espécie humana, como unidade, é comprovada na reprodução entre pessoas de 'raças' diferentes, gerando descendentes normais e férteis. (...) A capacidade de desvendar o genoma humano – que é uma revolução coperniquiana da biologia – permite dizer que conhecer uma espécie reduz a conhecer o seu genoma completo, e o seqüenciamento do genoma humano indica que as diferenças direitos especiais e facilidades em conseguir uma vaga de emprego e lugares garantidos nas faculdades". "Gostaríamos de mostrar ao mundo os **verdadeiros problemas de uniões inter-raciais**". Somos informados, também, que "**o Ku Klux Klan salvou o mundo duas vezes**" e que "**os judeus são filhos do demônio**" – "**aqueles judeus que mataram o Senhor Jesus, que nos perseguiram, que não são do agrado de Deus, que são inimigos de todos os homens**". "**Os verdadeiros filhos de Deus são os brancos**, que tem a fé, o sangue e a honra de ter uma vida justa. Devemos defender o futuro de nossa raça, evitando que um novo holocausto seja originado". A materialidade do delito tipificado no art. 20, *caput*, e § 2o, da Lei 7.716/89 está, como se vê, Excelência, perfeitamente demonstrada. Há também indícios suficientes da autoria delitiva. Todavia, o prosseguimento das investigações depende da apreensão dos computadores que contêm as páginas racistas, bem como de outros documentos e objetos que autorizem o ajuizamento da ação penal em face dos autores desse repugnante fato criminoso. A competência para a autorização da medida ora requerida pertence à Justiça Federal, nos termos do

disposto no art. 109, inciso V, da Constituição da República (*in verbis*: "aos juízes federais compete processar e julgar os crimes previstos em tratado ou convenção internacional, quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente"). Com efeito, o art. 4o da Convenção Internacional sobre a eliminação de todas as formas de discriminação racial (assinada pelo Brasil em 07 de março de 1966; ratificada, sem reservas, em 27 de março de 1968; e publicada através do Decreto Presidencial n.º 65.810, de 08 de dezembro de 1969), estabelece: **"Os Estados-partes condenam toda propaganda e todas as organizações que se inspiram em idéias ou teorias baseadas na superioridade de uma raça ou de um grupo de pessoas de uma certa cor ou de uma certa origem étnica ou que pretendam justificar ou encorajar qualquer forma de ódio e de descriminação raciais, e comprometem-se a adotar, imediatamente, medidas positivas destinadas a eliminar qualquer incitação a uma tal discriminação, ou quaisquer atos de discriminação com este objetivo, tendo em vista os princípios formulados na Declaração Universal dos Direitos do Homem e os direitos expressamente enumerados no art. V da presente Convenção, *inter alia*: a) a declarar, como delitos puníveis por lei, qualquer difusão de idéias baseadas na superioridade ou ódio** existentes no código genético de cada ser humano – que estão na escala dos milhões – não tem maior relação com a sua procedência geográfica ou étnica. No estudo da variabilidade genética humana, verifica-se que de 90 a 95% dela ocorre dentro dos chamados 'grupos raciais', não entre eles. Em síntese, como diz Sérgio Danilo Pena: 'há apenas uma raça do *homo sapiens*: a raça humana'" (pp. 61-62 do parecer, ora juntado aos autos). **raciais, qualquer incitamento à discriminação racial, assim como quaisquer atos de violência ou provocação a tais atos, dirigidos contra qualquer raça ou qualquer grupo de pessoas de outra cor, ou de outra origem étnica, como também qualquer assistência prestada a atividades racistas, inclusive seu financiamento (...)".** Em total consonância com o mandamento internacional, o Brasil editou, logo após a promulgação da Constituição democrática, a **Lei Federal n.º 7.716, de 05 de janeiro de 1989**, que "define os crimes resultantes de preconceitos de raça ou de cor". O art. 20 do citado diploma infraconstitucional definiu como crime "**praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional**" e previu uma forma qualificada do delito se "cometido por intermédio dos meios de comunicação social ou publicação de qualquer natureza". No caso dos autos, o crime de racismo foi cometido por intermédio do mais poderoso meio de comunicação da atualidade – a **rede mundial de computadores - INTERNET**. **Qualquer pessoa, em qualquer lugar do mundo, desde que conectada à rede, poderá acessar as páginas publicadas pelos investigados**. Evidente, portanto, o requisito da transnacionalidade, exigido pelo inciso V, art. 109, da Constituição da República, para justificar a competência desta Justiça Federal. Ante todo o exposto, pede o Ministério Público Federal, com fundamento nos arts. 240 e ss. do Código de Processo Penal, a expedição do competente mandado judicial para a busca e

apreensão de todos os **computadores** instalados nos dois endereços desta subseção judiciária referidos nesta petição, quais sejam, **Rua XXXXXX, 21 – Itaim Bibi** e **Rua XXXXXXXX, 86 – Jardim Hípico**. Pede, também, a **autorização judicial para busca e apreensão de objetos (inclusive CD's e disquetes) e documentos que possuam conteúdo discriminatório ou que auxiliem na apuração da participação de outras pessoas no delito aqui investigado**. Pede, ainda, desde logo, **autorização judicial para o acesso aos dados contidos nos computadores, disquetes e CD's que venham a ser apreendidos nos dois endereços**.

Termos em que, P. Deferimento. São Paulo, 29 de setembro de 2003. **2. Pedido de interceptação do fluxo de dados telemáticos. Pornografia infantil.**

EXCELENTÍSSIMO SENHOR JUIZ FEDERAL DA ª VARA CRIMINAL DA SEÇÃO JUDICIÁRIA DE SÃO PAULO. *O **MINISTÉRIO PÚBLICO FEDERAL**, pelo Procurador da República infra-assinado, vem respeitosamente à presença de Vossa Excelência expor e requerer o seguinte:* O presente procedimento de investigação foi instaurado para apurar *notitia criminis* enviada por *e-mail* a esta Procuradoria da República. Nela constava informação de que o *site* www.xxxxxxx.com.br estaria veiculando material pedófilo. O *site* seria, em princípio, destinado à divulgação de contos eróticos. Entretanto, pesquisa realizada na seção "incesto" revelou que alguns usuários utilizam o *site* para solicitar e oferecer imagens pornográficas de crianças e adolescentes . Um dos usuários, cujo e-mail é zzzzzzz@bol.com.br, postou a seguinte mensagem: "Título: Garotinha taradinha Oi, me chamo Samuel, gosto de brincar com menininhas de 5,6,7,8,9 e 10 aninhos. Se você quer trocar fotos de garotinhas me mande que mandarei também para você... Mas lembre-se só de garotinhas novinhas". Numa outra mensagem, o mesmo usuário revela: "Título: Garotinhas novinhas (...) Favor se você tiver fotos reais de garotinhas inocentes me envie que enviarei também de volta pra você uma foto que tirei em casa com a filhinha da minha vizinha de 6 aninhos, ela xxxxxxx e eu xxxxxxxxxxx". O usuário do *e-mail* xxxxxxxx@bol.com.br, por sua vez postou a seguinte mensagem: "Título: quer vc. ninfetas!!! Quero xxxxxx c/ ninfetas pois sou louco por ninfetinhas. Peço sigilo e discrição. (entre 11 a 13 anos). aguardo ansioso" No caso dos autos, os crimes acima indicados estão sendo cometidos por intermédio do mais poderoso meio de comunicação da atualidade – a **rede mundial de computadores - INTERNET**. A competência para a autorização da interceptação do fluxo e a quebra do sigilo de dados telemáticos, adiante requerida, pertence à Justiça Federal, nos termos do disposto no art. 109, inciso V, da Constituição da República (*in verbis*: "aos juízes federais compete processar e julgar os crimes previstos em tratado ou convenção internacional, quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente"). Evidente, aqui, o requisito da transnacionalidade, exigido pelo inciso V, art. 109, da Constituição da República, para justificar a competência desta Justiça Federal, vez que em qualquer lugar do mundo pode-se acessar as

mensagens postadas. É indispensável, para o prosseguimento das investigações, a identificação dos autores das mensagens e, mais ainda, é necessário verificar o que esses usuários veiculam em suas contas de e-mail, para saber se enviam e recebem imagens pornográficas de crianças e adolescentes. Numa fase posterior, poderá se apurar, também, os possíveis crimes de estupro e atentado violento ao pudor, sugeridos em algumas das mensagens postadas. Há nos autos, Excelência, indícios razoáveis da materialidade e da autoria do delito tipificado no artigo 241 da Lei 8.069/90, o qual é apenado com reclusão de 2 a 6 anos e multa. Ademais, a interceptação do fluxo telemático e a quebra do sigilo dos dados telemáticos, como exposto acima, é o único meio possível pelo qual pode ser feita a prova. Os usuários de Internet se beneficiam da Internet, face à dificuldade de investigação de crimes dessa natureza e, contando com a impunidade, continuando praticando seus crimes. Os *e-mails* xxxxxx@bol.com.br e xxxxxxx@bol.com.br são os únicos cujo provedor encontra-se no Brasil e optou-se, por esse motivo, requerer primeiramente o acesso aos dados desses usuários. O provedor dos dois e-mails é o Universo Online, sediado em São Paulo, na Av. Brigadeiro Faria Lima, 1384 – 10o andar. Todos os demais endereços eletrônicos possuem provedor estrangeiro, mesmo os que terminam em "br". Por todo o exposto, o Ministério Público Federal requer, quanto aos usuários dos endereços eletrônicos xxxxxxxxxx@bol.com.br e xxxxxxxxx@bol.com.br: (i) a imediata **INTERCEPTAÇÃO DO FLUXO DE DADOS TELEMÁTICOS**, nos termos do artigo 1º, parágrafo único, da Lei 9.296/96, pelo prazo de quinze dias, devendo o provedor de acesso UOL remeter ao Ministério Público Federal , em tempo real, e, posteriormente, também em papel, cópia de todos os *e-mails* recebidos e enviados pelos usuários, bem como dos arquivos neles anexados. A cópia em tempo real deverá ser encaminhada por meio de "conta-espelho" (conta criada pelo provedor com usuário e senha, réplica da conta original); e (ii)a **QUEBRA DO SIGILO DE DADOS TELEMÁTICOS**, devendo a empresa UOL apresentar, no prazo de cinco dias, todos os dados dos assinantes das mencionadas contas de *e*-mail, inclusive as datas de acesso e respectivos IPs e *e-mails* eventualmente armazenados. Com o objetivo de assegurar o prosseguimento da investigações, requer o Ministério Público Federal a **DECRETAÇÃO DO SIGILO ABSOLUTO DOS PRESENTES AUTOS**. Para o mesmo fim, requer que no ofício expedido à empresa STS conste ordem expressa para a **preservação do sigilo da ordem judicial ora requerida**. São Paulo, 04 de outubro de 2004. **3. Pedido de quebra de sigilo de dados telemáticos para provedor que hospeda *s ite* . Pornografia infantil.**

EXCELENTÍSSIMO SENHOR JUIZ FEDERAL DA ª VARA CRIMINAL DA SEÇÃO JUDICIÁRIA DE SÃO PAULO. Procedimento Criminal n.º XXXXXXXX O **MINISTÉRIO PÚBLICO FEDERAL**, pelo Procurador da República infra-assinado, vem respeitosamente à presença de Vossa Excelência expor e requerer o seguinte: O presente procedimento de investigação foi instaurado para apurar veiculação de imagens pornográficas envolvendo crianças e

adolescentes por usuários da Rede Mundial de Computadores, em virtude de *noticia criminis* enviada por e-mail a esta Procuradoria. Consta da notícia que o site www.ubbi.com.br hospeda páginas com imagens pornográficas de crianças e adolescentes. De fato, a pesquisa em referido site demonstrou existirem "álbuns" contendo imagens pornográficas de crianças e adolescentes, conforme cópias ora anexadas. Estando presentes indícios razoáveis da materialidade e da autoria do delito tipificado no artigo 241 da Lei 8.069/90, e sendo a quebra do sigilo dos dados telemáticos o único meio possível pelo qual pode ser feita a prova, requeiro a QUEBRA DO SIGILO DE DADOS TELEMÁTICOS, devendo a empresa UBBI16 apresentar, no prazo de quinze dias, cópias em CD-R das páginas anexas, todos os dados cadastrados do autor do "álbuns" e, ainda, dos logs e IPs gerados no momento da transmissão. São Paulo, 18 de janeiro de 2005. 16 Endereço: Rua XXXXX – São Paulo-SP, conforme pesquisa anexa. **4. Pedido de quebra de sigilo de dados telemáticos para concessionária de telefonia. Pornografia infantil.** 3a Vara Federal Criminal da Subseção Judiciária de São Paulo Autos n.º XXXXXXXXX MM. Juiz: 1. Ciente da decisão prolatada às fls. 59/61. 2. Analisando-se os documentos fornecidos pelo provedor Yahoo!, juntados às fls. 45/58, verificou-se, em primeiro lugar, através dos dados cadastrais fornecidos pelo usuário do e-mail xxxxxxxxxx@yahoo.com.br (fls. 45), que o IP utilizado por ele no momento da criação da conta foi o 200.171.135.82. Em pesquisa realizada junto ao site *registro.br*, constatou-se que o IP em questão está registrado na empresa TELECOMUNICACOES DE SAO PAULO S.A. – TELESP, sendo, portanto, este o provedor que fornece acesso à internet para o usuário. Diante do exposto, havendo indícios razoáveis da prática de crime gravíssimo – publicação, por meio da rede mundial de computadores, de fotografias e imagens com pornografia e cenas de sexo explícito envolvendo crianças e adolescentes – requer o Ministério Público Federal a **QUEBRA DE SIGILO DE DADOS TELEMÁTICOS**, devendo a concessionária TELESP (Rua Martiniano de Carvalho, n.º 851, São Paulo/SP) informar, no prazo de 05 (cinco) dias, os dados cadastrais do usuário que se conectou à internet no dia 09 de fevereiro de 2.002, às 19h50m06s (BRST GMT – 0200) e às 16h32m09s (EST GMT – 0500), utilizando-se do IP 200.171.135.82, em ambos os horários; São Paulo, 16 de março de 2005. **5. Quesitos para exame pericial em computadores apreendidos. Pornografia infantil.** 1ª Vara Criminal Federal da Seção Judiciária de São Paulo – SP Autos n.º XXXXXXXX MM. Juiz Federal: Trata-se de inquérito policial instaurado com o objetivo de apurar prática do crime previsto no artigo 241 da Lei 8.069/90. Da busca e apreensão realizada em três endereços apurados a partir de e-mails envolvidos em pedofilia, resultou vasto material que deverá ser encaminhado à perícia. Passo, então a formular os QUESITOS que deverão ser respondidos pela perícia:

1) Há *fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente* no material apreendido? Qual sua natureza (filmes, fotos, etc)?

2) É possível afirmar que houve divulgação de *fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente* desses computadores para outros usuários da Rede Mundial? Qual o material enviado? Para quem esse material foi enviado?

3) Há mensagens recebidas de outros usuários da Internet que contenham *fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente*? Quais os endereços eletrônicos dos remetentes? Qual o material recebido?

4) Quais páginas da Internet foram acessadas pelos usuários do material apreendido?

5) É possível afirmar que os usuários participavam de grupos de discussão e/ou comunidades em que se divulgavam ou publicam *fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente*? Quais são?

6) Os usuários possuem outra contas de e-mail cadastradas? Quais são?

7) É possível recuperar arquivos ou mensagens eletrônicas apagadas dos computadores? Em caso afirmativo, há arquivos ou mensagens recuperadas em que haja publicação ou divulgação de *fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente?*

8) Há elementos que permitam concluir que *fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente* foram produzidas ou editadas através dos comutadores apreendidos?

9)Existem aplicativos de edição e vídeos instalados nos computadores?

10) É possível afirmar que os usuários obtiveram para si ou para outrem vantagem patrimonial com a divulgação ou publicação de *fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente?*

11) Houve vendas de *fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente?*

12) Há outras informações úteis para a elucidação do caso? São Paulo, 21 de setembro de 2004.

6. Denúncia. Art. 241 do ECA.

EXCELENTÍSSIMO SENHOR JUIZ FEDERAL DA 1ª VARA CRIMINAL DA SEÇÃO JUDICIÁRIA DE SÃO PAULO. Autos n.º VVVVVVVVVVV O **MINISTÉRIO PÚBLICO FEDERAL**, pelo Procurador da República que esta subscreve, vem respeitosamente à presença de Vossa Excelência, oferecer a presente **DENÚNCIA** em face de **XXXXXXXXXX**, brasileiro, solteiro, advogado, portador da cédula de identidade RG 00000000000 SSP/SP, inscrito na OAB/SP sob o número 000000, nascido em 22 de abril de 1972 em São Paulo – SP, filho de XXXXXXX e de XXXXXXX, residente e domiciliado nesta capital na Rua TTTTTT; pela prática da conduta criminosa descrita a seguir: Consta dos inclusos autos de inquérito policial que o ora denunciado, usuário do e-mail xxxxxxxx@hotmail.com, no dia 31 de Maio de 2.001, às 23h43min06seg, nesta cidade e subseção judiciária, **publicou**, na rede mundial de computadores

(*internet*), remetendo ao usuário do e-mail yyyyyy@aol.com, um arquivo denominado "frag08_505.m1v", o qual continha um vídeo com **cena de sexo explícito e pornográfica envolvendo crianças.** Consta, ainda, que o ora denunciado, usuário do e-mail xxxxxxx@hotmail.com, no dia 31 de Maio de 2.001, às 23h46min21seg, nesta cidade e subseção judiciária, **publicou**, na rede mundial de computadores (*internet*), remetendo ao usuário do e-mail zzzzzz@aol.com, um arquivo denominado "frag08_505.m1v", o qual continha um vídeo com **cena de sexo explícito e pornográfica envolvendo crianças.** Segundo se apurou, a Divisão de Justiça Criminal do Departamento de Segurança Pública e Lei do Estado de Nova Jersey, nos Estados Unidos da América, noticiou à Superintendência Regional do Departamento de Polícia Federal, no Estado do Rio Grande do Sul, a prática da veiculação de exploração sexual infantil através de imagens divulgadas para todo o mundo pela Internet, detectadas em "site" sediado naquele país, sendo parte dessas imagens oriundas do Brasil (fls. 03/04). Imagens coletadas no site em questão (www.uuuuuuu.net) foram juntadas aos autos, constando das fls. 14/31. Nelas se verifica claramente o conteúdo pornográfico, no qual aparecem crianças em cenas de sexo. Conforme se verificou às fls. 09/13, um dos usuários provenientes do Brasil e que estaria participando desse site foi identificado pelo IP 200.183.97.81 e pelo e-mail xxxxxxxxxxx@hotmail.com. Em decisão de fls. 39/40, a MM. Juíza da 2ª Vara Criminal Federal determinou a quebra do sigilo das comunicações de dados do e-mail acima referido, no sentido de se obter, junto ao provedor de acesso à Internet "Hotmail.com", os dados cadastrais do seu assinante. E também foi determinada a intimação da empresa GLOBOCABO S/A, para que fornecesse os dados do usuário do IP supracitado. Em resposta, juntada às fls. 44, a "NET São Paulo" informou que o usuário do IP em questão tratava-se do ora denunciado, ou seja, XXXXXXXXX. Foi, ainda, fornecido o endereço do local onde ele realizava os acessos ao site supramencionado. Em decisão de fls. 54, foi determinada a realização de diligência junto ao endereço obtido, a fim de que fossem confirmadas as informações. Esta foi realizada com êxito, conforme relatório acostado às fls. 67, no qual os agentes federais informaram que no endereço realmente residia a pessoa do ora denunciado. Diante disso, foi deferida, pela MM. Juíza Federal da 2ª Vara Criminal Federal, a realização de busca domiciliar no endereço em questão, a fim de apreender computadores, fitas de vídeo, fotografias, disquetes, CD-ROMs, revistas e outros elementos que levassem à convicção sobre a prática de crime de pedofilia por parte do ora denunciado. Dando cumprimento ao mandado judicial, foram apreendidos os objetos descritos às fls. 82/83, os quais se encontravam em poder do ora denunciado. Entre eles, havia um equipamento eletrônico, marca "Toshiba", modelo Libretto 70 CT e uma CPU, completa, além de vários disquetes de 1.44Mb e CR Roms. O ora denunciado confessou, às fls. 86, que era responsável, à época dos fatos, pelo e-mail xxxxxx@hotmail.com, referido acima. Disse, ainda, que recebe e-mails contendo imagens de adolescentes em cenas de sexo ou pornográficas, sendo que costuma enviar as mensagens pornográficas que recebe a cerca

de vinte amigos. Quanto ao computador e o notebook apreendidos, seus respectivos discos rígidos foram submetidos a exame em mídia de armazenamento computacional, cujo laudo encontra-se às fls. 117/126 dos presentes autos. No exame feito no disco rígido do computador, verificou-se que ele apresentava indícios de que fora formatado em momento recente à elaboração do laudo, no entanto, logrou-se recuperar arquivos que haviam sido apagados e que continham imagens pornográficas envolvendo crianças e adolescentes. Os peritos da Polícia Federal gravaram o material relevante encontrado no computador e no notebook do ora denunciado em três CD-Roms, os quais encontram-se juntados nos presentes autos. Nestes CDs, há milhares de arquivos fotográficos e de vídeos, nos quais crianças com pouca idade e também adolescentes praticam sexo ou tiram a roupa e permanecem em posições degradantes. No arquivo "frag08_505.m1v", objeto do crime em questão, há um vídeo, no qual duas crianças do sexo masculino encontramse praticando sexo oral, conforme se verifica num dos CDs acostados aos autos. Verifica-se, ainda, que há várias mensagens encaminhadas pelo ora denunciado, nas quais ele se utiliza do idioma inglês para manter contato com outros pedófilos, a fim de combinar maneiras de obter novos arquivos contendo material pornográfico infantil. Um exemplo disso é a mensagem encaminhada no dia 31 de maio de 2001, por volta das 19h25min, na qual XXXXXXXXX questiona o seu interlocutor sobre a obtenção de "coisas" naquele dia. Além disso, em outra mensagem, o denunciado explica a um indivíduo como seria possível a troca de filmes e imagens através de ICQ (I Seek You), conforme atesta o laudo às fls. 122. Se não bastasse esse conteúdo, verificou-se no disco rígido do notebook apreendido que existem diversos arquivos que evidenciam que o usuário possuía cadastro em diversos sítios na Internet de acesso restrito com conteúdo pedófilo. Diversos desses sítios são localizados na Rússia.(fls. 122). Diante de todo exposto, estando configurada a materialidade do delito e indícios suficientes de sua autoria, **DENUNCIO XXXXXXXXX**, como incurso, por duas vezes, nas penas do art. 241 da Lei n.º 8.069/90, na forma do disposto no artigo 71 do Código Penal, requerendo que, recebida e autuada esta, seja instaurado o competente processo penal, citando e intimando o réu para todos os seus atos, até final condenação, nos termos dos arts. 394 a 405 e 498 a 502 do Código de Processo Penal. São Paulo, 28 de fevereiro de 2005.

ANEXO III:

ENDEREÇOS ÚTEIS

1. Provedores (de acesso, conteúdo, e-mail etc.).

RAZÃO SOCIAL RESPONSÁVEL ENDEREÇO TELEFONE

AOL Brasil – (América OnLine) Edson Costamilan Pavão Av. Industrial, 600 – Centro Industrial – Shopping ABC Plaza - 2º andar – São Paulo – SP – CEP 09080-500

(11) 2191-5900 **Click 21** – Comércio de Publicidade Ltda. (Embratel) Eduardo Vianna

Barreto R. Regente Feijó, 166, 14º andar – Centro - Rio de Janeiro - RJ - CEP 20060-060 (21) 4004 2121 TV Globo Ltda. **(Globo.Com)** Av. das Américas, 700 - Bloco 2A – Barra da Tijuca - Rio de Janeiro - RJ - CEP 22640-100 (21) 4003-8000/ 8003 **Google** Brasil (GMail e Orkut) Alexandre Hohagen Av. Brig. Faria Lima, 3729 – 5º andar – São Paulo – SP – CEP 04538-133 (11) 3443-6333 Internet Group do Brasil Ltda. **(IG)** Cássio Roberto Urbani Ribas Rua Amauri, 299 – 7º andar – Jd. Europa – São Paulo – SP – CEP 01448-901 (11) 3065- 9901/9999 Microsoft do Brasil (**Hotmail** e **Messenger**) Karine Yamassaki (Depto. Jurídico) Av. das Nações Unidas, 12901 - 27º andar - Torre Norte - São Paulo – SP CEP 04578-000 (11) 5504-2155 **Terra** Networks Brasil S.A. Carlos Henrique Severo Av. das Nações Unidas, 12901 – 12º andar – Torre Norte – São Paulo – SP – CEP 04578-000 (11) 5509 0644 **UOL** – Universo OnLine Victor Fernando Ribeiro Av. Brig. Faria Lima, 1384 – 6º andar – São Paulo – SP – CEP 01451-001 (11) 3038-8431 **Yahoo** do Brasil Internet Ltda. Regina Lima R. Fidêncio Ramos, 195 – 12º andar – São Paulo – SP – cep 04551-010 (11) 3054-5200

2. Concessionárias de telefonia fixa no Brasil.

SIGLA RAZÃO SOCIAL ENDEREÇO

TELEMAR/RJ Telemar Norte Leste S.A. Rua Gal. Polidoro, 99 – Botafogo – Rio de Janeiro – RJ – CEP 22280-001 TELEMAR/MG Telemar Norte Leste S.A. Av. Afonso Pena, 4001 – 1º andar – Belo Horizonte – MG – CEP 30130-008 CTBC TELECOM Cia. de Telecomunicações do Brasil Central Av. Afonso Pena, 3928 – Bairro Brasil – Uberlândia – MG – CEP 38400-710 TELEMAR/ES Telemar Norte Leste S.A. Av. Afonso Pena, 4001 – 1º andar – Belo Horizonte – MG – CEP 30130-008 TELEMAR/BA Telemar Norte Leste S.A. Rua Silveira Martins, 355 – Cabula – Salvador – BA – CEP 41156-900 TELEMAR/SE Telemar Norte Leste S.A. Rua Silveira Martins, 355 – Cabula – Salvador – BA – CEP 41156-900 TELEMAR/AL Telemar Norte Leste S.A. Rua Silveira Martins, 355 – Cabula – Salvador – BA – CEP 41156-900 TELEMAR/PE Telemar Norte Leste S.A. Av. Afonso Olindense, 1513 – Várzea – Recife – PE – CEP 50819-900 TELEMAR/PB Telemar Norte Leste S.A. Av. Afonso Olindense, 1513 – Várzea – Recife – PE – CEP 50819-900 TELEMAR/RN Telemar Norte Leste S.A. Av. Afonso Olindense, 1513 – Várzea – Recife – PE – CEP 50819-900 TELEMAR/CE Telemar Norte Leste S.A. Av. Borges de Melo, 1677 – 7º andar – Bairro de Fátima – Fortaleza – CE – CEP 60415-510 TELEMAR/PI Telemar Norte Leste S.A. Av. Borges de Melo, 1677 – 7º andar – Bairro de Fátima – Fortaleza – CE – CEP 60415-510 TELEMAR/MA Telemar Norte Leste S.A. Av. Borges de Melo, 1677 – 7º andar – Bairro de Fátima – Fortaleza – CE – CEP 60415-510 TELEMAR/PA Telemar Norte Leste S.A. Av. Borges de Melo, 1677 – 7º andar – Bairro de Fátima – Fortaleza – CE – CEP 60415-510 TELEMAR/AP Telemar Norte Leste S.A. Av. Borges de Melo, 1677 – 7º andar – Bairro de Fátima – Fortaleza – CE – CEP 60415-510 TELEMAR/AM Telemar Norte Leste S.A. Av. Borges de

Melo, 1677 – 7º andar – Bairro de Fátima – Fortaleza – CE – CEP 60415-510 TELEMAR/RR Telemar Norte Leste S.A. Av. Borges de Melo, 1677 – 7º andar – Bairro de Fátima – Fortaleza – CE – CEP 60415-510 BRASIL TELECOM/SC Brasil Telecom S.A. Av. Madre Benvenuta, 2080 – Itacorubi – Florianópolis – SC – CEP 88035-900 BRASIL TELECOM/PR Brasil Telecom S.A. Av. Manoel Ribas, 115 – Curitiba – PR – CEP 80510-900 SERCOMTEL Sercomtel S.A. Telecomunicações R. Prof. João Cândido, 555 – Centro – Londrina – PR – CEP 86010-000 BRASIL TELECOM/MS Brasil Telecom S.A. R. Tapajós, 660 – Vila Rica – Campo Grande – MS – CEP 79022-210 BRASIL TELECOM/MT Brasil Telecom S.A. R. Barão do Melgaço, 3209 – Centro Sul – Cuiabá – MT – CEP 78020-902 BRASIL TELECOM/GO-TO Brasil Telecom S.A. BR 153, km. 06 – CAEL – V. Redenção – Goiânia – GO – CEP 74845-090 BRASIL TELECOM/DF Brasil Telecom S.A. SCS Quadra 02 - Bloco E – Ed. Telebrasília – Brasília – DF – CEP 70390-025 BRASIL TELECOM/RO-AC Brasil Telecom S.A. Av. Lauro Sodré, 3290 – Bairro dos Tanques – Porto Velho – RO – CEP 78903-711 BRASIL TELECOM/Pelotas Brasil Telecom S.A. Av. Borges de Medeiros, 512 – Porto Alegre – RS – CEP 90020-022 BRASIL TELECOM/RS Brasil Telecom S.A. Av. Borges de Medeiros, 512 – Porto Alegre – RS – CEP 90020-022 BRASIL TELECOM/Matriz Brasil Telecom S.A. SAI SUL – ASP Lote D – Brasília – DF – CEP 71215-000 TELESP Telecomunicações de São Paulo S.A. Rua Martiniano de Carvalho, 851 – 20º e 21º andar – São Paulo – SP – CEP 01321-002

3. ABRANET e Comitê Gestor da Internet.

NOME CONTATO ENDEREÇO TELEFONE

Comitê Gestor da Internet no Brasil – CGI Demi Getschko e Hartmut Richard Glaser Avenida das Nações Unidas, 11541 - 7º andar – São Paulo – SP – CEP 04578-000 (11) 5509 3503/3513 ABRANET – Associação Brasileira dos Provedores de Acesso, Serviços e Informações da Rede Internet António Alberto Valente Tavares R. Tabapuã, 627 - 3º andar - sala 34 – CEP 04533-012 (11) 3078-3866

ANEXO IV:

ACORDOS CELEBRADOS PELA PR-SP

1. Termo de compromisso de integração operacional celebrado com principais provedores de acesso de São Paulo.

Pelo presente instrumento, A PROCURADORIA DA REPÚBLICA NO ESTADO DE SÃO PAULO, órgão integrante do Ministério Público Federal, sediada nesta capital, na Rua Peixoto Gomide, 768 – Cerqueira César, neste ato representada pela Excelentíssima Senhora Procuradora Chefe, Dra. ADRIANA ZAWADA MELO e pelos Procuradores Regionais dos Direitos do Cidadão, Dr. SERGIO GARDENGHI SUIAMA e Dra. ADRIANA DA SILVA FERNANDES; Os

provedores de acesso à internet UNIVERSO ON LINE, sediado na Avenida Brigadeiro Faria Lima, 1384 - 6º andar, neste ato representado pelo Ilustríssimo Senhor VICTOR FERNANDO RIBEIRO, RG 29.089.911-4 SSP/SP; INTERNET GROUP DO BRASIL LTDA. - IG, sediado na Rua Amauri, nº 299 - 7º andar, neste ato representado pelo Ilustríssimo Senhor CÁSSIO ROBERTO URBANI RIBAS - OAB/SP nº 154.045; TERRA NETWORKS BRASIL S.A., na Av. Nações Unidas, 12.901, 12º andar, Torre Norte, neste ato representado pelo Ilustríssimo Senhor CARLOS HENRIQUE SEVERO, RG nº 39590691-X; AOL BRASIL, sediado na Av. Industrial, 600 - Centro Empresarial ABC Plaza, 2º andar, neste ato representado pelo Ilustríssimo Senhor EDSON COSTAMILAN PAVÃO, OAB/SP nº 151.079; CLICK 21 COMÉRCIO DE PUBLICIDADE LTDA., sediado na Rua Rejente Feijó, 166, 14 andar, Centro, Rio de Janeiro – RJ, neste ato representado pelo Ilustríssimo Senhor EDUARDO VIANNA BARRETO, RG nº 066.078.12- 2 IFP/RJ; A ASSOCIAÇÃO BRASILEIRA DOS PROVEDORES DE ACESSO, SERVIÇOS E INFORMAÇÕES DA REDE INTERNET - ABRANET, sediada nesta capital, na Rua Tabapuã, 697 - 3° andar, neste ato representada por seu Presidente, o Ilustríssimo Senhor ANTÔNIO ALBERTO VALENTE TAVARES; As EMPRESAS DE SERVIÇOS DE INTERNET ASSOCIADAS À ABRANET SIGNATÁRIAS do presente termo; O COMITÊ GESTOR DA INTERNET NO BRASIL, sediada na Avenida das Nações Unidas, 11541, 7º andar, neste ato representado pelo Ilustríssimo Senhor DEMI GETSCHKO, RG nº 5.490.048-7; têm justo e acertado o seguinte: CONSIDERANDO que o art. 227 da Constituição da República estabelece ser dever da família, da sociedade e do Estado colocar as crianças e os adolescentes a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão; e que o parágrafo 4o do mesmo artigo obriga o Estado a punir severamente o abuso, a violência e a exploração sexual da criança e do adolescente; CONSIDERANDO que o art. 34 da Convenção das Nações Unidas sobre os Direitos da Criança, ratificada pelo Brasil, obriga os Estados-partes a proteger a criança contra todas as formas de exploração e abuso sexual, inclusive no que se refere à exploração da criança em espetáculos ou materiais pornográficos; CONSIDERANDO que a Conferência Internacional sobre o Combate à Pornografia Infantil na Internet (Viena, 1999) demanda a criminalização, em todo o mundo, da produção, distribuição, exportação, transmissão, importação, posse intencional e propaganda de pornografia infantil, e enfatiza a importância de cooperação e parceria mais estreita entre governos e a indústria da Internet; CONSIDERANDO que o art. 5o do Estatuto da Criança e do Adolescente (Lei Federal n.º 8.069/90) dispõe que nenhuma criança ou adolescente será objeto de qualquer forma de negligência, discriminação, exploração, violência, crueldade e opressão, punido na forma da lei qualquer atentado, por ação ou omissão, aos seus direitos fundamentais; CONSIDERANDO que o art. 70 do mesmo Estatuto determina ser dever de todos prevenir a ocorrência de ameaça ou violação dos direitos da criança e do adolescente; CONSIDERANDO que, nos termos do art. 201, inciso VIII, do Estatuto da Criança e do

Adolescente, compete ao Ministério Público zelar pelo efetivo respeito aos direitos e garantias legais assegurados às crianças e adolescentes, promovendo as medidas judiciais e extrajudiciais cabíveis; CONSIDERANDO que a Lei Federal n.º 10.764/03 alterou a redação do art. 241 do Estatuto da Criança e do Adolescente para incluir a responsabilização criminal de quem assegura o acesso à rede mundial de computadores ou os meios ou serviços para o armazenamento das fotografias, cenas ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente; CONSIDERANDO que a Convenção Internacional sobre a Eliminação de Todas as Formas de Discriminação Racial, promulgada pela Assembléia Geral das Nações Unidas em 21 de dezembro de 1965, e ratificada pelo Brasil em 27 de março de 1968, obriga os Estados-partes a declarar, como delitos puníveis por lei, qualquer difusão de idéias baseadas na superioridade ou ódio raciais, qualquer incitamento à discriminação racial, assim como quaisquer atos de violência ou provocação a tais atos, dirigidos contra qualquer raça ou qualquer grupo de pessoas de outra cor ou de outra origem étnica, como também qualquer assistência prestada a atividades racistas, inclusive seu financiamento; CONSIDERANDO que a mesma Convenção obriga os Estados-partes a tomar todas as medidas apropriadas para proibir e pôr fim à discriminação racial praticada por quaisquer pessoas, grupos ou organizações; CONSIDERANDO que é objetivo da República Federativa do Brasil a promoção do bem de todos, sem preconceitos de origem, raça, sexo, idade e quaisquer outras formas de discriminação (CR, art. 3o, IV); CONSIDERANDO, ainda, que o art. 5o, inciso XLI, da Constituição da República ordena a punição de qualquer discriminação atentatória dos direitos e liberdades fundamentais; CONSIDERANDO que a Lei Federal n.º 7.716, de 05 de janeiro de 1989, tipifica o delito de "praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional" e qualifica a conduta quando cometida por intermédio dos meios de comunicação social ou publicação de qualquer natureza (art. 20, caput, e § 3o); CONSIDERANDO que o Plano Nacional de Direitos Humanos (PNDH) ordena a edição de medidas que busquem coibir o uso da Internet para incentivar práticas de violação dos direitos humanos; CONSIDERANDO a competência da Justiça Federal para processar e julgar os crimes previstos em tratado ou convenção internacional, quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente (CR, art. 109, inciso V);CONSIDERANDO que a Organização Não-Governamental italiana "*Rainbow Phone*", em seu relatório anual publicado na Internet, apontou o Brasil como o quarto país no mundo em número de sítios de pornografia infantil; CONSIDERANDO, o grande número de denúncias de sítios brasileiros com conteúdo racista e discriminatório, o que está a exigir providências interinstitucionais, em decorrência dos bens jurídicos fundamentais atacados, quais sejam, a dignidade da pessoa humana, a cidadania e a igualdade fundamental entre todas as pessoas; CONSIDERANDO, finalmente, a necessidade de integrar as partes signatárias na aplicação dos dispositivos constitucionais e legais acima referidos; RESOLVEM celebrar o presente Termo de

Compromisso de Integração Operacional com a finalidade de unir esforços para prevenir e combater a pornografia infantil, a prática de racismo e outras formas de discriminação, instrumentalizadas via Internet. Para tal, ficam acordadas as seguintes CLÁUSULAS: Cláusula Primeira: Ficam o Ministério Público Federal e a Polícia Federal comprometidos a manter sítio na Internet de enfrentamento à pornografia infantil, ao racismo e a outras formas de discriminação, informando o público acerca da legislação aplicável e facultando ao usuário formular notícia de crimes cibernéticos cuja repressão esteja no âmbito da repressão do Estado brasileiro. Cláusula Segunda: Ficam os provedores de serviço de Internet signatários comprometidos a: a) manter, permanentemente, em suas páginas, selo institucional de campanha governamental contra a pornografia infantil e contra a veiculação de preconceitos quanto à origem, raça, etnia, sexo, orientação sexual, cor, idade, crença religiosa ou outras formas de discriminação; b) fazer, periodicamente, chamadas contra essas práticas, através de quaisquer meios de que dispõem para a comunicação regular com seus usuários, tais como documentos de cobrança, *e-mails* e instrumentos contratuais; c) orientar o público sobre a utilização não criminosa de salas de bate-papo, grupos e fóruns de discussão, *blogs*, páginas pessoais e outros serviços disponibilizados ao usuário; d) inserir, nos contratos de adesão ao serviço de acesso que venham a ser assinados a partir da vigência deste termo, cláusula que preveja a rescisão da relação jurídica na hipótese do usuário valer-se do provedor para veicular fotografias e imagens de pornografia infantil, ou idéias preconceituosas quanto à origem, raça, etnia, sexo, orientação sexual, cor, idade, crença religiosa ou outras formas de discriminação; e) manter *link* para o sítio previsto na cláusula primeira; f) manter, sem prejuízo do previsto na alínea anterior, *link* pelo qual os usuários possam noticiar ao provedor signatário as condutas referidas neste termo, quando praticadas em ambiente, página, grupo de discussão, álbum eletrônico, ou outro serviço prestado pelo próprio provedor; g) informar imediatamente ao Ministério Público Federal, por via eletrônica ou outros meios de comunicação, tão logo tomem conhecimento de que abrigam pornografia infantil ou conteúdo manifestamente discriminatório em razão da origem, raça, etnia, sexo, orientação sexual, cor, idade, crença religiosa ou outras formas de discriminação, ou ainda de que usuários do provedor estão usando o acesso à rede para praticar os crimes tipificados no art. 241 da Lei Federal n.º 8.069/90 e no art. 20 da Lei Federal n.º 7.716/89, assegurada a proteção ao sigilo dos dados telemáticos; h) preservar e armazenar, pelo prazo mínimo de 6 (seis) meses ou prazo superior que venha a ser estabelecido pela legislação, o registro de *logs* de acesso discado e, quando possível, também os IPs originários dos usuários dos serviços de *web page*, salas de bate-papo, *fotologs*, fóruns de discussão *on-line* e outros. O disposto nesta cláusula aplicar-se-á mesmo após o prazo mínimo indicado, se houver solicitação escrita da Polícia Federal ou do Ministério Público Federal, até que estas instituições providenciem a competente ordem judicial de quebra de sigilo de dados telemáticos; j) solicitar e manter os dados cadastrais informados por seus assinantes de acesso; l) exigir que os novos

usuários do serviço de acesso informem o número de algum documento validável de identificação, como por exemplo o número do RG ou do CPF; Cláusula Terceira: As obrigações assumidas no presente Termo permanecerão válidas e obrigam as empresas associadas à ABRANET, signatárias deste Termo, ainda que deixem de ser associadas à Associação signatária. Cláusula Quarta: O presente termo vigorará por tempo indeterminado e está aberto à adesão de outros provedores que concordem integralmente com seus termos. Cláusula Quinta: O presente termo entrará em vigor após 60 (sessenta) dias de sua assinatura. São Paulo, 10 de novembro de 2005. **2. Termo de cooperação celebrado com o hotline Safernet Brasil.** Pelo presente instrumento, A PROCURADORIA DA REPÚBLICA NO ESTADO DE SÃO PAULO, órgão do Ministério Público Federal sediado nesta capital, na Rua Peixoto Gomide, 768 – Cerqueira César, neste ato representada pela Excelentíssima Senhora Procuradora Chefe em exercício, Dra. Thaméa Danelon Valiengo e pelo Procurador Regional dos Direitos do Cidadão, Dr. SERGIO GARDENGHI SUIAMA e a SAFERNET BRASIL, associação civil de direito privado sem fins lucrativos e econômicos, de atuação nacional, de duração ilimitada e ilimitado número de membros, sem vinculação político partidária, inscrita no CNPJ/MF sob o número 07.837.984/0001-09, com sede provisória na cidade de Salvador, Estado da Bahia, na Avenida Tancredo Neves 1632, Torre Norte, sala 2101 - Caminho das Árvores, neste ato representada por seu Presidente, Dr. THIAGO TAVARES NUNES DE OLIVEIRA, CONSIDERANDO que o art. 227 da Constituição da República estabelece ser dever da família, da sociedade e do Estado colocar as crianças e os adolescentes a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão; e que o parágrafo 4o do mesmo artigo obriga o Estado a punir severamente o abuso, a violência e a exploração sexual da criança e do adolescente; CONSIDERANDO que o art. 34 da Convenção das Nações Unidas sobre os Direitos da Criança, ratificada pelo Brasil, obriga os Estados-partes a proteger a criança contra todas as formas de exploração e abuso sexual, inclusive no que se refere à exploração da criança em espetáculos ou materiais pornográficos; CONSIDERANDO que o art. 5o do Estatuto da Criança e do Adolescente (Lei Federal n.º 8.069/90) dispõe que nenhuma criança ou adolescente será objeto de qualquer forma de negligência, discriminação, exploração, violência, crueldade e opressão, punido na forma da lei qualquer atentado, por ação ou omissão, aos seus direitos fundamentais; CONSIDERANDO que, nos termos do art. 201, inciso VIII, do Estatuto da Criança e do Adolescente, compete ao Ministério Público zelar pelo efetivo respeito aos direitos e garantias legais assegurados às crianças e adolescentes, promovendo as medidas judiciais e extrajudiciais cabíveis; CONSIDERANDO que o art. 241 do Estatuto da Criança e do Adolescente tipifica as condutas criminosas de "apresentar, produzir, vender, fornecer, divulgar, ou publicar, por qualquer meio de comunicação, inclusive rede mundial de computadores ou internet, fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente"; CONSIDERANDO que a Convenção Internacional

sobre a Eliminação de Todas as Formas de Discriminação Racial, promulgada pela Assembléia Geral das Nações Unidas em 21 de dezembro de 1965, e ratificada pelo Brasil em 27 de março de 1968, obriga os Estados-partes a reprimir qualquer difusão de idéias baseadas na superioridade ou ódio raciais, qualquer incitamento à discriminação racial, assim como quaisquer atos de violência ou provocação a tais atos, dirigidos contra qualquer raça ou qualquer grupo de pessoas de outra cor ou de outra origem étnica, como também qualquer assistência prestada a atividades racistas, inclusive seu financiamento; CONSIDERANDO que a mesma Convenção obriga os Estados-partes a tomar todas as medidas apropriadas para proibir e pôr fim à discriminação racial praticada por quaisquer pessoas, grupos ou organizações; CONSIDERANDO que é objetivo da República Federativa do Brasil a promoção do bem de todos, sem preconceitos de origem, raça, sexo, idade e quaisquer outras formas de discriminação (CR, art. 3o, IV); CONSIDERANDO, ainda, que o art. 5o, inciso XLI, da Constituição da República ordena a punição de qualquer discriminação atentatória dos direitos e liberdades fundamentais; CONSIDERANDO que a Lei Federal n.º 7.716, de 05 de janeiro de 1989, tipifica o delito de "praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional" e qualifica a conduta quando cometida por intermédio dos meios de comunicação social ou publicação de qualquer natureza (art. 20, caput, e § 3o); CONSIDERANDO que o Plano Nacional de Direitos Humanos (PNDH) ordena a edição de medidas que busquem coibir o uso da Internet para incentivar práticas de violação dos direitos humanos; CONSIDERANDO a competência da Justiça Federal para processar e julgar os crimes previstos em tratado ou convenção internacional, quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente (CR, art. 109, inciso V); CONSIDERANDO que a Organização Não-Governamental italiana "*Rainbow Phone*", em relatório anual publicado na Internet, apontou o Brasil como o quarto país no mundo em número de sítios de pornografia infantil; CONSIDERANDO que a Conferência Internacional sobre Combate à Pornografia Infantil na Internet (Viena, 1999) demanda a criminalização, em todo o mundo, da produção, distribuição, exportação, transmissão, importação, posse intencional e propaganda de pornografia infantil, e enfatiza a importância de cooperação e parceria mais estreita entre o governo, a sociedade civil e a indústria da Internet; CONSIDERANDO o grande número de denúncias de sítios brasileiros com conteúdo racista e discriminatório, o que está a exigir providências interinstitucionais, em decorrência dos bens jurídicos fundamentais atacados, quais sejam, a dignidade da pessoa humana e a igualdade fundamental entre todas as pessoas; CONSIDERANDO a constituição, no âmbito da Procuradoria da República no Estado de São Paulo, de grupo especializado no combate aos crimes cibernéticos; CONSIDERANDO a experiência acumulada pelos fundadores da organização-parte na concepção, planejamento, desenvolvimento e operação do projeto "Hotline-Br"; CONSIDERANDO que a atual dispersão dos canais de denúncia de crimes cibernéticos prejudica, sensivelmente, a persecução penal,

favorecendo a impunidade em casos graves de pornografia infantil e crimes de ódio; CONSIDERANDO, finalmente, a necessidade de integrar as partes signatárias na aplicação dos dispositivos constitucionais e legais acima referidos; RESOLVEM celebrar o presente TERMO DE MÚTUA COOPERAÇÃO TÉCNICA, CIENTÍFICA E OPERACIONAL com a finalidade de unir esforços para prevenir e combater a pornografia infantil, a prática de racismo e outras formas de discriminação, instrumentalizadas via Internet. Para tal, ficam acordadas as seguintes CLÁUSULAS:

CLÁUSULA PRIMEIRA – OBJETO O presente termo tem por objeto a cooperação técnica, científica e operacional entre as partes celebrantes, com vistas: a. à centralização do recebimento, processamento, encaminhamento e acompanhamento on-line de notícias de crimes contra os direitos humanos praticados com o uso da rede mundial de computadores – Internet – no Brasil; b. ao intercâmbio e difusão de tecnologias baseadas em plataformas livres e de código aberto, para serem gratuitamente utilizadas pelas Procuradorias da República nos Estados e no Distrito Federal e também pelas autoridades policiais brasileiras; c. ao desenvolvimento de projetos e atividades voltadas para o treinamento de recursos humanos, editoração e publicação, planejamento e desenvolvimento institucional abrangendo as áreas de pesquisa e extensão, com o intuito de debater e assegurar a efetiva proteção e promoção dos direitos humanos na sociedade da informação. Parágrafo único. Para fins do disposto neste termo, a expressão "crimes contra os direitos humanos" compreende os seguintes delitos: a) crimes de ódio tipificados no art. 20 e §§ da Lei Federal n.º 7.716/89; b) crime de pornografia infantil tipificado no art. 241 da Lei Federal n.º 8.069/90; c) crimes contra o sentimento religioso tipificados no art. 208 do Código Penal brasileiro; d) crime de incitação ao genocídio, previsto no art. 3º da Lei Federal n.º 2.889/56; e) apologia ou incitação aos crimes acima indicados ou a outros delitos contra a vida, a integridade física, a liberdade (inclusive sexual) e a incolumidade pública, desde que de competência da Justiça Federal brasileira; e) crime de quadrilha ou bando (art. 288 do Código Penal brasileiro), se conexo aos crimes acima indicados.

CLÁUSULA SEGUNDA – COMPROMISSOS COMUNS Para a consecução dos objetivos indicados na cláusula primeira, as partes comprometem-se neste ato a: a. desenvolver, em parceria, estudos e pesquisas buscando criar e aperfeiçoar as tecnologias de enfrentamento aos crimes cibernéticos, disponibilizando o conhecimento gerado para as autoridades brasileiras envolvidas na persecução penal; b. produzir relatórios e notas técnicas com o objetivo de orientar a atuação das autoridades envolvidas no enfrentamento aos crimes contra os direitos humanos na Internet; c. promover o intercâmbio de informações, tecnologias, técnicas de rastreamento e assemelhadas, através da organização de cursos, oficinas e outras atividades de capacitação; d. promover campanhas conjuntas para a conscientização da sociedade em relação à utilização adequada da Internet, visando à proteção e promoção dos direitos humanos na sociedade da informação.

CLÁUSULA TERCEIRA – OBRIGAÇÕES DA SAFERNET BRASIL. A SAFERNET BRASIL compromete-se, neste ato, a: a. manter portal na Internet para a recepção de notícias de crimes contra os direitos humanos, contendo informações e orientações ao público sobre o uso seguro e lícito da Internet; b. processar e encaminhar exclusivamente à Procuradoria da República em São Paulo as notícias recebidas, quando o provedor de acesso ou de hospedagem do material criminoso estiver sediado no Estado de São Paulo, ou quando houver indícios de que o autor do fato delituoso estiver no mesmo Estado; c. comunicar as demais notícias de fatos criminosos recebidas às autoridades com atribuição para investigá-las, na forma do art. 4º, § 3º, do Código de Processo Penal, ou às Procuradorias da República nos Estados e no Distrito Federal, mediante a celebração de termos de cooperação específicos; d. fornecer, gratuitamente, os recursos tecnológicos e o treinamento necessários ao pleno desenvolvimento das ações previstas neste termo de cooperação. § 1º. A associação signatária declara-se, neste ato, ciente de que o presente ato tem natureza gratuita, e que, portanto, o adimplemento das obrigações contidas neste termo não importará em contraprestação financeira por parte da Procuradoria da República no Estado de São Paulo. § 2º. Na medida de suas possibilidades financeiras e jurídicas, a Procuradoria da República no Estado de São Paulo prestará o suporte necessário à execução das obrigações contidas no cláusula anterior e na alínea "d" da presente cláusula.

CLÁUSULA QUARTA – COMPROMISSOS DA PROCURADORIA DA REPÚBLICA NO ESTADO DE SÃO PAULO A PROCURADORIA DA REPÚBLICA NO ESTADO DE SÃO PAULO compromete-se, neste ato, a: a. receber e processar todas as notícias de fatos criminosos encaminhadas pela organização-parte na forma da alínea "b" da cláusula anterior, com o objetivo de comprovar a autoria e a materialidade dos fatos criminosos comunicados; b. manter, em sua página eletrônica, *banner* contendo os nomes das partes e link para o portal referido na alínea "a" da cláusula anterior; c. solicitar aos provedores de acesso e às instituições anuentes, signatários do documento "Termo de Compromisso de Integração Operacional" celebrado em 10 de novembro de 2005, que coloquem, em suas páginas, o *link* e o *banner* referidos na alínea anterior, como forma de cumprimento da obrigação assumida na alínea "e" da cláusula segunda do referido documento; d. noticiar a celebração do presente termo de cooperação à Procuradoria Geral da República, à Procuradoria Federal dos Direitos do Cidadão, às Procuradorias da República nos Estados e no Distrito Federal, ao Departamento de Polícia Federal e à Secretaria Especial dos Direitos Humanos da Presidência da República, e sugerir a esses e a outros órgãos afins que mantenham em suas páginas eletrônicas o *banner* e o *link* indicados na alínea "b" desta cláusula, com o objetivo de centralizar as notícias de crimes cibernéticos contra os direitos humanos em um único canal de denúncias.

CLÁUSULA QUINTA – SIGILO As partes se obrigam a manter sob o mais estrito sigilo os dados e informações referentes aos projetos e ações consideradas e definidas como confidenciais, não

podendo de qualquer forma, direta ou indiretamente, dar conhecimento, a terceiros não autorizados, das informações confidenciais trocadas entre os acordantes ou por eles geradas na vigência do presente termo.

CLÁUSULA SEXTA – CASOS OMISSOS: Os casos omissos no presente ajuste serão resolvidos de comum acordo entre as partes, podendo ser firmados, se necessário, Termos Aditivos que farão parte integrante deste instrumento.

CLÁUSULA SÉTIMA - ALTERAÇÃO E DENÚNCIA O presente instrumento poderá ser alterado em qualquer de suas cláusulas, mediante Termo Aditivo, bem como denunciado, independentemente de prévia notificação, no caso de inadimplemento das obrigações assumidas, ou por conveniência das partes, mediante notificação com antecedência de 30 (trinta) dias.

CLÁUSULA OITAVA – VIGÊNCIA O presente termo vigorará por tempo indeterminado, facultado às partes o exercício, a qualquer tempo, do direito potestativo referido na cláusula anterior. E por estarem justos e acordados, assinam o presente CONVËNIO DE COOPERAÇÃO TÉCNICA, CIENTÍFICA E OPERACIONAL em 03 (três) vias de igual teor e forma, na presença das testemunhas signatárias, para que se produzam os necessários efeitos jurídicos e legais. São Paulo, 29 de março de 2006.

ANEXO C

CONVENÇÃO DE BUDAPESTE SOBRE CIBERCRIME

CONVENTION ON CYBERCRIME

Budapest, 23.XI.2001

Preamble

The member States of the Council of Europe and the other States signatory hereto, Considering that the aim of the Council of Europe is to achieve a greater unity between its members; Recognising the value of fostering co-operation with the other States parties to this Convention; Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, *inter alia,* by adopting appropriate legislation and fostering international co-operation; Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks; Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks; Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies; Believing that an effective fight against cybercrime requires increased, rapid and wellfunctioning international co-operation in criminal matters; Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation; Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy; Mindful also of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data; Considering the 1989 United Nations Convention on the Rights of the Child and the

1999 International Labour Organization Worst Forms of Child Labour Convention; Taking into account the existing Council of Europe conventions on co-operation in the penal field, as well as similar treaties which exist between Council of Europe member States and other States, and stressing that the present Convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence; Welcoming recent developments which further advance international understanding and cooperation in combating cybercrime, including action taken by the United Nations, the OECD, the European Union and the G8; Recalling Committee of Ministers Recommendations No. R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, No. R (88) 2 on piracy in the field of copyright and neighbouring rights, No. R (87) 15 regulating the use of personal data in the police sector, No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, as well as No. R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and No. R (95) 13 concerning problems of criminal procedural law connected with information technology; Having regard to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, 10 and 11 June 1997), which recommended that the Committee of Ministers support the work on cybercrime carried out by the European Committee on Crime Problems (CDPC) in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation into such offences, as well as to Resolution No. 3 adopted at the 23rd Conference of the European Ministers of Justice (London, 8 and 9 June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions to enable the largest possible number of States to become parties to the Convention and acknowledged the need for a swift and efficient system of international co-operation, which duly takes into account the specific requirements of the fight against cybercrime; Having also regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe on the occasion of their Second Summit (Strasbourg, 10 and 11 October 1997), to seek common responses to the development of the new information technologies based on the standards and values of the Council of Europe; Have agreed as follows:

Chapter I – Use of terms

Article 1 – Definitions

For the purposes of this Convention: a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data; b “computer data” means any representation of facts, information or concepts in

a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function; c “service provider” means: i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service; d “traffic data” means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service.

Chapter II – Measures to be taken at the national level

Section 1 – Substantive criminal law

Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems

Article 2 – Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3 – Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4 – Data interference

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5 – System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering

without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 – Misuse of devices

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a the production, sale, procurement for use, import, distribution or otherwise making available of: i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

Title 2 – Computer-related offences

Article 7 – Computer-related forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 8 – Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a any input, alteration, deletion or suppression of computer data; b any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Title 3 – Content-related offences

Article 9 – Offences related to child pornography

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a producing child pornography for the purpose of its distribution through a computer system;

b offering or making available child pornography through a computer system;

c distributing or transmitting child pornography through a computer system;

d procuring child pornography through a computer system for oneself or for another person;

e possessing child pornography in a computer system or on a computer-data storage medium.

2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:

a a minor engaged in sexually explicit conduct;

b a person appearing to be a minor engaged in sexually explicit conduct;

c realistic images representing a minor engaged in sexually explicit conduct.

3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, subparagraphs d. and e, and 2, sub-paragraphs b. and c.

Title 4 – Offences related to infringements of copyright and related rights

Article 10 – Offences related to infringements of copyright and related rights

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

Title 5 – Ancillary liability and sanctions

Article 11 – Attempt and aiding or abetting

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7,8, and 9.1.a and c. of this Convention.

3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

Article 12 – Corporate liability

1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:

a a power of representation of the legal person;

b an authority to take decisions on behalf of the legal person;

c an authority to exercise control within the legal person.

2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.

4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

Article 13 – Sanctions and measures

1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

Section 2 – Procedural law

Title 1 – Common provisions

Article 14 – Scope of procedural provisions

1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.

2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

a the criminal offences established in accordance with Articles 2 through 11 of this Convention;

b other criminal offences committed by means of a computer system; and

c the collection of evidence in electronic form of a criminal offence.

3: a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.

b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:

I is being operated for the benefit of a closed group of users, and

II does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

Article 15 – Conditions and safeguards

1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

Title 2 – Expedited preservation of stored computer data

Article 16 – Expedited preservation of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 17 – Expedited preservation and partial disclosure of traffic data

1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:

a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and

b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 3 – Production order

Article 18 – Production order

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium;

b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

a the type of communication service used, the technical provisions taken thereto and the period of service;

b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Title 4 – Search and seizure of stored computer data

Article 19 – Search and seizure of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

a a computer system or part of it and computer data stored therein; and

b a computer-data storage medium in which computer data may be stored in its territory.

2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.

3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:

a seize or similarly secure a computer system or part of it or a computer-data storage medium;

b make and retain a copy of those computer data;

c maintain the integrity of the relevant stored computer data;

d render inaccessible or remove those computer data in the accessed computer system.

4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is

reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 5 – Real-time collection of computer data

Article 20 – Real-time collection of traffic data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

I to collect or record through the application of technical means on the territory of that Party; or

II to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 21 – Interception of content data

1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

I to collect or record through the application of technical means on the territory of that Party, or

II to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Section 3 – Jurisdiction

Article 22 – Jurisdiction

1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:

a in its territory; or

b on board a ship flying the flag of that Party; or

c on board an aircraft registered under the laws of that Party; or

d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.

3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

5 When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

Chapter III – International co-operation

Section 1 – General principles

Title 1 – General principles relating to international co-operation

Article 23 – General principles relating to international co-operation

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international cooperation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Title 2 – Principles relating to extradition

Article 24 – Extradition

1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.

b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.

2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.

3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.

4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.

6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.

7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.

b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

Title 3 – General principles relating to mutual assistance

Article 25 – General principles relating to mutual assistance

1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.

3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or email, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.

4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.

5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

Article 26 – Spontaneous information

1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.

2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless

be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

Title 4 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.

b The central authorities shall communicate directly with each other;

c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;

d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.

4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request.

The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).

c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.

e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

Article 28 – Confidentiality and limitation on use

1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:

a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or

b not used for investigations or proceedings other than those stated in the request.

3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.
4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

Section 2 – Specific provisions

Title 1 – Mutual assistance regarding provisional measures

Article 29 – Expedited preservation of stored computer data

1 A Party may request another Party to order or otherwise obtain the expeditious reservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.
2 A request for preservation made under paragraph 1 shall specify:
a the authority seeking the preservation;
b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;
c the stored computer data to be preserved and its relationship to the offence;
d any available information identifying the custodian of the stored computer data or the location of the computer system;
e the necessity of the preservation; and
f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.
3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.
4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.
5 In addition, a request for preservation may only be refused if:
a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

7 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data.

Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.

Article 30 – Expedited disclosure of preserved traffic data

1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

2 Disclosure of traffic data under paragraph 1 may only be withheld if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or

b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

Title 2 – Mutual assistance regarding investigative powers

Article 31 – Mutual assistance regarding accessing of stored computer data

1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.

2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.

3 The request shall be responded to on an expedited basis where:

a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or

b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

Article 32 – Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorisation of another Party:

a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Article 33 – Mutual assistance in the real-time collection of traffic data

1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.

2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

Article 34 – Mutual assistance regarding the interception of content data

The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.

Title 3 – 24/7 Network

Article 35 – 24/7 Network

1 Each Party shall designate a point of contact available on a twenty-four hour, sevenday- a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

a the provision of technical advice;

b the preservation of data pursuant to Articles 29 and 30;

c the collection of evidence, the provision of legal information, and locating of suspects.

2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.

b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

Chapter IV – Final provisions

Article 36 – Signature and entry into force

1 This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.

2 This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

3 This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

4 In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

Article 37 – Accession to the Convention

1 After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d. of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.

2 In respect of any State acceding to the Convention under paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 38 – Territorial application

1 Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.

2 Any State may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of the declaration by the Secretary General.

3 Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month

following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

Article 39 – Effects of the Convention

1 The purpose of the present Convention is to supplement applicable multilateral or bilateral treaties or arrangements as between the Parties, including the provisions of: – the European Convention on Extradition, opened for signature in Paris, on 13 December 1957 (ETS No. 24); – the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 20 April 1959 (ETS No. 30); – the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 17 March 1978 (ETS No. 99).

2 If two or more Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or have otherwise established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly. However, where Parties establish their relations in respect of the matters dealt with in the present Convention other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention's objectives and principles.

3 Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party.

Article 40 – Declarations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the possibility of requiring additional elements as provided for under Articles 2, 3, 6 paragraph 1.b, 7, 9 paragraph 3, and 27, paragraph 9.e.

Article 41 – Federal clause

1 A federal State may reserve the right to assume obligations under Chapter II of this Convention consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities provided that I is still able to co-operate under Chapter III.

2 When making a reservation under paragraph 1, a federal State may not apply the terms of such reservation to exclude or substantially diminish its obligations to provide for measures set forth in Chapter II. Overall, it shall provide for a broad and effective law enforcement capability with respect to those measures.

3 With regard to the provisions of this Convention, the application of which comes under the jurisdiction of constituent States or other similar territorial entities, that are not obliged by the constitutional system of the federation to take legislative measures, the federal government shall

inform the competent authorities of such States of the said provisions with its favourable opinion, encouraging them to take appropriate action to give them effect.

Article 42 – Reservations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article
29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

Article 43 – Status and withdrawal of reservations

1 A Party that has made a reservation in accordance with Article 42 may wholly or partially withdraw it by means of a notification addressed to the Secretary General of the Council of Europe. Such withdrawal shall take effect on the date of receipt of such notification by th Secretary General. If the notification states that the withdrawal of a reservation is to take effect on a date specified therein, and such date is later than the date on which the notification is received by the Secretary General, the withdrawal shall take effect on such a later date.

2 A Party that has made a reservation as referred to in Article 42 shall withdraw such reservation, in whole or in part, as soon as circumstances so permit.

3 The Secretary General of the Council of Europe may periodically enquire with Parties that have made one or more reservations as referred to in Article 42 as to the prospects for withdrawing such reservation(s).

Article 44 – Amendments

1 Amendments to this Convention may be proposed by any Party, and shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention as well as to any State which has acceded to, or has been invited to accede to, this Convention in accordance with the provisions of Article 37.

2 Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Committee of Ministers its opinion on that proposed amendment.

3 The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the CDPC and, following consultation with the non-member States Parties to this Convention, may adopt the amendment.

4 The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 of this article shall be forwarded to the Parties for acceptance.

5 Any amendment adopted in accordance with paragraph 3 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

Article 45 – Settlement of disputes

1 The European Committee on Crime Problems (CDPC) shall be kept informed regarding the interpretation and application of this Convention.

2 In case of a dispute between Parties as to the interpretation or application of this Convention, they shall seek a settlement of the dispute through negotiation or any other peaceful means of their choice, including submission of the dispute to the CDPC, to an arbitral tribunal whose decisions shall be binding upon the Parties, or to the International Court of Justice, as agreed upon by the Parties concerned.

Article 46 – Consultations of the Parties

1 The Parties shall, as appropriate, consult periodically with a view to facilitating: a the effective use and implementation of this Convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under this Convention; b the exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form; c consideration of possible supplementation or amendment of the Convention.

2 The European Committee on Crime Problems (CDPC) shall be kept periodically informe regarding the result of consultations referred to in paragraph 1.

3 The CDPC shall, as appropriate, facilitate the consultations referred to in paragraph 1 and take the measures necessary to assist the Parties in their efforts to supplement or amend the Convention. At the latest three years after the present Convention enters into force, the European Committee on Crime Problems (CDPC) shall, in co-operation with the Parties, conduct a review of all of the Convention's provisions and, if necessary, recommend any appropriate amendments.

4 Except where assumed by the Council of Europe, expenses incurred in carrying out the provisions of paragraph 1 shall be borne by the Parties in the manner to be determined by them.

5 The Parties shall be assisted by the Secretariat of the Council of Europe in carrying ou their functions pursuant to this article.

Article 47 – Denunciation

1 Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.

2 Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

Article 48 – Notification

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of this Convention as

well as any State which has acceded to, or has been invited to accede to, this Convention of: a any signature; b the deposit of any instrument of ratification, acceptance, approval or accession; c any date of entry into force of this Convention in accordance with Articles 36 and 37; d any declaration made under Article 40 or reservation made in accordance with Article 42; e any other act, notification or communication relating to this Convention. In witness whereof the undersigned, being duly authorised thereto, have signed this Convention. Done at Budapest, this 23rd day of November 2001, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention, and to any State invite to accede to it.

ANEXO D

LEI PENAL PORTUGUESA SOBRE CIBERCRIME

ASSEMBLEIA DA REPÚBLICA Lei n.º 109/2009 de 15 de Setembro Aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa. A Assembleia da República decreta, nos termos da alínea *c*) do artigo 161.º da Constituição, o seguinte:

CAPÍTULO I

Objecto e definições

Artigo 1.º **Objecto** A presente lei estabelece as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte electrónico, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adaptando o direito interno à Convenção sobre Cibercrime do Conselho da Europa. Artigo 2.º **Definições** Para efeitos da presente lei, considera -se: *a*) «Sistema informático», qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, protecção e manutenção; *b*) «Dados informáticos», qualquer representação de factos, informações ou conceitos sob uma forma susceptível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função; *c*) «Dados de tráfego», os dados informáticos relacionados com uma comunicação efectuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajecto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente; *d*) «Fornecedor de serviço», qualquer entidade, pública ou privada, que faculte aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema informático, bem como qualquer outra entidade que trate ou armazene dados informáticos em nome e por conta daquela entidade fornecedora de serviço ou dos respectivos utilizadores; *e*) «Intercepção», o acto destinado a captar informações contidas num sistema informático, através de dispositivos electromagnéticos, acústicos, mecânicos ou outros; *f*) «Topografia», uma série de imagens ligadas entre si, independentemente do modo como são fixadas ou codificadas, que representam a configuração

tridimensional das camadas que compõem um produto semicondutor e na qual cada imagem reproduz o desenho, ou parte dele, de uma superfície do produto semicondutor, independentemente da fase do respectivo fabrico; *g*) «Produto semicondutor», a forma final ou intermédia de qualquer produto, composto por um substrato que inclua uma camada de material semicondutor e constituído por uma ou várias camadas de matérias condutoras, isolantes ou semicondutoras, segundo uma disposição conforme a uma configuração tridimensional e destinada a cumprir, exclusivamente ou não, uma função electrónica.

CAPÍTULO II

Disposições penais materiais

Artigo 3.º **Falsidade informática** 1 — Quem, com intenção de provocar engano nas relações jurídicas, introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos, com a intenção de que estes sejam considerados ou utilizados para finalidades juridicamente relevantes como se o fossem, é punido com pena de prisão até 5 anos ou multa de 120 a 600 dias. **6320** *Diário da República, 1.ª série — N.º 179 — 15 de Setembro de 2009* 2 — Quando as acções descritas no número anterior incidirem sobre os dados registados ou incorporados em cartão bancário de pagamento ou em qualquer outro dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, a pena é de 1 a 5 anos de prisão. 3 — Quem, actuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiro, usar documento produzido a partir de dados informáticos que foram objecto dos actos referidos no n.º 1 ou cartão ou outro dispositivo no qual se encontrem registados ou incorporados os dados objecto dos actos referidos no número anterior, é punido com as penas previstas num e noutro número, respectivamente. 4 — Quem importar, distribuir, vender ou detiver para fins comerciais qualquer dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, sobre o qual tenha sido praticada qualquer das acções prevista no n.º 2, é punido com pena de prisão de 1 a 5 anos. 5 — Se os factos referidos nos números anteriores forem praticados por funcionário no exercício das suas funções, a pena é de prisão de 2 a 5 anos. Artigo 4.º

Dano relativo a programas ou outros dados informáticos 1 — Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, apagar, alterar, destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis ou não acessíveis programas ou outros dados informáticos alheios ou por qualquer forma lhes afectar a capacidade de uso, é punido com pena de prisão até 3 anos ou pena de multa. 2 — A tentativa é punível. 3 — Incorre na mesma pena do n.º 1 quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos,

programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas nesse número. 4 — Se o dano causado for de valor elevado, a pena é de prisão até 5 anos ou de multa até 600 dias. 5 — Se o dano causado for de valor consideravelmente elevado, a pena é de prisão de 1 a 10 anos. 6 — Nos casos previstos nos n.os 1, 2 e 4 o procedimento penal depende de queixa. Artigo 5.º **Sabotagem informática** 1 — Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, entravar, impedir, interromper ou perturbar gravemente o funcionamento de um sistema informático, através da introdução, transmissão, deterioração, danificação, alteração, apagamento, impedimento do acesso ou supressão de programas ou outros dados informáticos ou de qualquer outra forma de interferência em sistema informático, é punido com pena de prisão até 5 anos ou com pena de multa até 600 dias. 2 — Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no número anterior. 3 — Nos casos previstos no número anterior, a tentativa não é punível. 4 — A pena é de prisão de 1 a 5 anos se o dano emergente da perturbação for de valor elevado. 5 — A pena é de prisão de 1 a 10 anos se: *a*) O dano emergente da perturbação for de valor consideravelmente elevado; *b*) A perturbação causada atingir de forma grave ou duradoura um sistema informático que apoie uma actividade destinada a assegurar funções sociais críticas, nomeadamente as cadeias de abastecimento, a saúde, a segurança e o bem -estar económico das pessoas, ou o funcionamento regular dos serviços públicos. Artigo 6.º **Acesso ilegítimo** 1 — Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, de qualquer modo aceder a um sistema informático, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias. 2 — Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no número anterior. 3 — A pena é de prisão até 3 anos ou multa se o acesso for conseguido através de violação de regras de segurança. 4 — A pena é de prisão de 1 a 5 anos quando: *a*) Através do acesso, o agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei; ou *b*) O benefício ou vantagem patrimonial obtidos forem de valor consideravelmente elevado. 5 — A tentativa é punível, salvo nos casos previstos no n.º 2. 6 — Nos casos previstos nos n.os 1, 3 e 5 o procedimento penal depende de queixa. Artigo 7.º **Intercepção ilegítima** 1 — Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, e através de meios técnicos, interceptar transmissões de dados informáticos que se processam no interior de um sistema informático, a ele destinadas ou dele provenientes, é punido com pena de prisão até 3 anos ou com

pena de multa. 2 — A tentativa é punível. 3 — Incorre na mesma pena prevista no n.º 1 quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no mesmo número. *Diário da República, 1.ª série — N.º 179 — 15 de Setembro de 2009* **6321**Artigo 8.º **Reprodução ilegítima de programa protegido**1 — Quem ilegitimamente reproduzir, divulgar ou comunicar ao público um programa informático protegido por lei é punido com pena de prisão até 3 anos ou com pena de multa. 2 — Na mesma pena incorre quem ilegitimamente reproduzir topografia de um produto semicondutor ou a explorar comercialmente ou importar, para estes fins, uma topografia ou um produto semicondutor fabricado a partir dessa topografia. 3 — A tentativa é punível. Artigo 9.º**Responsabilidade penal das pessoas colectivas e entidades equiparadas** As pessoas colectivas e entidades equiparadas são penalmente responsáveis pelos crimes previstos na presente lei nos termos e limites do regime de responsabilização previsto no Código Penal.Artigo 10.º **Perda de bens** 1 — O tribunal pode decretar a perda a favor do Estado dos objectos, materiais, equipamentos ou dispositivos que tiverem servido para a prática dos crimes previstos na presente lei e pertencerem a pessoa que tenha sido condenada pela sua prática. 2 — À avaliação, utilização, alienação e indemnização de bens apreendidos pelos órgãos de polícia criminal que sejam susceptíveis de vir a ser declarados perdidos a favor do Estado é aplicável o disposto no Decreto – Lei n.º 11/2007, de 19 de Janeiro.

CAPÍTULO III

Disposições processuais Artigo 11.º **Âmbito de aplicação das disposições processuais** 1 — Com excepção do disposto nos artigos 18.º e 19.º, as disposições processuais previstas no presente capítulo aplicam -se a processos relativos a crimes: *a*) Previstos na presente lei; *b*) Cometidos por meio de um sistema informático; ou *c*) Em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico. 2 — As disposições processuais previstas no presente capítulo não prejudicam o regime da Lei n.º 32/2008, de 17 de Julho. Artigo 12.º **Preservação expedita de dados** 1 — Se no decurso do processo for necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos armazenados num sistema informático, incluindo dados de tráfego, em relação aos quais haja receio de que possam perder -se, alterar -se ou deixar de estar disponíveis, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados, designadamente a fornecedor de serviço, que preserve os dados em causa. 2 — A preservação pode também ser ordenada pelo órgão de polícia criminal mediante autorização da autoridade judiciária competente ou quando haja urgência ou perigo na demora, devendo aquele, neste último caso, dar notícia imediata do facto à autoridade judiciária e transmitir -lhe o relatório previsto no artigo 253.º do Código de Processo Penal. 3 — A ordem de

preservação discrimina, sob pena de nulidade: *a*) A natureza dos dados; *b*) A sua origem e destino, se forem conhecidos; e *c*) O período de tempo pelo qual deverão ser preservados, até um máximo de três meses. 4 — Em cumprimento de ordem de preservação que lhe seja dirigida, quem tenha disponibilidade ou controlo sobre esses dados, designadamente o fornecedor de serviço, preserva de imediato os dados em causa, protegendo e conservando a sua integridade pelo tempo fixado, de modo a permitir à autoridade judiciária competente a sua obtenção, e fica obrigado a assegurar a confidencialidade da aplicação da medida processual. 5 — A autoridade judiciária competente pode ordenar a renovação da medida por períodos sujeitos ao limite previsto na alínea *c*) do n.º 3, desde que se verifiquem os respectivos requisitos de admissibilidade, até ao limite máximo de um ano. Artigo 13.º **Revelação expedita de dados de tráfego** Tendo em vista assegurar a preservação dos dados de tráfego relativos a uma determinada comunicação, independentemente do número de fornecedores de serviço que nela participaram, o fornecedor de serviço a quem essa preservação tenha sido ordenada nos termos do artigo anterior indica à autoridade judiciária ou ao órgão de polícia criminal, logo que o souber, outros fornecedores de serviço através dos quais aquela comunicação tenha sido efectuada, tendo em vista permitir identificar todos os fornecedores de serviço e a via através da qual aquela comunicação foi efectuada. Artigo 14.º **Injunção para apresentação ou concessão do acesso a dados** 1 — Se no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados que os comunique ao processo ou que permita o acesso aos mesmos, sob pena de punição por desobediência. 2 — A ordem referida no número anterior identifica os dados em causa. 3 — Em cumprimento da ordem descrita nos n.os 1 e 2, quem tenha disponibilidade ou controlo desses dados comunica esses dados à autoridade judiciária competente ou permite, sob pena de punição por desobediência, o acesso ao sistema informático onde os mesmos estão armazenados. **6322** *Diário da República, 1.ª série — N.º 179 — 15 de Setembro de 2009* 4 — O disposto no presente artigo é aplicável a fornecedores de serviço, a quem pode ser ordenado que comuniquem ao processo dados relativos aos seus clientes ou assinantes, neles se incluindo qualquer informação diferente dos dados relativos ao tráfego ou ao conteúdo, contida sob a forma de dados informáticos ou sob qualquer outra forma, detida pelo fornecedor de serviços, e que permita determinar: *a*) O tipo de serviço de comunicação utilizado, as medidas técnicas tomadas a esse respeito e o período de serviço; *b*) A identidade, a morada postal ou geográfica e o número de telefone do assinante, e qualquer outro número de acesso, os dados respeitantes à facturação e ao pagamento, disponíveis com base num contrato ou acordo de serviços; ou *c*) Qualquer outra informação sobre a localização do equipamento de comunicação, disponível com base num contrato ou acordo de serviços. 5 — A injunção prevista no presente artigo não pode ser dirigida a suspeito ou arguido nesse processo. 6

— Não pode igualmente fazer -se uso da injunção prevista neste artigo quanto a sistemas informáticos utilizados para o exercício da advocacia, das actividades médica e bancária e da profissão de jornalista. 7 — O regime de segredo profissional ou de funcionário e de segredo de Estado previsto no artigo 182.º do Código de Processo Penal é aplicável com as necessárias adaptações. Artigo 15.º **Pesquisa de dados informáticos** 1 — Quando no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente autoriza ou ordena por despacho que se proceda a uma pesquisa nesse sistema informático, devendo, sempre que possível, presidir à diligência. 2 — O despacho previsto no número anterior tem um prazo de validade máximo de 30 dias, sob pena de nulidade. 3 — O órgão de polícia criminal pode proceder à pesquisa, sem prévia autorização da autoridade judiciária, quando: *a*) A mesma for voluntariamente consentida por quem tiver a disponibilidade ou controlo desses dados, desde que o consentimento prestado fique, por qualquer forma, documentado; *b*) Nos casos de terrorismo, criminalidade violenta ou altamente organizada, quando haja fundados indícios da prática iminente de crime que ponha em grave risco a vida ou a integridade de qualquer pessoa. 4 — Quando o órgão de polícia criminal proceder à pesquisa nos termos do número anterior: *a*) No caso previsto na alínea *b*), a realização da diligência é, sob pena de nulidade, imediatamente comunicada à autoridade judiciária competente e por esta apreciada em ordem à sua validação; *b*) Em qualquer caso, é elaborado e remetido à autoridade judiciária competente o relatório previsto no artigo 253.º do Código de Processo Penal. 5 — Quando, no decurso de pesquisa, surgirem razões para crer que os dados procurados se encontram noutro sistema informático, ou numa parte diferente do sistema pesquisado, mas que tais dados são legitimamente acessíveis a partir do sistema inicial, a pesquisa pode ser estendida mediante autorização ou ordem da autoridade competente , nos termos dos n.os 1 e 2. 6 — À pesquisa a que se refere este artigo são aplicáveis, com as necessárias adaptações, as regras de execução das buscas previstas no Código de Processo Penal e no Estatuto do Jornalista. Artigo 16.º **Apreensão de dados informáticos** 1 — Quando, no decurso de uma pesquisa informática ou de outro acesso legítimo a um sistema informático, forem encontrados dados ou documentos informáticos necessários à produção de prova, tendo em vista a descoberta da verdade, a autoridade judiciária competente autoriza ou ordena por despacho a apreensão dos mesmos. 2 — O órgão de polícia criminal pode efectuar apreensões, sem prévia autorização da autoridade judiciária, no decurso de pesquisa informática legitimamente ordenada e executada nos termos do artigo anterior, bem como quando haja urgência ou perigo na demora. 3 — Caso sejam apreendidos dados ou documentos informáticos cujo conteúdo seja susceptível de revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade do respectivo titular ou de terceiro, sob pena de nulidade esses dados ou documentos são apresentados ao juiz, que ponderará a sua junção aos autos tendo em conta os

interesses do caso concreto. 4 — As apreensões efectuadas por órgão de polícia criminal são sempre sujeitas a validação pela autoridade judiciária, no prazo máximo de 72 horas. 5 — As apreensões relativas a sistemas informáticos utilizados para o exercício da advocacia e das actividades médica e bancária estão sujeitas, com as necessárias adaptações, às regras e formalidades previstas no Código de Processo Penal e as relativas a sistemas informáticos utilizados para o exercício da profissão de jornalista estão sujeitas, com as necessárias adaptações, às regras e formalidades previstas no Estatuto do Jornalista. 6 — O regime de segredo profissional ou de funcionário e de segredo de Estado previsto no artigo 182.º do Código de Processo Penal é aplicável com as necessárias adaptações. 7 — A apreensão de dados informáticos, consoante seja mais adequado e proporcional, tendo em conta os interesses do caso concreto, pode, nomeadamente, revestir as formas seguintes: *a*) Apreensão do suporte onde está instalado o sistema ou apreensão do suporte onde estão armazenados os dados informáticos, bem como dos dispositivos necessários à respectiva leitura; *b*) Realização de uma cópia dos dados, em suporte autónomo, que será junto ao processo; *c*) Preservação, por meios tecnológicos, da integridade dos dados, sem realização de cópia nem remoção dos mesmos; ou *d*) Eliminação não reversível ou bloqueio do acesso aos dados. *Diário da República, 1.ª série — N.º 179 — 15 de Setembro de 2009* **6323** 8 — No caso da apreensão efectuada nos termos da alínea *b*) do número anterior, a cópia é efectuada em duplicado, sendo uma das cópias selada e confiada ao secretário judicial dos serviços onde o processo correr os seus termos e, se tal for tecnicamente possível, os dados apreendidos são certificados por meio de assinatura digital. Artigo 17.º **Apreensão de correio electrónico e registos de comunicações de natureza semelhante** Quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio electrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, aplicando -se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal. Artigo 18.º**Intercepção de comunicações** 1 — É admissível o recurso à intercepção de comunicações em processos relativos a crimes: *a*) Previstos na presente lei; ou *b*) Cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico, quando tais crimes se encontrem previstos no artigo 187.º do Código de Processo Penal. 2 — A intercepção e o registo de transmissões de dados informáticos só podem ser autorizados durante o inquérito, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter, por despacho fundamentado do juiz de instrução e mediante requerimento do Ministério Público. 3 — A intercepção pode destinar -se ao registo de dados relativos ao conteúdo das comunicações ou visar apenas a recolha e registo

de dados de tráfego, devendo o despacho referido no número anterior especificar o respectivo âmbito, de acordo com as necessidades concretas da investigação. 4 — Em tudo o que não for contrariado pelo presente artigo, à intercepção e registo de transmissões de dados informáticos é aplicável o regime da intercepção e gravação de conversações ou comunicações telefónicas constante dos artigos 187.º, 188.º e 190.º do Código de Processo Penal. Artigo 19.º **Acções encobertas** 1 — É admissível o recurso às acções encobertas previstas na Lei n.º 101/2001, de 25 de Agosto, nos termos aí previstos, no decurso de inquérito relativo aos seguintes crimes: *a*) Os previstos na presente lei; *b*) Os cometidos por meio de um sistema informático, quando lhes corresponda, em abstracto, pena de prisão de máximo superior a 5 anos ou, ainda que a pena seja inferior, e sendo dolosos, os crimes contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes, a burla qualificada, a burla informática e nas comunicações, a discriminação racial, religiosa ou sexual, as infracções económico -financeiras, bem como os crimes consagrados no título IV do Código do Direito de Autor e dos Direitos Conexos. 2 — Sendo necessário o recurso a meios e dispositivos informáticos observam-se, naquilo que for aplicável, as regras previstas para a intercepção de comunicações.

CAPÍTULO IV

Cooperação internacional

Artigo 20.º **Âmbito da cooperação internacional** As autoridades nacionais competentes cooperam com as autoridades estrangeiras competentes para efeitos de investigações ou procedimentos respeitantes a crimes relacionados com sistemas ou dados informáticos, bem como para efeitos de recolha de prova, em suporte electrónico, de um crime, de acordo com as normas sobre transferência de dados pessoais previstas na Lei n.º 67/98, de 26 de Outubro. Artigo 21.º **Ponto de contacto permanente para a cooperação internacional** 1 — Para fins de cooperação internacional, tendo em vista a prestação de assistência imediata para os efeitos referidos no artigo anterior, a Polícia Judiciária assegura a manutenção de uma estrutura que garante um ponto de contacto disponível em permanência, vinte e quatro horas por dia, sete dias por semana. 2 — Este ponto de contacto pode ser contactado por outros pontos de contacto, nos termos de acordos, tratados ou convenções a que Portugal se encontre vinculado, ou em cumprimento de protocolos de cooperação internacional com organismos judiciários ou policiais. 3 — A assistência imediata prestada por este ponto de contacto permanente inclui: *a*) A prestação de aconselhamento técnico a outros pontos de contacto; *b*) A preservação expedita de dados nos casos de urgência ou perigo na demora, em conformidade com o disposto no artigo seguinte; *c*) A recolha de prova para a qual seja competente nos casos de urgência ou perigo na demora; *d*) A localização de suspeitos e a prestação de informações de carácter jurídico, nos casos de urgência ou perigo na demora; *e*) A transmissão imediata ao Ministério Público de pedidos relativos às medidas referidas nas alíneas *b*) a *d*), fora

dos casos aí previstos, tendo em vista a sua rápida execução. 4 — Sempre que actue ao abrigo das alíneas *b*) a *d*) *d*o número anterior, a Polícia Judiciária dá notícia imediata do facto ao Ministério Público e remete -lhe o relatório previsto no artigo 253.º do Código de Processo Penal. **6324** *Diário da República, 1.ª série — N.º 179 — 15 de Setembro de 2009* Artigo 22.º **Preservação e revelação expeditas de dados informáticos em cooperação internacional** 1 — Pode ser solicitada a Portugal a preservação expedita de dados informáticos armazenados em sistema informático aqui localizado, relativos a crimes previstos no artigo 11.º, com vista à apresentação de um pedido de auxílio judiciário para fins de pesquisa, apreensão e divulgação dos mesmos. 2 — A solicitação especifica: *a*) A autoridade que pede a preservação; *b*) A infracção que é objecto de investigação ou procedimento criminal, bem como uma breve exposição dos factos relacionados; *c*) Os dados informáticos a conservar e a sua relação com a infracção; *d*) Todas as informações disponíveis que permitam identificar o responsável pelos dados informáticos ou a localização do sistema informático; *e*) A necessidade da medida de preservação; e *f*) A intenção de apresentação de um pedido de auxílio judiciário para fins de pesquisa, apreensão e divulgação dos dados. 3 — Em execução de solicitação de autoridade estrangeira competente nos termos dos números anteriores, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados, designadamente a fornecedor de serviço, que os preserve. 4 — A preservação pode também ser ordenada pelaPolícia Judiciária mediante autorização da autoridade judiciária competente ou quando haja urgência ou perigo na demora, sendo aplicável, neste último caso, o disposto no n.º 4 do artigo anterior. 5 — A ordem de preservação especifica, sob pena de nulidade: *a*) A natureza dos dados; *b*) Se forem conhecidos, a origem e o destino dos mesmos; e *c*) O período de tempo pelo qual os dados devem ser preservados, até um máximo de três meses. 6 — Em cumprimento de ordem de preservação que lhe seja dirigida, quem tem disponibilidade ou controlo desses dados, designadamente o fornecedor de serviço, preserva de imediato os dados em causa pelo período de tempo especificado, protegendo e conservando a sua integridade. 7 — A autoridade judiciária competente, ou a Polícia Judiciária mediante autorização daquela autoridade, podem ordenar a renovação da medida por períodos sujeitos ao limite previsto na alínea *c*) do n.º 5, desde que se verifiquem os respectivos requisitos de admissibilidade, até ao limite máximo de um ano. 8 — Quando seja apresentado o pedido de auxílio referido no n.º 1, a autoridade judiciária competente para dele decidir determina a preservação dos dados até à adopção de uma decisão final sobre o pedido. 9 — Os dados preservados ao abrigo do presente artigo apenas podem ser fornecidos: *a*) À autoridade judiciária competente, em execução do pedido de auxílio referido no n.º 1, nos mesmos termos em que poderiam sê -lo, em caso nacional semelhante, ao abrigo dos artigos 13.º a 17.º; *b*) À autoridade nacional que emitiu a ordem de preservação, nos mesmos termos em que poderiam sê -lo, em caso nacional semelhante, ao abrigo do artigo 13.º 10 — A autoridade nacional à qual, nos termos do número anterior, sejam comunicados dados de tráfego identificadores de fornecedor de

serviço e da via através dos quais a comunicação foi efectuada, comunica -os rapidamente à autoridade requerente, por forma a permitir a essa autoridade a apresentação de nova solicitação de preservação expedita de dados informáticos. 11 — O disposto nos n.os 1 e 2 aplica -se, com as devidas adaptações, aos pedidos formulados pelas autoridades portuguesas. Artigo 23.º **Motivos de recusa** 1 — A solicitação de preservação ou revelação expeditas de dados informáticos é recusada quando: *a*) Os dados informáticos em causa respeitarem a infracção de natureza política ou infracção conexa segundo as concepções do direito português; *b*) Atentar contra a soberania, segurança, ordem pública ou outros interesses da República Portuguesa, constitucionalmente definidos; *c*) O Estado terceiro requisitante não oferecer garantias adequadas de protecção dos dados pessoais. 2 — A solicitação de preservação expedita de dados informáticos pode ainda ser recusada quando houver fundadas razões para crer que a execução de pedido de auxílio judiciário subsequente para fins de pesquisa, apreensão e divulgação de tais dados será recusado por ausência de verificação do requisito da dupla incriminação. Artigo 24.º **Acesso a dados informáticos em cooperação internacional** 1 — Em execução de pedido de autoridade estrangeira competente, a autoridade judiciária competente pode proceder à pesquisa, apreensão e divulgação de dados informáticos armazenados em sistema informático localizado em Portugal, relativos a crimes previstos no artigo 11.º, quando se trata de situação em que a pesquisa e apreensão são admissíveis em caso nacional semelhante. 2 — A autoridade judiciária competente procede com a maior rapidez possível quando existam razões para crer que os dados informáticos em causa são especialmente vulneráveis à perda ou modificação ou quando a cooperação rápida se encontre prevista em instrumento internacional aplicável. 3 — O disposto no n.º 1 aplica -se, com as devidas adaptações, aos pedidos formulados pelas autoridades judiciárias portuguesas. Artigo 25.º **Acesso transfronteiriço a dados informáticos armazenadosquando publicamente disponíveis ou com consentimento** As autoridades estrangeiras competentes, sem necessidade de pedido prévio às autoridades portuguesas, de acordo com as normas sobre transferência de dados pessoais previstas na Lei n.º 67/98, de 26 de Outubro, podem: *a*) Aceder a dados informáticos armazenados em sistema informático localizado em Portugal, quando publicamente disponíveis; *Diário da República, 1.ª série — N.º 179 — 15 de Setembro de 2009* **6325** *b*) Receber ou aceder, através de sistema informático localizado no seu território, a dados informáticos armazenados em Portugal, mediante consentimento legal e voluntário de pessoa legalmente autorizada a divulgá -los. Artigo 26.º **Intercepção de comunicações em cooperação internacional** 1 — Em execução de pedido da autoridade estrangeira competente, pode ser autorizada pelo juiz a intercepção de transmissões de dados informáticos realizadas por via de um sistema informático localizado em Portugal, desde que tal esteja previsto em acordo, tratado ou convenção internacional e se trate de situação em que tal intercepção seja admissível, nos termos do artigo 18.º, em caso nacional semelhante. 2 — É competente para a recepção dos pedidos de intercepção a Polícia Judiciária, que os apresentará ao

Ministério Público, para que os apresente ao juiz de instrução criminal da comarca de Lisboa para autorização. 3 — O despacho de autorização referido no artigo anterior permite também a transmissão imediata da comunicação para o Estado requerente, se tal procedimento estiver previsto no acordo, tratado ou convenção internacional com base no qual é feito o pedido. 4 — O disposto no n.º 1 aplica -se, com as devidas adaptações, aos pedidos formulados pelas autoridades judiciárias portuguesas.

CAPÍTULO V

Disposições finais e transitórias

Artigo 27.º **Aplicação no espaço da lei penal portuguesa e competência dos tribunais portugueses** 1 — Para além do disposto no Código Penal em matéria de aplicação no espaço da lei penal portuguesa, e salvo tratado ou convenção internacional em contrário, para efeitos da presente lei, a lei penal portuguesa é ainda aplicável a factos: *a*) Praticados por Portugueses, se aos mesmos não for aplicável a lei penal de nenhum outro Estado; *b*) Cometidos em benefício de pessoas colectivas com sede em território português; *c*) Fisicamente praticados em território português, ainda que visem sistemas informáticos localizados fora desse território; ou *d*) Que visem sistemas informáticos localizados em território português, independentemente do local onde esses factos forem fisicamente praticados. 2 — Se, em função da aplicabilidade da lei penal portuguesa, forem simultaneamente competentes para conhecer de um dos crimes previstos na presente lei os tribunais portugueses e os tribunais de outro Estado membro da União Europeia, podendo em qualquer um deles ser validamente instaurado ou prosseguido o procedimento penal com base nos mesmos factos, a autoridade judiciária competente recorre aos órgãos e mecanismos instituídos no seio da União Europeia para facilitar a cooperação entre as autoridades judiciárias dos Estados membros e a coordenação das respectivas acções, por forma a decidir qual dos dois Estados instaura ou prossegue o procedimento contra os agentes da infracção, tendo em vista centralizá -lo num só deles. 3 — A decisão de aceitação ou transmissão do procedimento é tomada pela autoridade judiciária competente, tendo em conta, sucessivamente, os seguintes elementos: *a*) O local onde foi praticada a infracção; *b*) A nacionalidade do autor dos factos; e *c*) O local onde o autor dos factos foi encontrado. 4 — São aplicáveis aos crimes previstos na presente lei as regras gerais de competência dos tribunais previstas no Código de Processo Penal. 5 — Em caso de dúvida quanto ao tribunal territorialmente competente, designadamente por não coincidirem o local onde fisicamente o agente actuou e o local onde está fisicamente instalado o sistema informático visado com a sua actuação, a competência cabe ao tribunal onde primeiro tiver havido notícia dos factos. Artigo 28.º **Regime geral aplicável** Em tudo o que não contrarie o disposto na presente lei, aplicam -se aos crimes, às medidas processuais e à cooperação internacional em matéria penal nela previstos, respectivamente, as disposições do Código Penal, do Código de Processo Penal e da Lei

n.º 144/99, de 31 de Agosto. Artigo 29.º **Competência da Polícia Judiciária para a cooperação internacional** A competência atribuída pela presente lei à Polícia Judiciária para efeitos de cooperação internacional é desempenhada pela unidade orgânica a quem se encontra cometida a investigação dos crimes previstos na presente lei. Artigo 30.º **Protecção de dados pessoais** O tratamento de dados pessoais ao abrigo da presente lei efectua -se de acordo com o disposto na Lei n.º 67/98, de 26 de Outubro, sendo aplicável, em caso de violação, o disposto no respectivo capítulo VI. Artigo 31.º **Norma revogatória** É revogada a Lei n.º 109/91, de 17 de Agosto. Artigo 32.º **Entrada em vigor** A presente lei entra em vigor 30 dias após a sua publicação. Aprovada em 23 de Julho de 2009. O Presidente da Assembleia da República, *Jaime Gama.* Promulgada em 29 de Agosto de 2009. Publique –se O Presidente da República, ANÍBAL CAVACO SILVA. Referendada em 31 de Agosto de 2009. O Primeiro -Ministro, *José Sócrates Carvalho Pinto de Sousa.*

ANEXO E

LEI ARGENTINA SOBRE CIBERCRIME

CODIGO PENAL

Ley 26.388

Modificación.

Sancionada: Junio 4 de 2008

Promulgada de Hecho: Junio 24 de 2008

El Senado y Cámara de Diputados de la Nación Argentina reunidos en Congreso, etc. sancionan con fuerza de Ley:

ARTICULO 1º — Incorpóranse como últimos párrafos del artículo 77 del Código Penal, los siguientes:

El término "documento" comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión.

Los términos "firma" y "suscripción" comprenden la firma digital, la creación de una firma digital o firmar digitalmente.

Los términos "instrumento privado" y "certificado" comprenden el documento digital firmado digitalmente.

ARTICULO 2º — Sustitúyese el artículo 128 del Código Penal, por el siguiente:

Artículo 128: Será reprimido con prisión de seis (6) meses a cuatro (4) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores.

Será reprimido con prisión de cuatro (4) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización.

Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años.

ARTICULO 3º — Sustitúyese el epígrafe del Capítulo III, del Título V, del Libro II del Código Penal, por el siguiente:

"Violación de Secretos y de la Privacidad"

ARTICULO 4º — Sustitúyese el artículo 153 del Código Penal, por el siguiente:

Artículo 153: Será reprimido con prisión de quince (15) días a seis (6) meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.

En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido.

La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica.

Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena.

ARTICULO 5º — Incorpórase como artículo 153 bis del Código Penal, el siguiente:

Artículo 153 bis: Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.

La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.

ARTICULO 6º — Sustitúyese el artículo 155 del Código Penal, por el siguiente:

Artículo 155: Será reprimido con multa de pesos un mil quinientos ($ 1.500) a pesos cien mil ($ 100.000), el que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros.

Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público.

ARTICULO 7º — Sustitúyese el artículo 157 del Código Penal, por el siguiente:

Artículo 157: Será reprimido con prisión de un (1) mes a dos (2) años e inhabilitación especial de un (1) a cuatro (4) años, el funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos.

ARTICULO 8º — Sustitúyese el artículo 157 bis del Código Penal, por el siguiente:

Artículo 157 bis: Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que:

1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;

2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.
3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.
Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4) años.

ARTICULO 9º — Incorpórase como inciso 16 del artículo 173 del Código Penal, el siguiente:
Inciso 16. El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.

ARTICULO 10. — Incorpórase como segundo párrafo del artículo 183 del Código Penal, el siguiente:
En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños.

ARTICULO 11. — Sustitúyese el artículo 184 del Código Penal, por el siguiente:
Artículo 184: La pena será de tres (3) meses a cuatro (4) años de prisión, si mediare cualquiera de las circunstancias siguientes:
1. Ejecutar el hecho con el fin de impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones;
2. Producir infección o contagio en aves u otros animales domésticos;
3. Emplear substancias venenosas o corrosivas;
4. Cometer el delito en despoblado y en banda;
5. Ejecutarlo en archivos, registros, bibliotecas, museos o en puentes, caminos, paseos u otros bienes de uso público; o en tumbas, signos conmemorativos, monumentos, estatuas, cuadros u otros objetos de arte colocados en edificios o lugares públicos; o en datos, documentos, programas o sistemas informáticos públicos;
6. Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público.

ARTICULO 12. — Sustitúyese el artículo 197 del Código Penal, por el siguiente:
Artículo 197: Será reprimido con prisión de seis (6) meses a dos (2) años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida.

ARTICULO 13. — Sustitúyese el artículo 255 del Código Penal, por el siguiente:
Artículo 255: Será reprimido con prisión de un (1) mes a cuatro (4) años, el que sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o

de otra persona en el interés del servicio público. Si el autor fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo.

Si el hecho se cometiere por imprudencia o negligencia del depositario, éste será reprimido con multa de pesos setecientos cincuenta ($ 750) a pesos doce mil quinientos ($ 12.500).

ARTICULO 14. — Deróganse el artículo 78 bis y el inciso 1º del artículo 117 bis del Código Penal.

ARTICULO 15. — Comuníquese al Poder Ejecutivo.

DADA EN LA SALA DE SESIONES DEL CONGRESO ARGENTINO, EN BUENOS AIRES, A LOS CUATRO DIAS DEL MES DE JUNIO DEL AÑO DOS MIL OCHO.

— REGISTRADO BAJO EL Nº 26.388 —

EDUARDO A. FELLNER. — JULIO C. C. COBOS. — Enrique Hidalgo. — Juan H. Estrada.

ANEXO F

LEI CHILENA SOBRE CIBERCRIME

Tipo Norma: Ley 19223
Fecha Publicación: 07-06-1993
Fecha Promulgación: 28-05-1993
Organismo: MINISTERIO DE JUSTICIA
Título: TIPIFICA FIGURAS PENALES RELATIVAS A LA INFORMATICA
Tipo Version: Unica De: 07-06-1993
Inicio Vigencia: 07-06-1993
Id Norma: 30590
URL: http://www.leychile.cl/N?i=30590&f=1993-06-07&p

TIPIFICA FIGURAS PENALES RELATIVAS A LA INFORMATICA

Teniendo presente que el H. Congreso Nacional ha dado su aprobación al Siguiente Proyecto de Ley:

"Artículo 1°.- El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo. Si como consecuencia de estas conductas se afectaren los datos contenidos en El sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.

Artículo 2°.- El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.

Artículo 3°.- El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presídio menor en su grado medio.

Artículo 4°.- El que maliciosamente revele o difunda los datos contenidos en um sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado"..

Y por cuanto he tenido a bien aprobarlo y sancionarlo; por tanto promúlguese y llévese a efecto como Ley de la República.

Santiago, 28 de Mayo de 1993.- ENRIQUE KRAUSS RUSQUE, Vicepresidente de la República.- Francisco Cumplido Cereceda, Ministro de Justicia. Lo que transcribo a Ud. para su conocimiento.- Saluda atentamente a Ud., Martita Worner Tapia, Subsecretario de Justicia.

ANEXO G

PROJETO DE LEI SUBSTITUTIVO SENADOR EDUARDO AZEREDO

Substitutivo do Senado ao Projeto de Lei da Câmara nº 89, de 2003 (PL nº 84, de 1999, na Casa de origem), que "Altera o Decreto- Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal e a Lei nº 9.296, de 24 de julho de 1996, e dá outras providências".

Substitua-se o Projeto pelo seguinte:

Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), o Decreto-Lei nº .001, de 21 de outubro de 1969 (Código Penal Militar), a Lei nº 7.716, de 5 de janeiro de 1989, a Lei nº 8.069, de 13 de julho de 1990, e a Lei nº 10.446, de 8 de maio de 2002, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares, e dá outras providências.

O Congresso Nacional decreta:

Art. 1º Esta Lei altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), o Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), a Lei nº 7.716, de 5 de janeiro de 1989, a Lei nº 8.069, de 13 de julho de 1990, e a Lei nº 10.446, de 8 de maio de 2002, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares, e dá outras providências.

Art. 2º O Título VIII da Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) fica acrescido do Capítulo IV, com a seguinte redação:

"CAPÍTULO IV

DOS CRIMES CONTRA A SEGURANÇA DOS SISTEMAS INFORMATIZADOS

Acesso não autorizado a rede de computadores, dispositivo de comunicação ou sistema informatizado

Art. 285-A. Acessar, mediante violação de segurança, rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso:

Pena - reclusão, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único. Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte. Obtenção, transferência ou fornecimento não autorizado de dado ou informação

Art. 285-B. Obter ou transferir, sem autorização ou em desconformidade com autorização do legítimo titular da rede de computadores, dispositivo de comunicação ou sistema informatizado,

protegidos por expressa restrição de acesso, dado ou informação neles disponível:

Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único. Se o dado ou informação obtida desautorizadamente é fornecida a terceiros, a pena é aumentada de um terço.

Ação Penal

Art. 285-C. Nos crimes definidos neste Capítulo somente se procede mediante representação, salvo se o crime é cometido contra a União, Estado, Município, empresa concessionária de serviços públicos, agências, fundações, autarquias, empresas públicas ou sociedade de economia mista e subsidiárias".

Art. 3º O Título I da Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) fica acrescido do seguinte artigo, com a seguinte redação:

"Divulgação ou utilização indevida de informações e dados pessoais

Art. 154-A. Divulgar, utilizar, comercializar ou disponibilizar dados e informações pessoais contidas em sistema informatizado com finalidade distinta da que motivou seu registro, salvo nos casos previstos em lei ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal:

Pena – detenção, de 1 (um) a 2 (dois) anos, e multa.

Parágrafo único. Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte".

Art. 4º O caput do art. 163 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) passa a vigorar com a seguinte redação:

"Dano

Art. 163. Destruir, inutilizar ou deteriorar coisa alheia ou dado eletrônico alheio:

.....". (NR)

Art. 5º O Capítulo IV do Título II da Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) fica acrescido do art. 163-A, assim redigido:

"Inserção ou difusão de código malicioso

Art. 163-A. Inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado:

Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.

Inserção ou difusão de código malicioso seguido de dano

§ 1º Se do crime resulta destruição, inutilização, deterioração, alteração, dificultação do funcionamento, ou funcionamento desautorizado pelo legítimo titular, de dispositivo de comunicação, de rede de computadores, ou de sistema informatizado:

Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa.

§ 2º Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte".

Art. 6º O art. 171 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) passa a vigorar acrescido dos seguintes dispositivos:

"Art. 171. .....

.....

§ 2º Nas mesmas penas incorre quem:

.....

Estelionato Eletrônico

VII – difunde, por qualquer meio, código malicioso com intuito de facilitar ou permitir acesso indevido à rede de computadores, dispositivo de comunicação ou sistema informatizado.

§ 3º Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime previsto no inciso VII do § 2º, a pena é aumentada de sexta parte". (NR)

Art. 7º Os arts. 265 e 266 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) passam a vigorar com as seguintes redações:

"Atentado contra a segurança de serviço de utilidade pública

Art. 265. Atentar contra a segurança ou o funcionamento de serviço de água, luz, força, calor, informação ou telecomunicação, ou qualquer outro de utilidade pública:

.....". (NR)

"Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático, dispositivo de comunicação, rede de computadores ou sistema informatizado

Art. 266. Interromper ou perturbar serviço telegráfico, radiotelegráfico, telefônico, telemático, informático, de dispositivo de comunicação, de rede de computadores, de sistema informatizado ou de telecomunicação, assim como impedir ou dificultar-lhe o restabelecimento:

.....". (NR)

Art. 8º O caput do art. 297 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) passa a vigorar com a seguinte redação:

"Falsificação de dado eletrônico ou documento público

Art. 297. Falsificar, no todo ou em parte, dado eletrônico ou documento público, ou alterar documento público verdadeiro:

.....". (NR)

Art. 9º O caput do art. 298 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) passa a vigorar com a seguinte redação:

"Falsificação de dado eletrônico ou documento particular

Art. 298. Falsificar, no todo ou em parte, dado eletrônico ou documento particular ou alterar documento particular verdadeiro:

.....". (NR)

Art. 10. O art. 251 do Capítulo IV do Título V da Parte Especial do Livro I do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), passa a vigorar acrescido do inciso VI ao seu § 1º, e do § 4º, com a seguinte redação:

"Art. 251. .....

§ 1º Nas mesmas penas incorre quem:

.....

Estelionato Eletrônico

VI - Difunde, por qualquer meio, código malicioso com o intuito de facilitar ou permitir o acesso indevido a rede de computadores, dispositivo de comunicação ou a sistema informatizado, em prejuízo da administração militar.

.....

§ 4º Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte". (NR)

Art. 11. O caput do art. 259 e o caput do art. 262 do Capítulo VII do Título V da Parte Especial do Livro I do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), passam a vigorar com a seguinte redação:

"Dano Simples

Art. 259. Destruir, inutilizar, deteriorar ou fazer desaparecer coisa alheia ou dado eletrônico alheio, desde que este esteja sob administração militar:

.....". (NR)

"Dano em material ou aparelhamento de guerra ou dado eletrônico

Art. 262. Praticar dano em material ou aparelhamento de guerra ou dado eletrônico de utilidade militar, ainda que em construção ou fabricação, ou em efeitos recolhidos a depósito, pertencentes ou não às forças armadas:

.....". (NR)

Art. 12. O Capítulo VII do Título V da Parte Especial do Livro I do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), fica acrescido do art. 262-A, com a seguinte redação:

"Inserção ou difusão de código malicioso

Art. 262-A. Inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado, desde que o fato atente contra a administração militar:

Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.

Inserção ou difusão de código malicioso seguido de dano

§ 1º Se do crime resulta destruição, inutilização, deterioração, alteração, dificultação do funcionamento, ou funcionamento não autorizado pelo titular, de dispositivo de comunicação, de rede de computadores, ou de sistema informatizado:

Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa.

§ 2º Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte".

Art. 13. O Título VII da Parte Especial do Livro I do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), fica acrescido do Capítulo VIII, com a seguinte redação:

"CAPÍTULO VIII

DOS CRIMES CONTRA A SEGURANÇA DOS SISTEMAS INFORMATIZADOS

Acesso não autorizado a rede de computadores, dispositivo de comunicação ou sistema informatizado

Art. 339-A. Acessar, mediante violação de segurança, rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso, desde que o fato atente contra a administração militar:

Pena - reclusão, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único. Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte.

Obtenção, transferência ou fornecimento não autorizado de dado ou informação

Art. 339-B. Obter ou transferir, sem autorização ou em desconformidade com autorização do legítimo titular da rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso, dado ou informação neles disponível, desde que o fato atente contra a administração militar:

Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único. Se o dado ou informação obtida desautorizadamente é fornecida a terceiros, a pena é aumentada de um terço.

Divulgação ou utilização indevida de informações e dados pessoais

Art. 339-C. Divulgar, utilizar, comercializar ou disponibilizar dados e informações pessoais contidas em sistema informatizado sob administração militar com finalidade distinta da que motivou seu registro, salvo nos casos previstos em lei ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal:

Pena – detenção, de 1 (um) a 2 (dois) anos, e multa.

Parágrafo único. Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte".

Art. 14. O caput do art. 311 do Capítulo V do Título VII do Livro I da Parte Especial do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), passa a vigorar com a seguinte redação:

“Falsificação de documento

Art. 311. Falsificar, no todo ou em parte, documento público ou particular, ou dado eletrônico ou alterar documento verdadeiro, desde que o fato atente contra a administração ou o serviço militar:

.....”. (NR)

Art. 15. Os incisos II e III do art. 356 do Capítulo I do Título I do Livro II da Parte Especial do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), passam a vigorar com a seguinte redação:

“CAPÍTULO I

DA TRAIÇÃO

Favor ao inimigo

Art. 356. .....

II - entregando ao inimigo ou expondo a perigo dessa conseqüência navio, aeronave, força ou posição, engenho de guerra motomecanizado, provisões, dado eletrônico ou qualquer outro elemento de ação militar;

III - perdendo, destruindo, inutilizando, deteriorando ou expondo a perigo de perda, destruição, inutilização ou deterioração, navio, aeronave, engenho de guerra motomecanizado, provisões, dado eletrônico ou qualquer outro elemento de ação militar.

.....”. (NR)

Art. 16. Para os efeitos penais considera-se, dentre outros:

I – dispositivo de comunicação: qualquer meio capaz de processar, armazenar, capturar ou transmitir dados utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia;

II – sistema informatizado: qualquer sistema capaz de processar, capturar, armazenar ou transmitir dados eletrônica ou digitalmente ou de forma equivalente;

III – rede de computadores: o conjunto de computadores, dispositivos de comunicação e sistemas informatizados, que obedecem a um conjunto de regras, parâmetros, códigos, formatos e outras informações agrupadas em protocolos, em nível topológico local, regional, nacional ou mundial através dos quais é possível trocar dados e informações;

IV – código malicioso: o conjunto de instruções e tabelas de informações ou qualquer outro sistema desenvolvido para executar ações danosas ou obter dados ou informações de forma indevida;

V – dados informáticos: qualquer representação de fatos, de informações ou de conceitos sob forma suscetível de processamento numa rede de computadores ou dispositivo de comunicação ou sistema informatizado;

VI – dados de tráfego: todos os dados informáticos relacionados com sua comunicação efetuada por meio de uma rede de computadores, sistema informatizado ou dispositivo de comunicação, gerados por eles como elemento de uma cadeia de comunicação, indicando origem da

comunicação, o destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente.

Art. 17. Para efeitos penais consideram-se também como bens protegidos o dado, o dispositivo de comunicação, a rede de computadores, o sistema informatizado.

Art. 18. Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.

Art. 19. O inciso II do § 3º do art. 20 da Lei nº 7.716, de 5 de janeiro de 1989, passa a vigorar com a seguinte redação:

"Art. 20 .....

.....

§ 3º.....

.....

II – a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas, ou da publicação por qualquer meio.

.....". (NR)

Art. 20. O caput do art. 241 da Lei nº 8.069, de 13 de julho de 1990, passa a vigorar com a seguinte redação:

"Art. 241. Apresentar, produzir, vender, receptar, fornecer, divulgar, publicar ou armazenar consigo, por qualquer meio de comunicação, inclusive rede mundial de computadores ou Internet, fotografias, imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente:

.....". (NR)

Art. 21. O art. 1º da Lei nº 10.446, de 8 de maio de 2002, passa a vigorar com a seguinte redação:

"Art. 1º

.....

V – os delitos praticados contra ou mediante rede de computadores, dispositivo de comunicação ou sistema informatizado.

.....". (NR)

Art. 22. O responsável pelo provimento de acesso a rede de computadores mundial, comercial ou do setor público é obrigado a:

I – manter em ambiente controlado e de segurança, pelo prazo de 3 (três) anos, com o objetivo de provimento de investigação pública formalizada, os dados de endereçamento eletrônico da origem, hora, data e a referência GMT da conexão efetuada por meio de rede de computadores e fornecê-los exclusivamente à autoridade investigatória mediante prévia requisição judicial;

II – preservar imediatamente, após requisição judicial, outras informações requisitadas em curso de investigação, respondendo civil e penalmente pela sua absoluta confidencialidade e inviolabilidade;
III – informar, de maneira sigilosa, à autoridade competente, denúncia que tenha recebido e que contenha indícios da prática de crime sujeito a acionamento penal público incondicionado, cuja perpetração haja ocorrido no âmbito da rede de computadores sob sua responsabilidade.

§ 1º Os dados de que cuida o inciso I deste artigo, as condições de segurança de sua guarda, a auditoria à qual serão submetidos e a autoridade competente responsável pela auditoria, serão definidos nos termos de regulamento.

§ 2º O responsável citado no caput deste artigo, independentemente do ressarcimento por perdas e danos ao lesado, estará sujeito ao pagamento de multa variável de R$ 2.000,00 (dois mil reais) a R$ 100.000,00 (cem mil reais) a cada requisição, aplicada em dobro em caso de reincidência, que será imposta pela autoridade judicial desatendida, considerando-se a natureza, a gravidade e o prejuízo resultante da infração, assegurada a oportunidade de ampla defesa e contraditório.

§ 3º Os recursos financeiros resultantes do recolhimento das multas estabelecidas neste artigo serão destinados ao Fundo Nacional de Segurança Pública, de que trata a Lei nº 10.201, de 14 de fevereiro de 2001.

Art. 23. Esta Lei entra em vigor 120 (cento e vinte) dias após a data de sua publicação.

Senado Federal, em de julho de 2008

Senador Garibaldi Alves Filho

Presidente do Senado Federal

vpl/plc03-089