VANESSA COPETTI CRAVO

CRIMES CIBERNÉTICOS E AS PRINCIPAIS INICIATIVAS REGIONAIS E INTERNACIONAIS

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Direito da Faculdade de Direito da Universidade Federal do Rio Grande do Sul como requisito final para a obtenção do título de Mestre em Direito.

Orientador: Dr. TUPINAMBÁ PINTO DE AZEVEDO

PORTO ALEGRE

2011

TERMO DE APROVAÇÃO

Vanessa Copetti Cravo, autora da Dissertação de Mestrado intitulada Crimes Cibernéticos e as Principais Iniciativas Regionais e Internacionais, apresentada como requisito final para a obtenção do título de Mestre em Direito no Programa de Pós-Graduação em Direito da Faculdade de Direito da Universidade Federal do Rio Grande do Sul, submeteu-se à banca avaliadora na data abaixo, sendo aprovada.

Porto Alegre, _____ de _____ de 2012.

_____

Prof° Dr. Tupinambá Pinto de Azevedo

_____

_____

_____

Aos meus pais e irmãos, agradeço pela compreensão e pelo auxílio. Ao William, pelo companheirismo e apoio na busca de meus objetivos. À minha filha Laura que domina meus pensamentos e motiva-me a conquistar esse título.

Agradeço à Agência Nacional de Telecomunicações – Anatel que proporcionou a minha participação no Curso de Pós-Graduação Stricto Senso – Mestrado em Direito, concedendo-me horário especial para a frequentar às disciplinas e afastamento parcial para a elaboração da dissertação, acreditando no potencial dos seus servidores, investindo na capacitação e aprimoramento de seu mais importante recurso. Ao meu orientador, Prof.° Dr. Tupinambá Pinto de Azevedo, agradeço pela orientação, pela instigação e, acima de tudo, pelo exemplo profssional e de vida.

RESUMO

A universalização do acesso e do uso das Tecnologias de Informação e Comunicação - TICs, especialmente da Internet, tem sido acompanhada pelo crescimento exponencial dos incidentes de segurança e dos crimes cibernéticos, os quais comprometem a confiança e a segurança na utilização destas tecnologias, tão essenciais para a nossa sociedade contemporânea. Estes delitos, ainda que objeto das mais variadas terminologias, representam o mesmo amplo fenômeno que é geralmente definido pela prática de condutas contra estas tecnologias e/ou pela utilização das mesmas para a execução de crimes. Ou seja, as TICs podem ser o alvo da conduta criminosa ou a ferramenta para a execução da infração. A característica mais marcante dessa nova categoria de crimes é justamente a sua transnacionalidade, visto que, com grande facilidade, rapidez e sem demandar demasiados recursos humanos e financeiros, a execução da conduta delituosa e/ou o seu resultado atingem inúmeros países, tornando impossível a sua prevenção e repressão sem cooperação internacional. A transnacionalidade aliada ao grande potencial lesivo destas condutas exige um enfrentamento internacional do problema, o qual tem sido objeto dos esforços de diversas organizações regionais e internacionais desde a Década de 90, acentuados a partir da virada do século, notadamente de órgãos e agência integrantes do Sistema das Nações Unidas (Assembléia Geral das Nações Unidas, Escritório das Nações Unidas sobre Drogas e Crime e União Internacional de Telecomunicações), do Conselho da Europa e da Organização para a Cooperação e Desenvolvimento Econômico, cuja evolução dos estudos, discussões e iniciativas pode viabilizar a negociação de um tratado internacional.

PALAVRAS-CHAVE: Crimes Cibernéticos. Segurança Cibernética. Iniciativas Regionais e Internacionais.

ABSTRACT

The universal access and use of the Information and Communication Technologies - ICTs, especially the Internet has been followed by exponential growth of security incidents and cybercrimes, which undermine the trust and the confidence in using these technologies, that are so essential to our contemporary society. Although these crimes have been named with several terminologies, they do describe the same and broad phenomenon that is generally defined as actions committed against these technologies and/or the use of ICTs to perpetrate crimes. In other words, ICTs can be the target of the criminal conduct or the tool that is used to commit the offense. The most striking feature of this new category of crimes is precisely the fact that they are borderless and their execution and/or their results can affect, easily, quickly and without demanding too many human and financial resources, many countries, making it impossible to prevent and prosecute them without international cooperation. Due to the fact that they are borderless and potentially harmful, these behaviors require an international approach to deal with this problem, being subject of the efforts of various regional and international organizations since the 90's, accented from the turn of the century, especially of the organs and agencies of the United Nations System (United Nations General Assembly, United Nations Office on Drugs and Crime and the International Telecommunication Union), of the Council of Europe and of the Organization for Economic Co-operation and Development, whose studies, discussions and initiatives can evolve to the negotiation of an international treaty.

KEYWORDS: Cybercrime. Cybersecurity. Regional and International Initiatives**.**

LISTA DE SIGLAS E ABREVIATURAS

AGNU – Assembléia Geral das Nações Unidas

AGSC - Agenda Global de Segurança Cibernética

CMDT - Conferência Mundial de Desenvolvimento das Telecomunicações

CMSI – Cúpula Mundial sobre a Sociedade da Informação

DSIC - Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República.

COE – Conselho da Europa

GEAN - Grupo de Experts de Alto Nível

GOOGLE - Google Brasil Internet Ltda.

ICCP - Comitê sobre Políticas de Informação, Computadores e Comunicação da OCDE

ICI - Infraestruturas Críticas da Informação

MIT - Massachusets Institute of Technology

MP – Ministério Público

MPF – Ministério Público Federal

OCDE – Organização para a Cooperação e Desenvolvimento Econômico

ONU – Organização das Nações Unidas

SI – Sociedade da Informação

TAC – Termo de Ajustamento de Conduta

TICs – Tecnologias de Informação e Comunicação

UNODC - Escritório das Nações Unidas sobre Drogas e Crime

UIT – União Internacional de Telecomunicações

UIT-D – Setor de Desenvolvimento das Telecomunicações da UIT

UIT-R – Setor de Radiocomunicação da UIT

UIT-T – Setor de Normalização das Telecomunicações da UIT

WPISP - Grupo de Trabalho sobre Segurança da Informação e Privacidade do ICCP da OCDE

SUMÁRIO

INTRODUÇÃO

Os crimes cibernéticos representam um dos maiores desafios da atualidade, uma vez que comprometem o desenvolvimento, a confiabilidade, a disponibilidade e a estabilidade da Rede Mundial de Computadores, que, em menos de duas décadas, tornou-se um dos bens mais importantes e indispensáveis da sociedade contemporânea.

Pode-se afirmar inclusive que, em uma visão mais pessimista, as infrações praticadas colocam em risco a continuidade da Internet, conforme hoje é conhecida, enquanto espaço destinado ao livre acesso à informação, ao conhecimento, à inovação, ao lazer, às relações sociais e aos negócios. Segundo Smith[1], a Internet conecta indivíduos, comunidades e mercados em maneiras que são totalmente novas, mudando a forma como nos comunicamos, como conduzimos negócios, como nos divertimos, como compramos e como educamos.

A ameaça dos crimes cibernéticos à Internet é demostrada com um raciocínio bastate simplista. Se as pessoas são vítimas de delitos como estelionato na Internet com frequência, é provável que reduzam ou até mesmo eliminem toda a sua atividade econômica na rede, prejudicando assim as atividades comerciais e bancárias que são crescentemente realizadas online. Da mesma forma, um indivíduo que seja vítima de um crime contra a honra em uma rede social, como injúria ou calúnia, pode até retirar-se desse espaço de convivência virtual. Além disso, pode-se também citar que os custos decorrentes das fraudes podem inviabilizar atividades comerciais, reduzindo portanto as funcionalidades do espaço virtual.

Assim, a efetiva prevenção e repressão dos ilícitos praticados na Internet, por meio dela ou contra ela, é um imperativo para que as finalidades da sua utilização não sejam limitadas em face da insegurança gerada por esta criminalidade.

A universalização do acesso e do uso da Internet está sendo, indevidamente, acompanhada pelo crescimento exponencial dos incidentes de segurança. As mais diversas técnicas utilizadas para causar dano, obter acesso não autorizado a dados e/ou obter algum proveito econômico ilicitamente, como vírus, *phishing, worns, trojan horses, spam*[2]*, scans,* dentre outras dezenas, fazem parte do cotidiano dos usuários mais atentos e preocupados com

---

[1] SMITH, Bradford L. The Third Industrial Revolution: Law and Policy for the Internet. *Recueil des cours de l'Académie de droit international de La Haye*, vol. 282, 2000. p. 229-464. p. 247.

[2] Cabe a ressalva inicial de que existe grande controvérsia sobre a caracterização do envio de *spam* como conduta criminosa, salientando-se que é considerado crime em diversos Estados dos Estados Unidos, onde a legislação penal é de competência estadual, tais como Virginia, Ohio, Maryland e Georgia. Sobre o combate ao *spam* nos Estados Unidos, ver: SCANLAN, Emma. The Fight to Save America's Inbox: State Legislation and Litigation in the Wake of CAN-SPAM, *2 Shidler J. L. Com. & Tech*, dez. 2005. 7 p. Disponível em: <http://www.lctjournal.washington.edu/Vol2/a012Scanlan.html>. Acesso em: 20/08/2011.

a integridade, disponibilidade e confiabilidade de suas informações, sendo estudadas ao longo do texto.

A segurança nacional e a defesa nacional também ganham novos contornos com a era cibernética, visto que a crescente interconectividade coloca novos desafios e episódios como o WikiLeaks e os ataques aos sites governamentais federais do Brasil pelo grupo de hackers LulzSecBrazil em junho de 2011 reacendem acaloradas discussões de como reprimir tais práticas. Destaca-se que hoje se fala até mesmo em guerra cibernética que seria a utilização das Tecnologias de Informação e Comunicação em guerras, temática também presente nas agendas diplomáticas internacionais e atual objeto de estudo de grupo de trabalho no âmbito da Organização do Tratado do Atlântico Norte (OTAN)[3], o qual prepara manual de direito internacional aplicável à guerra cibernética. Ainda que pertinentes, questões referentes à segurança nacional e guerra cibernética não são objeto desta dissertação, na medida em que exigem pesquisa específica.

Embora a universalização e o crescimento destas ameaças e delitos sejam incontestáveis, esta conjuntura não tem sido sustentada com a conscientização dos usuários sobre os riscos a que estão diariamente expostos, nem sobre as medidas que podem e devem ser tomadas para prevenir e responder aos incidentes. Da mesma maneira, nem todos os países promoveram a necessária adaptação, atualização e inovação legislativa de seus ordenamentos internos, não se preparando para lidar com os novos paradigmas impostos por essa nova categoria de crimes.

Diante do preocupante quadro, diversas organizações regionais e a comunidade internacional, principalmente a partir da virada do século, têm insistido na necessidade do enfrentamento coordenado do tema, que tem sido alvo constante de discussões, especialmente, no âmbito da Assembléia Geral das Nações Unidas (AGNU), do Escritório das Nações Unidas sobre Drogas e Crime (UNODC), da Cúpula Mundial sobre a Sociedade da Informação (CMSI), do Conselho da Europa (COE), da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) e da União Internacional de Telecomunicações (UIT).

Nota-se que a mobilização internacional, semelhante à verificada para o combate ao terrorismo, ao tráfico de entorpecentes e à lavagem de dinheiro, baseia-se no fato que esses

[3] Maiores informações podem ser obtidas na página do Centro de Excelência de Tallin, Estônia, de Defesa Cibernética Cooperativa da OTAN, disponível em: <http://www.ccdcoe.org/249.html>. Acesso em: 25/08/2011. Não é coincidência que o centro esteja situado justamente na Estônia, um dos casos clássicos de guerra cibernética, ocorrido em 2007. Sobre o caso da Estônia, ver artigo do The New York Times, Digital Fears Emerge After Data Siege in Estonia, disponível em: <http://www.nytimes.com/2007/05/29/technology/29estonia.html?ei=5070&en=2e77eb21a1ab42ac&ex=1188360000&pagewanted=print>. Acesso em: 29/11/2011.

crimes são essencialmente transnacionais e, consequentemente, a cooperação internacional é imprescindível para a sua prevenção e repressão.

A facilidade e a velocidade com que esta criminalidade ultrapassa fronteiras, envolvendo assim diversos países, tanto na execução quanto no resultado da ação, torna a transnacionalidade uma de suas marcantes características, expondo assim a questão de qual país possui jurisdição para a persecução criminal e impondo a necessidade de cooperação entre órgãos de segurança para a investigação da conduta.

Dessa forma, a pesquisa buscou compreender - o quê é - essa categoria de crimes e como é tratada pelo direito brasileiro, no intuito de que esses conhecimentos obtidos possam balizar o exame da reação na esfera regional e internacional, focada no trabalho das organizações mais atuantes.

Para tanto, dividiu-se esta dissertação em duas partes. A primeira é destinada a descrever o fenômeno dessa nova criminalidade. Aborda-se a terminologia utilizada, ressalvando a existência de nomenclatura diversa na doutrina para descrever o fenômeno, sendo escolhida para o presente trabalho a expressão "crimes cibernéticos", escolha justificada no texto.

Na sequência, apresenta-se uma compilação de definições obtidas na doutrina, visto que inexiste um conceito legal, e propõe-se um conceito de trabalho abrangente, a fim de abarcar todas as espécies, o qual compreende as condutas praticadas contra as Tecnologias de Informação e Comunicação e através delas, e evitar que a evolução tecnológica prejudique a sua aplicação. Como bem jurídico, após apresentar as opiniões de diversos autores, sustenta-se a existência de um bem jurídico difuso da segurança da informação, para o qual se busca preservar a sua integridade, disponibilidade e confidencialidade dessa informação, ao lado dos bens tradicionalmente protegidos pelo direito penal, tais como vida, honra e patrimônio.

Percebe-se que a diferença dos bens jurídicos protegidos decorre justamente da definição ampla desta criminalidade, que contempla as condutas praticadas contra estas tecnologias, nas quais o bem jurídico é a segurança da informação, e as condutas praticadas com a utilização destas tecnologias como ferramenta, nas quais os bens jurídicos protegidos são os bens tradicionais. Essa diferença reflete-se na classificação, que agrupa os crimes cibernéticos puros ou próprios (bem jurídico é a segurança da informação) e os crimes cibernéticos impuros ou impróprios (bens jurídicos tradicionalmente tutelados).

O histórico desses ilícitos remonta à Década de 60, mas é com a popularização do acesso e do uso destas tecnologias, especialmente com a Internet, que esta criminalidade ganha vulto e torna-se objeto de preocupação internacional.

Os crimes cibernéticos, fruto de uma sociedade de risco, globalizada e pós-moderna, possuem as seguintes características que serão explicadas ao longo do texto: transnacionalidade, inserção na macrocriminalidade, especialidade do agente, tendência à sofisticação, grande lesividade, difícil rastreabilidade e comprovação e a existência de cifra negra, impondo-se salientar o fato de que esses crimes não respeitam fronteiras nem jurisdições, possuindo um enorme potencial para causar danos.

Como sujeitos do crime, evidencia-se que qualquer pessoa, física ou jurídica, pode ser vítima. Já quanto ao sujeito ativo, qualquer indivíduo pode cometer o delito, ainda que possa ser vislumbrada uma tendência à especialidade do agente em face do emprego de tecnologia, existindo na doutrina uma terminologia específica de acordo com a técnica utilizada ou o foco dos crimes, a qual é descrita ao longo da dissertação. Ainda na primeira parte, após discorrer sobre o panorama geral desta criminalidade e relacionar as técnicas usadas (Parte I, A), contextualiza-se o combate desses ilícitos pelo Sistema Penal Brasileiro, mencionando, ainda que brevemente, jurisprudência, tipos penais que contemplam esses delitos e projetos de lei em trâmite no Congresso Nacional (Parte I, B), dentro dos quais se realça o Projeto de Lei n.° 84/1999, que tramita há mais de uma década no Congresso e está longe de obter consenso para lograr sua aprovação.

Desde já se assenta que o nosso sistema oferece resposta aos crimes tradicionalmente tutelados (crimes cibernéticos impuros ou impróprios), e uma resposta parcial aos crimes cibernéticos puros ou próprios, vez que já existem alguns tipos específicos no ordenamento nacional, restando o questionamento quanto à necessidade de tipificação de condutas ainda não criminalizadas e à proporcionalidade das penas para os crimes impuros, em face da sua lesividade.

Faz-se necessário esclarecer que o objeto desta pesquisa não abarca a análise material dos tipos penais, assunto que, por si só, ensejaria um trabalho específico, limitando-se a descrever as condutas que poderiam ser enquadradas nesta nova categoria, consoante doutrina nacional e internacional, a fim de viabilizar a compreensão da temática e possibilitar o exame das iniciativas regionais e internacionais.

Passando para a segunda parte, relata-se as maiores iniciativas e estudos de prevenção e repressão a essas infrações, no âmbito regional e internacional, a partir do trabalho desenvolvido pelos principais atores destas esferas, a saber, a Assembléia Geral das Nações Unidas, o Conselho da Europa, o Escritório das Nações Unidas sobre Drogas e Crime, a Organização para a Cooperação e Desenvolvimento Econômico e a União Internacional de Telecomunicações. Destaca-se ainda que esta segunda parte subdivide-se no exame dos

esforços realizados no seio do Sistema das Nações Unidas (Parte II, A) e no espaço de atuação de outras organizações (Parte II, B), abordando-se a Convenção do Conselho da Europa sobre Crimes Cibernético, único tratado cogente na matéria, ainda que regional e a posição brasileira sobre a possibilidade de adesão à mesma.

No âmbito das Nações Unidas, sobressai as resoluções da Assembléia Geral, órgão deliberativo máximo que desde 1998 tem se debruçado sobre o tópico do avanço tecnológico e os seus reflexos na questão de segurança, especialmente sobre o combate ao uso criminoso das Tecnologias de Informação e Comunicação e sobre a criação de uma cultura de segurança cibernética.

Evidencia-se que a agência especializada das Nações Unidas para estas tecnologias, a União Internacional das Telecomunicações recebeu um mandato da Cúpula Mundial para a Sociedade da Informação referente à segurança cibernética, incluindo a prevenção aos crimes cibernéticos, ampliando assim o escopo de atribuições da União, fazendo com que desenvolva diversas iniciativas focadas na sua *expertise* técnica, que incluem a coletânea de melhores práticas e legislação pertinente, assim como assistência aos países em desenvolvimento para que elaborem ou adaptem leis nacionais reprimindo tais delitos, como se verá ao longo do texto.

Ainda no contexto das Nações Unidas, tem-se o Escritório das Nações Unidas sobre Drogas e Crime, o qual deve fornecer assistência aos Estados para aperfeiçoamento da legislação nacional no tocante aos crimes cibernéticos por força da Declaração de Salvador do Décimo-Segundo Congresso sobre Prevenção ao Crime e Justiça Criminal, sendo encarregado pelo desenvolvimento de compreensivo estudo dessa criminalidade, atualmente em andamento, o qual permite obter importantes consensos que podem dar base a negociação internacional.

Já na última parte da dissertação, analisa-se as iniciativas do Conselho da Europa e da Organização para a Cooperação e Desenvolvimento Econômico. O primeiro é responsável pela Convenção de Budapeste, Convenção do Conselho da Europa sobre Crimes Cibernético, único tratado sobre crimes cibernéticos existente até o presente momento, documento regional com pretensão internacional que já data de 2001 e possui um protocolo adicional para os atos de natureza racista e xenófoba cometidos através de sistemas informáticos. Já o segundo tem tradição na edição de melhores práticas e recomendações e vem concentrando esforços na área de segurança da informação e privacidade, incluindo combate ao *spam*, fraudes na Internet, proteção das crianças na Intenet, vírus de computador, cooperação internacional, etc,

elaborando princípios para uma cultura de segurança cibernética, os quais foram inclusive adotados pela Assembléia Geral das Nações Unidas.

PARTE I: ANÁLISE DO FENÔMENO DOS CRIMES CIBERNÉTICOS E SUA CONTEXTUALIZAÇÃO NO SISTEMA PENAL BRASILEIRO

A: DESCRIÇÃO DA CRIMINALIDADE CIBERNÉTICA

Ao abordar a temática dos crimes cibernéticos, o primeiro esclarecimento que deve ser feito é justamente quanto à terminologia utilizada, uma vez que esse tipo de criminalidade é denominado na doutrina de diferentes formas, ainda que todas se refiram ao mesmo fenômeno. Desta maneira, verifica-se na literatura a utilização, geralmente como sinônimos[4], das seguintes nomenclaturas: crimes telemáticos, crimes informáticos, crimes de informática, crimes virtuais, crimes da Internet, crimes eletrônicos, crimes informacionais, crimes computacionais, crimes de computador, crimes do ciberespaço etc.

Adota-se a terminologia 'crimes cibernéticos' a fim de se obter uma uniformidade quanto à nomenclatura, visto que foi a denominação escolhida pelo Conselho da Europa (COE), pela União Internacional de Telecomunicações (UIT) e pelo Escritório das Nações Unidas sobre Drogas e Crime (UNODC) e são estes uns dos principais atores no tocante ao combate desta criminalidade na esfera regional e internacional, sendo estudados na segunda parte deste texto. Ademais, percebe-se a crescente utilização dessa terminologia na esfera nacional e internacional, sendo adotada pelos documentos dos órgãos e agências integrantes do Sistema das Nações Unidas[5].

Após essas rápidas notas sobre a terminologia adotada, faz-se necessário apontar um conceito para essa criminalidade[6], ressaltando-se o alerta de Cruz[7] de que o *nomem juris* só

---

[4] Existem autores que diferenciam as expressões. Para os fins de compreensão do presente trabalho são usadas como sinônimos.

[5] Ainda assim, registra-se aqui a opinião de VIANNA que julga ser uma denominação completamente equivocada. Nesse sentido ver VIANNA, Túlio Lima. *Fundamentos de Direito Penal Informático: do acesso não autorizado a sistemas computacionais.* Rio de Janeiro: Forense, 2003. 167 p. 11-12.

[6] Deve-se ressaltar a existência de autores que são contra uma definição formal dos crimes cibernéticos. Nesse sentido ALBUQUERQUE, Roberto Chacon de. *A Criminalidade Informática*. São Paulo: Editora Juarez de Oliveira, 2006. 264 p. p. 40, destaca a desvantagem de tentar conceituar o termo "crimes de informática", alegando que "Dificilmente, pode-se elaborar uma definição sucinta e precisa sem que se deixem dúvidas quer com relação ao seu objeto, quer com respeito à própria utilização da definição que lhe for conferida. A noção de crime informático envolve várias espécies de crimes. Não se deve adotar uma definição formal, estática, o que pode criar mais confusão que soluções". Na mesma linha, GOUVÊA, Sandra. O Direito na Era Digital: crimes praticados por meio da informática. Rio de Janeiro: Mauad, 1997. 164 p. p. 57, que afirma: "A doutrina mundial dificilmente chegará a uma definição uniforme, uma vez que o desenvolvimento tecnológico, assim como os bens eleitos para a proteção jurídica, variam de país para país". Por fim, recorda-se que a publicação da INTERNATIONAL TELECOMMUNICATION UNION. *Understanding Cybercrime: a guide for developing*

pode ser compreendido como uma categoria criminal, visto que abriga diversas espécies de delitos. Ensina a autora[8]:

> A criminalidade informática tem uma conceituação muito ampla, onde se reúnem diversas formas delitivas, apresentando diferentes formas de comissão, como também distintos são os bens jurídicos passíveis de lesão. Desse modo, é impossível limitarmo-nos a um conceito de delito informático como uma figura típica autônoma.

Lima[9] opta pela nomenclatura: crimes de computador, pois é este o instrumento básico para a execução desses crimes, apresentando a seguinte definição[10]:

> crimes de computador são qualquer conduta humana (omissiva ou comissiva) típica, antijurídica e culpável, em que a máquina computadorizada tenha sido utilizada e, de alguma forma, facilitado de sobremodo a execução ou a consumação da figura delituosa, ainda que cause um prejuízo a pessoas sem que necessariamente se beneficie o autor ou que, pelo contrário, produza um benefício ilícito a seu autor, embora não prejudique a vítima de forma direta ou indireta.

Daoun[11] conceitua os crimes cibernéticos como uma "ação típica e antijurídica cometida contra ou pela utilização de processamento automático de dados ou sua transmissão, englobando-se a rede mundial de computadores"[12]. I. S. Ferreira[13] entende que constitui crime de informática "toda ação típica, antijurídica e culpável cometida contra ou pela utilização de processamento automático de dados ou sua transmissão". A autora ensina que seu conceito difere pouco do proposto pela Organização para a Cooperação e Desenvolvimento Econômico (OCDE) na Década de 90, o qual é caracterizado como "qualquer comportamento ilegal, aético ou não autorizado envolvendo o processamento automático de dados e/ou transmissão de dados"[14].

---

countries. 225 p. p. 17-18. Disponível em: <http://www.itu.int /ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf>. Acesso em: 07/10/2009, destaca que as descrições mais refinadas correm o risco de excluir condutas consideradas crime em instrumentos internacionais, como a Convenção de Budapeste, que será estudada na segunda parte deste trabalho. Assim a publicação defende que não há problema na inexistência de uma definição de crimes cibernéticos, desde que o termo não seja utilizado com conotação legal.

[7] CRUZ, Danielle da Rocha. *Criminalidade Informática – Tipificação Penal das Condutas Ilícitas Realizadas com Cartões de Crédito***.** Rio de Janeiro: Forense, 2006. 224 p. p. 26.

[8] CRUZ, Op. Cit., p. 27-28.

[9] LIMA, Paulo Marco Ferreira. *Crimes de Computador e Segurança Computacional***.** Campinas: Millenium, 2007. 234 p. p. 24.

[10] LIMA, Op. Cit., p. 31.

[11] DAOUN, Alexandre Jean. Crimes Informáticos e o Papel do Direito Penal na Tecnologia da Informação. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.). *Direito & Internet: aspectos jurídicos relevantes.* Vol. II. São Paulo: Quartier Latin, 2008. 718 p. p. 173-183. p. 179.

[12] DAOUN, *Op. Cit*., p. 170.

[13] FERREIRA, Ivette Senise. A Criminalidade Informática. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.). *Direito & Internet: aspectos jurídicos relevantes*. 2 ed. São Paulo: Quartier Latin, 2005. 543 p. p. 237-267. p. 240.

[14] FERREIRA, Ivette. Op. Cit., p. 240.

Silva Júnior[15] propõe uma conceituação mais restrita, no seguinte sentido:

> Crimes informáticos são aqueles em que são acessados, inseridos, modificados ou danificados, de forma ilegal ou não autorizada, os dados e informações constantes de um sistema computacional, não importando para tanto, a maneira pela qual é feita o ataque.

Atenta para a nomenclatura utilizada, Silva[16] define como "ação ou omissão, típica, antijurídica e culpável, produzida por meio de atividades que envolvam dispositivos que integram o sistema informático". Aqui cabe mencionar que a autora utiliza-se da terminologia "sistema informático", na medida em que possui maior abrangência, abarcando tudo que integra os sistemas de computador e de informação[17].

Rosa[18] defende que o crime de informática seria aquela "conduta típica, ilícita e culpável, praticada sempre com a utilização de dispositivos de sistemas de processamento ou comunicação de dados, da qual poderá ou não suceder a obtenção de uma vantagem indevida e ilícita". Já para Corrêa[19] 'crimes digitais' "seriam todos aqueles relacionados às informações arquivadas ou em trânsito por computadores, sendo esses dados, acessados ilicitamente, usados para ameaçar ou fraudar; para tal prática é indispensável a utilização de um meio eletrônico".

Cabe mencionar a detalhada conceituação de Rossini[20]:

> Neste trabalho o conceito de "delito informático" poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade e a confidencialidade.

A publicação da UIT sobre crimes cibernéticos[21] sintetiza que uma das definições usuais para estes delitos o descreve como uma atividade em que os computadores são a ferramenta, o objeto ou o lugar da atividade criminosa.

---

[15] SILVA JÚNIOR, Délio Lins e. Crimes informáticos: sua vitimização e a questão do tipo objetivo. In: D'ÁVILA, Fábio Roberto; SOUZA, Paulo Vinicius Sporleder de (Coords.) *Direito Penal secundário*. São Paulo: RT e Coibra Editora, 2006. 506 p. p. 311-337. p. 315.

[16] SILVA, Rita de Cássia Lopes da. *Direito Penal e Sistema Informático*. São Paulo: Editora Revista dos Tribunais, 2003. 141 p. p. 58.

[17] SILVA, Op. Cit., p. 57.

[18] ROSA, Fabrízio. *Crimes de Informática*. 3 ed. São Paulo: Bookseller, 2007. 141 p. p. 58.

[19] CORRÊA, Gustavo Testa. *Aspectos Jurídicos da Internet*. 4 ed. rev. e atual. São Paulo: Saraiva, 2008. 151 p. p. 44-45.

[20] ROSSINI, Augusto. *Informática, Telemática e Direito Penal*. São Paulo: Memória Jurídica, 2004. 352 p. p. 110.

[21] Ver INTERNATIONAL TELECOMMUNICATION UNION, *Understanding*, p. 17: "*One common definition describes cybercrime as any activity in which computers or networks are a tool, a target or a place of criminal activity. One example for an international approach is Art. 1.1 of the Draft International Convention to Enhance*

Kurbalija[22] esclarece que o conceito desta criminalidade é uma das questões centrais, visto que tem impacto legal na abrangência dos delitos. Se o foco estiver em crimes cometidos contra sistemas de computadores, iria abarcar as seguintes condutas: acesso não autorizado, dano a dados de computador ou programas, sabotagem para evitar o funcionamento de sistemas de computador e redes, interceptação ilegal de dados, assim como espionagem de computador. Se a definição concentrar todos os delitos cometidos através da Internet e dos sistemas de computador, abraçaria um campo mais amplo de crime, incluindo, os da Convenção sobre Crimes Cibernéticos, que é objeto de exame da segunda parte deste estudo.

Keyser[23] menciona que o Departamento de Justiça dos Estados Unidos define crime de computador como qualquer violação de lei penal que envolva o conhecimento de informática para sua execução, investigação ou persecução. Ademais, o autor relembra que o computador pode ser o objeto da criminalidade, ou seja, o alvo, ou o sujeito do crime, em outras palavras, o lugar físico do ilícito; ou ainda, a fonte, ou a razão para uma forma única de perda de ativos[24].

Após a análise dos conceitos mencionados, propõe-se, com base na Teoria Tripartite do Crime, a seguinte definição: a categoria de crimes cibernéticos abarca toda conduta típica (ação ou omissão), antijurídica e culpável, executada com a utilização das Tecnologias de Informação e Comunicação (TICs) ou contra elas, pressupondo-se o processamento automático e/ou a transmissão de dados[25]. Nesse sentido, é importante conceituar as TICs,

---

Protection from Cyber Crime and Terrorism (CISAC) that points out that cybercrime refers to acts in respect to cyber systems. Some definitions try to take the objectives or intentions into account and define cybercrime more precisely, defining cybercrime as "computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks". Grifo não original.

[22] KURBALIJA, Jovan. *An Introduction to Internet Governance*. 164 p. DiploFoundation and National Internet Exchange of India (NIXI): 2008. Disponível em: <http://www.diplomacy.edu/poolbin.asp?IDPool=806>. Acesso em: 13/03/2011. p. 93-94: "*The definition of cybercrime is one of the core issues of cyberlaw, since it will uphold a practical legal result impact by also impacting the coverage of cybercrime. If the focus is on offences committed against computer systems, cybercrime would include: unauthorized access, damage to computer data or programs, sabotage to hinder the functioning of a computer system or network, unauthorized interception of data to, from, and within a system or network, as well as computer espionage. A definition of cybercrime as all crimes committed via the Internet and computer systems would include a broader range of crimes, including those specified in the Cybercrime Convention: computer-related fraud, infringements of copyright, child pornography, and network security*".

[23] KEYSER, Mike. The Council of Europe Convention on Cybercrime, *J. Transnational Law & Policy*, vol. 12:2, spring 2003, p. 287-326. p. 290-291. Disponível em: <http://www.law.fsu.edu/Journals/transnational/vol12_2/keyser.pdf>. Acesso em 20/03/2011.

[24] KEYSER, Op. Cit., p. 290-291.

[25] Dessa forma, exclui-se, casos em que estas TICs são utilizadas como armas para a prática de conduta criminosa, porém sem utilizar das suas características de tratamento automatizado das informações. Por exemplo, o caso em que o agente utiliza um notebook para golpear a cabeça da vítima, cometendo um homicídio. Neste caso, não houve na execução qualquer ato que importe na inclusão deste fato típico na categoria de crimes cibernéticos. No mesmo sentido, ROSA, *Op. Cit*., p. 57, ressalta que: "nem toda conduta praticada contra ou

como “tecnologias utilizadas para tratamento, organização e disseminação de informações”, consoante definição adotada pelo Programa da Sociedade de Informação, sob coordenação do Ministério da Ciência e Tecnologia, no Livro Verde[26]. Opta-se por TICs pela generalidade do conceito, a fim de acompanhar a evolução decorrente da convergência tecnológica.

No tocante ao bem jurídico tutelado existe grande discussão doutrinária. Silva[27] defende que seria a informação, podendo ser atingidos outros bens, conforme se extrai do trecho abaixo[28]:

> [...]nos delitos praticados com o uso do sistema informático, de regra, tem-se como bem jurídico tutelado a informação. No entanto, esta informação poderá traduzir-se em patrimônio, se a ação for ofensa ao patrimônio; em honra, se ofenderem a honra; e, assim, numa cadeia lógica e coerente, proteger-se-á o bem jurídico tutelado pela norma e que efetivamente corresponde à lesão provocada pela conduta praticada.

Para Daoun[29] o objeto a ser protegido é a segurança informática. Traz-se a cotejo[30]:

> a “segurança informática” torna-se um bem jurídico específico ensejador de tutela penal. O conceito protetivo está consubstanciado em elementos próprios, tais como integridade, disponibilidade e confidencialidade da informação, e já alcançam, em alguns segmentos do ordenamento, *status* de lei, como pode ser constatado no referido dispositivo da lei n.° 9.983/00, que impôs tratamento penal rígido para condutas praticadas no âmbito da administração pública, protegendo, expressamente, dados, banco de dados e sistemas informatizados, traduzindo exatamente a inquietude com a interpretação e a aplicação da lei aos conceitos de informática.

Da mesma forma, Rossini[31] vislumbra que os delitos telemáticos, espécie do gênero dos delitos informáticos, podem ser praticados remotamente com o uso das novas tecnologias, possuem um bem jurídico sempre presente direta ou indiretamente, qual seja a segurança informática[32]. Além disso, o autor destaca a natureza difusa deste bem jurídico e a importância da sua proteção pelo Direito Penal[33]:

> A Segurança Informática é um bem jurídico penal de natureza difusa, pois além de atingir indeterminado número de pessoas, gera conflituosidade entre elas ou grupos, e as empresas, grandes ou pequenas, embora todos, pessoas e

---

através de computador será um ‘crime de informática’. Basta exemplificarmos com aquele indivíduo que com uma marreta destrói um computador, cometendo um crime de dano, previsto no art. 163 do Código Penal, e não-informático...”.

[26] BRASIL. Ministério da Ciência e Tecnologia. *Sociedade da Informação no Brasil:* livro verde. Brasília, 2000. Disponível em: < http://www.socinfo.org.br/livro_verde/download.htm>. Acesso em: 15 /08/2008. 231 p. p. 176.

[27] SILVA, Op. Cit., p. 66.

[28] Id., Op. Cit., p. 66.

[29] DAOUN, Op. Cit., p. 182.

[30] Id., Op. Cit., p. 182.

[31] Id., Op. Cit., p. 249.

[32] Id., Op. Cit., p. 110.

[33] Id., Op. Cit., p. 249.

> empresas, possuam legítimos interesses de uso e fruição das estruturas e potencialidades da Rede Mundial de Computadores.
> Se o Direito Penal não garantir a Segurança Informática, apenas a utilização lúdica restará para a Rede, em prejuízo de atividades empresariais, comerciais, educacionais etc., que inquestionavelmente geram empregos e tributos, enfim, legítimos dividendos das mais variadas espécies, de forma que o Estado, através do direito de *ultima ratio*, deve efetivamente interferir na Internet, posto que os demais ramos do Direito não têm se apresentado eficazes a enfrentar as condutas indesejadas e prejudiciais praticadas por pessoas e empresas inescrupulosas, muitas delas ilícitos penais.

De maneira semelhante, Vianna[34] aponta que o bem penalmente tutelado é justamente a inviolabilidade das informações automatizadas (dados). Contrariamente, Cruz[35] questiona a possibilidade de elencar a informação informatizada como único bem jurídico a ser tutelado pela categoria dos crimes cibernéticos, uma vez que os delitos praticados com a utilização das TICs nem sempre têm por finalidade a violação dessas informações.

Na mesma esteira, Lima[36] enxerga como alvo do ataque da criminalidade informática diversos bens jurídicos já tradicionalmente protegidos pelo Direito Penal, tais como a liberdade e a intimidade, ressaltando que a evolução tecnológica provocou sua exposição. I. S. Ferreira[37] segue o mesmo rumo, ressaltando que a criminalidade cibernética utiliza-se de um sistema informático para "atentar contra um bem ou interesse juridicamente protegido, pertencente ele à ordem econômica, à liberdade individual, à honra, ao patrimônio público ou privado, etc".

Pinheiro[38] também admite a pluralidade de bens jurídicos tutelados ao afirmar a existência de distintas modalidades de crimes virtuais, justamente em decorrência do bem protegido.

Cita-se ainda que, para Albuquerque[39], seriam três as espécies de interesses jurídicos a serem tuteladas pelos crimes informáticos: disponibilidade de meios; integridade de sistemas e dados; e exclusividade de meios e de dados.

Embora não exista consenso acerca do bem jurídico que é lesionado pela criminalidade cibernética, parece assentado que nos casos em que as TICs não são o alvo da prática ilícita, não há que se falar em lesão à segurança informática, visto que são utilizadas

---

[34] VIANNA, *Fundamentos*, p. 10.
[35] CRUZ, Op. Cit., p. 28.
[36] LIMA, Op. Cit., p. 29.
[37] FERREIRA, Ivette, Op. Cit., p. 240.
[38] PINHEIRO, Patricia Peck. *Direito digital*. 2 ed. 2 tir. rev., atual. e ampl. São Paulo: Saraiva, 2008. 407 p. p. 251.
[39] ALBUQUERQUE, Op. Cit., p. 46-47.

como mero instrumento para a execução de crimes que já são usualmente reprimidos pelos ordenamentos jurídicos, pois atingem vida, patrimônio, honra, liberdade etc.

Como marco do surgimento dessa espécie de criminalidade, E. L. L. Ferreira[40] relata que a primeira infração cibernética foi cometida por um estudante de 18 anos do *Massachusets Institute of Technology* (MIT), em 1964 e recebeu como punição uma advertência dos superiores. Na mesma linha Albuquerque[41] ensina:

> O primeiro caso de crime informático remonta à década de sessenta, quando os primeiros relatos apareceram na imprensa. Eles incluíam, basicamente, a utilização do computador como instrumento para a prática de crimes com projeção econômica, como o estelionato. A partir da década de setenta, apareceram os primeiros estudos empíricos sobre a criminalidade informática. Eles lançaram luzes sobre um número limitado de casos, mas ao mesmo tempo salientaram que uma quantidade considerável de condutas criminosas ora não eram detectadas, ora sequer eram divulgadas por suas vítimas, em virtude de temerem danos à sua imagem.

Vianna[42] descreve que propostas de tipificação de acesso não autorizado, um dos crimes cibernéticos, cujo bem lesionado seria a própria informação, remontam à década de 70 nos Estados Unidos, sendo adotada, em 1984, legislação visando combater esta criminalidade, cuja revisão deu origem em 1986 ao *Computer Fraud and Abuse Act*. O primeiro precedente referente à aplicação desta legislação foi em 1988, o caso: USA *versus* Robert Tappan Morris, no qual um estudante da Universidade de Cornell disponibilizou na Internet programa de computador que localizava as máquinas vulneráveis e as infectava com cópias de si mesmo (*worm)*[43]. O autor ainda relata[44] que o acontecimento gerou grande preocupação para a sociedade americana no tocante à segurança dos sistemas computacionais, uma vez que o programa provocou sobrecarga na rede.

Sobre o mesmo caso, Rustad[45] explica que originou o primeiro precedente na Corte da Apelação em que a Internet é mencionada. O estudante em questão cursava doutorado em ciência da computação, pesquisando justamente sobre segurança da informação, cujo projeto envolveu a criação do *worm*, testado com a sua liberação através de um dos computadores do laboratório de ciência do MIT, replicando-se rapidamente e desligando computadores de

---

[40] FERREIRA, Érica. *Internet: Macrocriminalidade e Jurisdição Internacional.* Curitiba: Juruá, 2008. 204 p. p. 100.
[41] ALBUQUERQUE, Op. Cit., p. 35.
[42] VIANNA, *Fundamentos*, p. 36.
[43] *Worm* é um vírus de computador que gera cópia de si mesmo.
[44] VIANNA, *Fundamentos*, p. 36.
[45] RUSTAD, Michael L. Private Enforcement of Cybercrime on the Electronic Frontier, *Southern California Interdisciplinary Law Journal*, v. 11:63, 2001, p. 63-116. p. 84. Disponível em: <http://www-bcf.usc.edu /~idjlaw /PDF/11-1/11-1%20Rustad.pdf >. Acesso: 21/03/2011

universidades e de instituições médicas e de defesa por todo Estados Unidos. Ainda que o criador do *worm* tenha atuado para prevenir maior propagação e que a criação e transmissão tenham sido realizadas para fins científicos, o acusado foi condenado a três anos de *probation*, 400 horas de serviço comunitário e uma multa de 10.500,00 dólares[46].

Ainda sobre os antecedentes desses delitos, Albuquerque[47] leciona que 1989 marca o nascimento dos crimes informáticos em redes abertas de computadores, prenúncio da criminalidade praticada na Internet, quando foram identificados *hackers* alemães que utilizavam redes de transmissão de dados internacionais para acessar dados sigilosos contidos em sistemas de informática localizados nos Estados Unidos e na Inglaterra, a fim de vendê-los ao serviço secreto russo.

Posteriormente, em 1993, com o início da exploração comercial da Internet[48], tem-se novo marco, o qual determina, essencialmente, a transnacionalização sem volta dessas infrações, visto que ela possibilita a interligação de computadores e usuário de todo o mundo. Silva[49] revela que, no Brasil, a ação de *hackers* em sistemas bancários e órgãos públicos foi primeiramente identificada em 1988 e Vianna[50] detalha que o marco histórico brasileiro dos crimes de Internet data de 18 de junho de 1999, quando diversas páginas oficiais do governo foram invadidas por *hackers*, sendo que o conteúdo inicial do site do Supremo Tribunal Federal foi substituído por texto de protesto contra o Presidente da República, o Fundo Monetário Internacional e o Plano Real. Para o autor, esse ano determina, portanto, o início da preocupação com os crimes cibernéticos no Brasil [51].

Ao falar do despertar dessa nova delinqüência, menciona-se todo contexto em que se enquadra e que envolve diversos fenômenos. Assim, pode-se citar a globalização, aqui compreendida como a "integração de natureza eminentemente sistêmica", conforme ensinamentos de Faria[52] que destaca o papel da tecnologia como um dos seus alicerces. Além disso, tem-se a revolução tecnológica que proporcionou o aparecimento das TICs, que Lima[53] descreve como a segunda revolução industrial, com a substituição do trabalho das mentes

---

[46] RUSTAD, Op. Cit., p. 96.
[47] ALBUQUERQUE, Op. Cit., p. 36.
[48] Sobre a criação, desenvolvimento e histórico da Internet ver: FINKELSTEIN, Maria Eugênia. Fraude Eletrônica. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.). *Direito & Internet: aspectos jurídicos relevantes*. Vol. II. São Paulo: Quartier Latin, 2008. 718 p. p. 403-440. p. 406-408; e SILVA, *Op. Cit*., p. 22-26.
[49] SILVA, Op. Cit., p. 80.
[50] VIANNA, Túlio Lima. Dos Crimes pela Internet. *In:* REINALDO FILHO, Demócrito (coord.). *Direito da Informática: temas polêmicos.* Bauru: EDIPRO, 2002. 432 p. p. 211-224. p. 213.
[51] VIANNA, *Dos Crimes*, p. 213.
[52] FARIA, José Eduardo C. O. *O direito na economia globalizada*. São Paulo: Malheiros, 1999. 359 p. p. 199.
[53] LIMA, Op. Cit., p. 2.

humanas pelo tratamento automatizado de informações pelas máquinas, e Smith[54] descreve como a terceira revolução industrial. Rossini[55] sintetiza com propriedade essa conjuntura:

> Com efeito, os dias atuais se caracterizam pela singularidade da transnacionalidade de acontecimentos ordinários, corriqueiros, como por exemplo a compra e venda, a troca de informações, as pesquisas, enfim, uma gama de atividades que permitem que pessoas, físicas ou jurídicas, mesmo separadas por milhares de quilômetros, ajam conforme seus interesses. Tal agilidade que acontece independentemente das distâncias é uma das características do que se denomina globalização, sendo inquestionável que a Internet é uma das principais, senão a principal ferramenta para seu estabelecimento.

Deve-se ainda falar sobre as lições de Beck[56] sobre a sociedade de risco, na medida em que esses delitos são fruto da evolução científico-tecnológica, tornando-se um ameaça que ultrapassa a esfera pessoal, em decorrência da globalidade do seu alcance[57], caracterizando-se como um risco global que não respeita qualquer diferença ou fronteira social e nacional[58].

Por fim, cabe referir ainda, a cultura da pós-modernidade, expressão de Jayme[59] que denota todo o processo de mudança e de crise vivenciado por nossa sociedade e pelo Direito na atualidade, salientando-se como características: o pluralismo, a comunicação, a narração e o retorno dos sentimentos. O autor descreve com propriedade o novo paradigma imposto às pessoas ao afirmar que "qualquer um pode facilmente se libertar das marras de sua existência limitada: velocidade, ubiqüidade, liberdade; o espaço, para a comunicação, não existe mais"[60].

Seguindo a mesma linha, ao tratar do tema dos negócios jurídicos de consumo no comércio eletrônico e a proteção dos consumidores, Marques[61] esclarece com maestria as características destas relações contratuais no âmbito virtual, que permitem classificá-las como pós-modernas, destacando-se a desmaterialização, a fluidez, a rapidez, a interatividade, a despersonalização, a internacionalização e a desterritorialização. Note-se que estas características não se limitam aos negócios jurídicos no comércio eletrônico, estando

---

[54] SMITH, Op. Cit., p. 242.
[55] ROSSINI, Op. Cit., p. 82.
[56] BECK, Ulrich. *Sociedade de Risco: rumo a uma outra modernidade.*Tradução de Sebstião Nascimento. São Paulo: Ed. 34, 2010. 383 p.
[57] BECK, Op. Cit., p. 26.
[58] Id., Op. Cit., p. 56.
[59] JAYME, Erik (vários textos). *Cadernos do Programa de Pós-Graduação em Direito da Universidade Federal do Rio Grande do Sul - PPGDir/UFRGS*, vol. 1, nº 1, março 2003. p. 27-28.
[60] JAYME, Op. Cit., p. 86.
[61] MARQUES, Cláudia Lima. *Confiança no Comércio Eletrônico e a Proteção do Consumidor: (um estudo dos negocios jurídicos no comercio eletrônico)*. São Paulo: Editora Revista dos Tribunais, 2004. 544 p. p. 60-61.

presentes, em menor ou maior grau, na mais ampla gama de relações que se estabelecem através das TICs.

Outro ponto de contato entre o direito penal e outros ramos do direito, no tocante aos novos paradigmas decorrentes da Sociedade da Informação e de seu elemento chave, a Internet[62], reside nos novos obstáculos impostos aos mecanismos tradicionais de proteção e garantia de direitos, como bem observa Marques[63] ao lecionar que a "distância física, a imaterialidade do meio eletrônico, a atemporalidade e a internacionalidade eventual da contratação, dificultam a eficácia do uso dos instrumentos tradicionais de proteção dos consumidores...". Mais uma vez, o apontamento da autora, na esfera do Direito do Consumidor, pode ser compreendido de forma mais ampla, visto que aquelas características traduzem as relações na sociedade contemporânea, aplicando-se perfeitamente à conjuntura vivenciada pelo Sistema Penal que precisa lidar com esta nova realidade.

É justamente no seio de todas essas manifestações que emergem os crimes cibernéticos, como típico produto de sua época e para os quais se exige uma resposta adequada do direito, inclusive, na esfera penal.

Rossini[64] faz uma interessante observação, recordando que, até meados da última fase histórica de desenvolvimento da Internet, correspondente à sua exploração comercial, passadas as fases de uso militar e acadêmico, acreditava-se na sua autoregulamentação, restando desnecessária a intervenção estatal sobre a Internet. No entanto, este panorama se modificou rapidamente com a tragédia de 11 de Setembro de 2001, com as constantes invasões de sistemas por *hackers* e *crackers* e com a propagação de pedofilia pela rede, demandando assim a atuação do Estado para garantir a tutela de bens jurídicos.

São características dessas infrações seu caráter transfronteiriço, transnacional; a inserção na macrocriminalidade e na criminalidade organizada; a especialidade do agente e tendência à sofisticação; a grande lesividade; a difícil rastreabilidade e comprovação e a cifra negra.

Em que pese a utilização de terminologia mais específica e própria do Direito Penal, verifica-se que revelam as características já apontadas por Marques[65], visto que a transnacionalidade reflete a internacionalização e a desterritorialização, assim como a difícil rastreabilidade e comprovação aponta para a despersonificação e imaterialidade do meio, dificultando e, por vezes, impedindo a persecução penal.

---

[62] MARQUES, Op. Cit., p. 37.
[63] Id., Op. Cit., p. 59.
[64] ROSSINI, Op. Cit., p. 31.
[65] MARQUES, Op. Cit., p. 60-61.

Analisando, especificamente cada uma das características, inicia-se com uma das notas mais particulares dos novos delitos que é a transnacionalidade, visto que a evolução das TICs, em especial da Internet, como alega Cruz[66], possibilita o cometimento de crimes, envolvendo a jurisdição de diversos países, fato que complica a prevenção e repressão dos mesmos, uma vez que exige determinação da lei aplicável, existência de criminalização das condutas nos países envolvidos e cooperação entre os mesmos no intuito de possibilitar a apuração dos fatos. Ressalta-se que muitos ordenamentos nacionais ainda não possuem solução para o problema (inovação e/ou adequação legislativa) e a comunidade internacional, em que pese os diversos e valiosos esforços, ainda não conseguiu alcançar um consenso a fim de promover uma harmonização.

Sofaer e Goodman[67] explicam que a fraqueza significativa no sistema atual está justamente na disparidade das legislações e práticas dos países, necessárias à investigação e persecução penal desses crimes, sustentando que a natureza transnacional dos crimes cibernéticos, demanda uma resposta transnacional[68]. Para os autores[69], um programa efetivo de combate à criminalidade transnacional cibernética requer cooperação legal entre os Estados e envolve a aplicação de padrões consensuais, existindo uma convergência ampla entre os Estados sobre as muitas formas de condutas que devem ser tipificadas dentro das fronteiras nacionais. O programa, portanto, deve ser traduzido num regime legal no qual os países proíbam condutas consideradas destrutivas ou impróprias.

Corroborando a dificuldade enfrentada pelos ordenamento nacionais, Smith[70] alerta que pela primeira vez é muito difícil esperar que leis promulgadas nacionalmente possam ter um forte efeito se existe uma variação fundamental entre as legislações nacionais. O autor ainda complementa que quando uma montanha de dados podem se mover de um lado do mundo para outro na velocidade da luz, começa a ficar muito mais difícil para os governos controlar e mudar a conduta das pessoas com leis nacionais que começam e terminam nas suas respectivas fronteiras[71].

---

[66] CRUZ, Op. Cit., p. 19.
[67] SOFAER, Abraham D.; GOODMAN, Seymour E. Cyber Crime and Security: the transnational dimension. In: *The Transnational Dimension of Cyber Crime and Terrorism.* Hoover Press, 2001. p. 15. Disponível em: <http://media.hoover.org/documents/ 0817999825_1.pdf>. Acesso em: 21/03/2011.
[68] SOFAER; GOODMAN, Op. Cit., p. 30.
[69] Id., Op. Cit., p. 2.
[70] SMITH, Op. Cit., p. 456.
[71] Id., Op. Cit., p. 456.

Gercke[72] reforça que os crimes cibernéticos são realmente um fenômeno mundial e que, devido à estrutura da rede, um criminoso pode atuar em qualquer lugar do mundo e atingir as vítimas em todo o mundo, embora o poder dos órgãos de persecução criminal seja limitado pelo Princípio da Soberania, restringindo a possibilidade de investigação em territórios estrangeiros e exigindo a cooperação de órgãos e agências de outros países com fulcro em arcabouços legais para cooperação internacional. Ademais, o autor esclarece os aspectos técnicos que implicam em transnacionalidade, elucidando que, muitas vezes, o processamento da transferência de dados afeta mais de um país, sendo resultado do desenho da rede, assim como do protocolo da Internet, que assegura transmissões com sucesso, ainda que linhas diretas estejam bloqueadas temporariamente e do fato de que grande número de serviços é oferecido por empresas situadas no exterior[73].

Também relacionando as questões técnicas, Rosenne[74] esclarece que a rede mundial de computadores coloca novos problemas que a tecnologia até então não desenvolveu métodos para controlar, sendo que as soberanias nacionais são incapazes de regular quais impulsos eletromagnéticos passam pelo seu território através do espectro eletromagnético. O autor[75], já em 2001, antecipou ação coordenada internacional nas esferas civil e militar que surgiria nos próximos anos para enfrentar o problema, notadamente no seio das Nações Unidas.

Ainda sobre transnacionalidade, Ginsburg[76] explica que a natureza transnacional da Internet confunde as leis tradicionais de jurisdição territorial e fronteiras nacionais, e Keyser[77] afirma que os crimes cibernéticos não estão confinados às fronteiras nacionais e um criminoso 'armado' com um computador e uma conexão tem a capacidade de vitimizar pessoas, empresas e até governos em qualquer parte do mundo. O autor exemplifica que o criminoso pode cometer crimes violentos, participar em atos de terrorismo internacional, vender drogas, roubar identidade, transmitir vírus, distribuir pornografia infantil, violar propriedade intelectual, vender segredos comerciais e acessar ilegalmente sistemas de computadores

---

[72] GERCKE, Marco. *An Introduction to Cybercrime*. UNAFEI 140th International Training Course, Resource Material Series n.° 79, 2008, 29 p. p. 5-6. Disponível em: <http://www.unafei.or.jp/english/pdf/RS_No79/No79_05VE_Gerke.pdf> Acesso em: 20/03/2011.
[73] GERCKE, Op. Cit., p. 9.
[74] ROSENNE, Shabtai. The perplexities of modern international law: general course on public international law. *Recueil des cours de l'Académie de droit international de La Haye*, vol. 291, 2001. p. 10-463. p. 350.
[75] ROSENNE, Op. Cit., p. 351.
[76] GINSBURG, Jane C. The Private International Law of Copyright in an Era of Technological Change. *Recueil des cours de l'Académie de droit international de La Haye*, vol. 273, 1998. p. 239-405. p. 383.
[77] KEYSER, Op. Cit., p. 325.

privados e de empresas, podendo esconder seus rastros através do entrelaçamento das suas comunicações via numerosos provedores de serviço da Internet[78].

Especificamente quanto ao combate destas infrações, Keyser[79] defende que esta nova criminalidade transnacional tem impedido os esforços dos órgãos de segurança pública de maneira nunca antes enfrentada, visto que apesar da Internet não possuir fronteiras, é preciso respeitar a soberania de outras nações, tornando assim a cooperação entre órgãos estrangeiros para o combate aos crimes cibernéticos um imperativo para qualquer esforço de captura desses criminosos. Dessa forma, Keyser[80] entende que, infelizmente, sistemas legais diferentes e disparidades na legislação representam os maiores obstáculos para o combate efetivo da criminalidade cibernética.

A fim de exemplificar as dificuldades enfrentadas pelos órgãos de segurança pública. O autor[81] introduz o seguinte exemplo: um *hacker* de Vancouver, no Canadá, interrompe uma rede coorporativa de comunicações em Seattle, nos Estados Unidos, mas antes de acessar a rede atacada ele faz o roteamento da sua comunicação através de provedores de serviço de Internet situados no Japão, Itália e Austrália. Neste caso, os órgãos de segurança do Canadá precisarão do auxílio das autoridades sediadas em Tóquio, Roma e Sydney, antes de descobrir que o criminoso está em seu próprio quintal.

Rustad[82] corrobora que crimes na Internet cruzam as fronteiras nacionais, criando a necessidade de cooperação internacional na aplicação da lei. Ainda sobre a Internet, Marques explica[83]:

> A maior tendência da Internet é para a globalização, justamente, porque, no meio eletrônico, desaparecem os limites (*borders*) estatais e territoriais. O mundo eletrônico (*cyber world*) teve como efeito a desterritorialização ou, para muitos, a desnacionalização dos negócios jurídicos. No *cyberspace*, a noção de soberania clássica (estatal-jurídica ou política), isto é, fazer leis, impor leis e julgar as condutas, rendendo efetivas as leis postas pelo Estado (*enforceability*) diminui sua força (ou mesmo desaparece, para alguns). É bastante difícil tonar efetiva a regulamentação estatal ou assegurar competência das jurisdições estatais na Internet.

Na mesma direção, E. L. L. Ferreira[84] ilustra a desnacionalização e desterritorialização da Internet.

---

[78] Id., Op. Cit., p. 325.
[79] Id., Op. Cit., p. 326.
[80] KEYSER, Op. Cit., p. 326.
[81] Id., Op. Cit., p. 326.
[82] RUSTAD, Op. Cit., p. 86.
[83] MARQUES, Op. Cit. p. 88-89.
[84] FERREIRA, Érica, *Internet*, p. 79.

> A Internet não tem proprietário, não tem nacionalidade e não está em território algum. Os crimes praticados através dela podem atingir mais de uma pessoa, em territórios diversos, com leis distintas, portanto, é conhecida como multijurisdicional (uma mensagem pode viajar por vários países) e ajurisdicional (localização física e geográfica são irrelevantes), de natureza, pois, multipolar [...].

A autora insere a criminalidade cibernética dentro da macrocriminalidade que "rompe os limites territoriais, criando uma rede de criminalidade mundial, sem respeito à soberania ou qualquer sistema de acordo internacional, realizado entre os Estados"[85]. Nesse sentido, explica E. L. L. Ferreira[86]:

> Podem-se citar como exemplos de crimes de macrocriminalidade, os delitos informáticos, econômicos, tributários, ambientais, criminalidade no comércio exterior, contrabando internacional de armas, drogas, órgãos, entre outros, todos permeados por características comuns, sendo que as principais são: geralmente a ausência de vítimas individualizadas; pouca visibilidade dos danos causados; bens jurídicos supra-individuais, universais ou vagos; novo e específico *modus operando*; ausência de violência física e muita organização.
> Em síntese: "*criminalidade organizada, criminalidade internacional e criminalidade dos poderosos são, provavelmente, as expressões que melhor definem traços gerais da delinqüência da globalização*"[87].

É justamente pela sua característica de não respeitar fronteiras que o enfrentamento desta criminalidade não se limita ao processo de tipificação das condutas, tornando a cooperação internacional imprescindível, como bem alerta Rosa[88].

Beck[89], ao tratar dos problemas ambientais na sociedade de risco, sustenta que "somente podem ser solucionados de forma objetiva e razoável em negociações transfronteiriças e acordos internacionais", alerta que também serve aos crimes cibernéticos os quais emergem como risco global.

Da mesma forma, Draetta[90] identifica que a cooperação internacional é a única resposta possível para esta criminalidade, salientando que os crimes tradicionais adquiriram nova dimensão com sua prática pela rede, sendo que essa cooperação, mesmo antes do advento da Internet, foi utilizada para coordenar a luta contra o crime organizado.

Ainda que os crimes cibernéticos possam ser praticados por qualquer pessoa, em face da universalização do acesso às TICs e também do conhecimento e do funcionamento das

---

[85] FERREIRA, Érica, *Internet*, p. 19.
[86] Id., *Internet*, p. 70.
[87] Grifo do autor.
[88] ROSA, Op. Cit., p. 76.
[89] BECK, Op. Cit., p. 58.
[90] DRAETTA, Ugo. Internet et commerce électronique en droit international des affaires. *Recueil des cours de l'Académie de droit international de La Haye*, vol. 314, 2005. p. 9-232. p. 186-187.

TICs, é exigida uma habilidade especial do sujeito ativo do crime, atributo explanado por Lima[91]. Sobre o tema, Pinheiro[92] destaca a disponibilidade na Internet de programas que viabilizam a invasão de computadores e a criação de vírus, descaracterizando a concepção inicial de um sujeito ativo de inteligência excepcional. Rosa[93] corrobora essa visão, esclarecendo:

> É um engano pensar que os "crimes de Informática" são cometidos apenas por especialistas, pois, com a evolução dos meios de comunicação, o aumento de equipamentos, o crescimento da tecnologia e, principalmente, da acessibilidade e dos sistemas disponíveis, qualquer pessoa pode ser um criminoso de Informática, o que requer apenas conhecimentos rudimentares para tanto; uma pessoa com o mínimo de conhecimento é potencialmente capaz de cometer crimes de Informática. É claro que, em regra, o delinqüente de Informática é um operador de computadores e de sistemas, mas, como dito, não se pode generalizar.

Cruz[94] reforça a existência de divergência doutrinária no aspecto referente à qualificação do agente, defendendo que muitos crimes cibernéticos podem ser cometidos sem que o agente necessite de conhecimentos especiais. Aqui reside um interessante paradoxo, pois, ao mesmo tempo em que se verifica uma popularização dos agentes desses crimes, Lima[95] narra a tendência de sofisticação e de sua ocorrência na esfera militar.

Ainda sobre a capacidade intelectual do sujeito ativo, Albuquerque[96] leciona:

> Os envolvidos com crimes informáticos costumam ser divididos em duas categorias. Os profissionais e os amadores. Crimes mais sérios do que a violação de segredo informático, envolvendo grandes prejuízos econômicos, são praticados por pessoas com experiência em invasão de sistemas. Muitos são empregados insatisfeitos que sabem muito bem como o sistema informático da empresa na qual trabalham funciona. Sua motivação é orientada pelo lucro, às vezes pela necessidade. Atentados contra a segurança de sistemas informáticos por empregados, geralmente, são atos de vingança. Às vezes, uma revolta contra a estrutura supostamente desumana e anti-social da empresa, um sentido de desafio, de competição. A segunda categoria, a dos amadores, compreende os jovens gênios em informática, aos quais já fizemos alusão, que aprenderam todos os truques da tecnologia da informação, incluindo como violar códigos de segurança.

Outro ponto bastante relevante sobre os delitos cibernéticos é a sua utilização pela criminalidade organizada, uma vez que as TICs são uma poderosa ferramenta para funcionamento e gerenciamento empresarial da corporação, também oferecendo novos nichos

---

[91] LIMA, Op. Cit., p. 32.
[92] PINHEIRO, Op. Cit., 261.
[93] ROSA, Op. Cit., p. 61.
[94] CRUZ, Op. Cit., p. 17.
[95] LIMA, Op. Cit., p. 34.
[96] ALBUQUERQUE, Op. Cit., p. 42-43.

de mercado para esses grupos. Pinheiro[97] cita exemplos da utilização das transações eletrônicas para a lavagem de dinheiro pela Máfia e do terrorismo cibernético. O terrorismo cibernético nada mais é que a transcendência das práticas terroristas para o ambiente cibernético, possibilitando que a TICs sejam utilizadas em uma ação ou sejam o alvo da mesma com motivação política e/ou ideológica, provocando violência contra pessoas ou causando interrupção e/ou prejuízo ao funcionamento de serviços essenciais para um determinado grupo de pessoas, instalando medo em determinada comunidade[98].

Outra marca registrada dos ilícitos informáticos é o seu grande potencial ofensivo[99], destacando-se que a Internet permite a interligação de milhões de pessoas, situadas em todo o mundo, viabilizando, assim, que uma ação lesione dezenas de milhões de pessoas, imediata e concomitantemente, algo nunca vivenciado antes pela comunidade internacional. Na mesma esteira, cria-se um novo paradigma para a tutela de bens como a honra, a propriedade intelectual, a privacidade etc. Por exemplo: não é possível comparar e tratar juridicamente da mesma maneira uma calúnia propagada oralmente e uma calúnia postada em um site de relacionamento na Internet, possibilitando a divulgação imediata e concomitante a milhões de pessoas, inclusive e especificamente, a toda rede de relacionamentos da vítima, causando um dano imensurável e irreparável. Além disso, ainda que a justiça conceda uma ordem decorrente de pedido imediato da vítima, com o objetivo de retirar o conteúdo calunioso da Internet, a probabilidade de sucesso é ínfima, pois o controle sobre todos os sites disponíveis na rede mundial é impossível em razão da quantidade de páginas existentes e da limitação jurisdicional. Justamente por isso, ouve-se com frequência a expressão que "*a Internet nunca esquece*".

No aspecto econômico, a grande lesividade dos crimes virtuais mostra realmente o seu potencial, fazendo os ganhos da atividade ilícita superarem largamente o risco, sendo desnecessária a presença física do agente infrator[100].

O Centro de Denúncias de Crimes de Internet dos Estados Unidos[101] expõe no Relatório Anual de 2009 que o prejuízo financeiro causado pelas fraudes denunciadas no país chegou ao patamar de 559,7 milhões de dólares no ano de 2009, com uma média de prejuízo

---

[97] PINHEIRO, Op. Cit., p. 258-259.

[98] Sobre Terrorismo Cibernético ver KERR, Kathryn. Putting cyberterrorism into context. *AusCERT Member Newsletter,* vol. 7, n. 2, jul. 2003. Disponível em: <http://www.auscert.org.au/render.html?it=3552>. Acesso em: 09/07/2009.

[99] Ainda que o grande potencial lesivo seja uma das grandes características desta criminalidade, não é obrigatório para a sua categorização como tal, existindo casos de pequeno potencial lesivo, sem grande dano ao bem juridicamente tutelado.

[100] LIMA, Op. Cit., p. 33.

[101] *Internet Crime Complaint Center – IC3*.

de 575 dólares por incidente comunicado, fato que representa mais que a duplicação das perdas comunicadas em 2008, as quais totalizaram 264,6 milhões de dólares[102]. Sobre o tema Keyser[103] apresenta a alarmante estimativa do *Federal Bureau of Investigation* (FBI) dos Estados Unidos, que o custo dos crimes eletrônicos ultrapassa o montante de 10 bilhões de dólares por ano.

A dificuldade de rastreabilidade do agente e de comprovação também são propriedades dessas infrações penais, em face de diversos fatores, dentre eles, a possibilidade de anonimato na rede, ainda que relativo, apontada por Pinheiro[104], que é facilitado pelo uso de elementos informáticos, segundo Cruz[105]; a utilização de um meio antes desconhecido, ensinada por Finkelstein[106]; a necessidade de qualificação técnica para a verificação de vestígios e a existência de registros transitórios destacadas por Lima[107] e a inexistência de legislação que obrigue os provedores de acesso à Internet a preservar os chamados "*logs*"[108] de acesso, que abrangem, em essência, dados relativos ao endereço de IP (*Internet Protocol*)[109] utilizado, às datas e aos horários de início e de término do acesso, levantada por Barros[110].

Rustad[111] comenta, em um artigo datado de 2001, que a pobreza dos casos de crimes cibernéticos refletia um lapso substancial entre o direito criminal cibernético dos livros e a aplicação da lei, salientando que poucos criminosos foram processados com sucesso, devido a vários fatores interrelacionados, incluindo o problema do anonimato, questões de jurisdição e

---

[102] INTERNET CRIME COMPLAINT CENTER – IC3. *2009 Internet Crime Report*. 25 p. p. 2. Disponível em: <http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf>. Acesso em: 10/03/2011. De acordo com o documento, o montante foi calculado com base no prejuízo econômico notificado ao IC3 pelas vítimas dos incidentes, conforme explicitado na página 6 do relatório.

[103] KEYSER, Op. Cit., p. 289.

[104] PINHEIRO, Op. Cit., p. 251-252, que afirma que "[...] IP constitui uma forma de identificação virtual. Isso significa que o anonimato na rede é relativo, assim como muitas Identidades Virtuais podem não ter um correspondente de Identidade Real".

[105] CRUZ, Op. Cit., p. 14.

[106] FINKELSTEIN, Maria Eugênia. Fraude Eletrônica. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.). *Direito & Internet: aspectos jurídicos relevantes*. Vol. II. São Paulo: Quartier Latin, 2008. 718 p. p. 403-440. p. p. 403.

[107] LIMA, Op. Cit., p. 34.

[108] Definido por PINHEIRO, Op. Cit., p. 365, como "registro de atividades gerado por programas de computador".

[109] Definido por PINHEIRO, Op. Cit., p. 358, como "é o endereçamento real de uma máquina na Internet. Consiste em uma série de números separados por pontos. Cada máquina conectada à rede tem um endereço IP. Os Domain Name Servers servem para relacionar os 'endereços com letras' com o endereço IP". A autora ainda define IP na mesma obra, p. 364, como "protocolo responsável pelo percurso de pacotes entre dois sistemas que utilizam a família de protocolos TCP/IP desenvolvida e utilizada na Internet".

[110] BARROS, Marco Antonio de. Tutela Punitiva Tecnológica. *In*: PAESANI, Liliana Minardi (Coord.). *O Direito na Sociedade da Informação*. São Paulo: Editora Atlas, 2007. 333 p. p. 275-300. p. 292.

[111] RUSTAD, Op. Cit., p. 85.

a falta de recursos dos órgãos de segurança pública, dificuldades estas que justamente caracterizam essas infrações penais, conforme visto anteriormente.

Ainda cabe menção ao problema da cifra negra[112] em relação aos crimes cibernéticos, chamada de 'zona escura' por Cruz[113], que explica a pequena quantidade de notificações. Ao estudar o sujeito do passivo desses crimes; Lima[114] indica que as grandes empresas não comunicam as ocorrências à polícia, para evitar publicidade negativa quanto aos seus sistemas de segurança. No mesmo sentido, Rosa[115] relata que, a exemplo do que ocorre nos Estados Unidos, as grandes empresas seguradoras no Brasil não divulgam os incidentes de segurança, para não abalar a credibilidade das empresas vítimas.

A importância do combate a esta criminalidade, objeto de destaque das agendas diplomáticas de diversas organizações regionais e internacionais, a serem analisadas no segunda parte deste trabalho, reside justamente em suas características, especialmente em seu grande poder lesivo, no fato de prejudicar a confiança na utilização das TICs, bem como a funcionalidade dos sistemas de informação, fazendo com que seu uso possa ser restringido face aos riscos associados, por exemplo, tornando inviável o comércio eletrônico, a utilização de *home bankings* etc. Ou seja, a ineficácia no combate desses ilícitos pode impedir o gozo das facilidades advindas do uso das TICs na vida cotidiana. Neste aspecto, Gercke[116] aponta que a habilidade de lutar efetivamente contra os crimes cibernéticos é uma exigência essencial para apoiar o início e a continuidade do processo de transformação dos países em sociedades da informação, caracterizadas pelo emergente uso das TICs para acessar e compartilhar informação, sendo a existência de um quadro jurídico suficiente, um requisito essencial para o comércio eletrônico.

A doutrina apresenta diversas classificações dos crimes cibernéticos, enquadrando-os, geralmente, tanto ao bem jurídico protegido, à finalidade visada, ao sujeito ativo quanto ao elemento do computador utilizado[117]. Acredita-se que a classificação mais relevante é a que divide, os crimes cibernéticos em dois grandes grupos, basicamente, comparando, justamente os crimes cometidos contras as TICs dos que são cometidos por meio das TICs, revisitando-se o conceito apresentado de crimes cibernéticos. Desta maneira, considera-se crime puro

[112] Sobre cifra negra e delito informático ver também SILVA JÚNIOR, Op. Cit., p. 322-323.
[113] CRUZ, Op. Cit., p. 14.
[114] LIMA, Op. Cit., p. 66.
[115] ROSA, Op. Cit., p. 47.
[116] GERCKE, Op Cit., p. 3-4.
[117] Nesse sentido ver FERREIRA, Ivette. Op. Cit., p. 243-245; e LIMA, Op. Cit., p. 36-51.

(próprio)[118] aquele cujo alvo são as TICs, ou seja, que lesiona o bem jurídico da segurança informática. Já os crimes impuros (impróprios) são todas aquelas condutas já criminalizadas que podem utilizar as TICs para sua execução, atingindo, assim, os mais variados bens jurídicos, tais como honra, patrimônio, privacidade, propriedade intelectual etc.

Silva[119] divide a categoria delitiva em crimes puros, impuros ou comuns. Os puros seriam aqueles que atacam justamente as TICs, enquanto que os impuros são crimes que atacam outros bens jurídicos, mas só podem ser praticados com o auxílio das TICs. Já os comuns também atingem bens jurídicos diversos da segurança informática, sendo executados com o uso das TICs, ainda que pudessem ter sido executados com outras ferramentas, ou seja, com outro *modus operandi*. Como se pode observar, essa classificação subdivide os crimes que são considerados impuros (impróprios) da primeira, diferenciando os em razão da exclusividade do meio, ou seja, se podem ser executados de outras formas além do uso das TICs.

Vianna[120] propõe classificar esses delitos em próprios, impróprios e mistos. Os primeiros ofenderiam ao bem jurídico da inviolabilidade da informatização automatizada (dados), os segundos, o bem jurídico diverso e os últimos seriam delitos complexos em que além do bem jurídico da inviolabilidade de dados, a norma também tutelaria outro bem jurídico diverso. Além disso, o autor ainda destaca que os delitos próprios podem ser executados como crime-meio para prática de um crime-fim que não seria informático, casos em que seriam denominados de delitos mediatos ou indiretos.

Rossini[121] opta por uma classificação binária, agrupando-os em delitos informáticos puros e delitos informáticos mistos. Os primeiros seriam aqueles em que a conduta do sujeito visa ao sistema de informática, como por exemplo, acesso não autorizado e a conduta de *hackers* e *crackers*. Já nos mistos, o computador é mera ferramenta em atos visando lesão a outros bens jurídicos, não exclusivos ao sistema informático. Gouvêa[122] apresenta classificação semelhante, dividindo os crimes em duas categorias: as dirigidas contra sistemas de informática (inserção, alteração, supressão, furto de informações etc) e as que utilizam os sistemas como ferramentas na execução de crimes já tipificados (homicídio, sedução, tráfico de entorpecentes etc).

---

[118] Classificação de JESUS e SMANIO apud LIMA, Op. Cit., p. 41-42. Já E. L. L. FERREIRA restringe essa classificação à terminologia de crimes próprios/impróprios, utilizando o vocábulo puro para outra classificação, que pode ser consultada em FERREIRA, Érica, *Internet*, p. 103.
[119] SILVA, Op. Cit., p. 60.
[120] VIANNA, *Fundamentos*, p. 13-14.
[121] ROSSINI, Op. Cit., p. 122-123.
[122] GOUVÊA, Op. Cit., p. 67-68.

Albuquerque[123] prefere classificar os delitos, em questão, entre comuns e específicos. Estes seriam condutas ainda não tuteladas pelo direito penal enquanto que aqueles utilizariam a informática para praticar condutas já tipificadas. Embora o autor defenda ser uma classificação análoga[124], a classificação foge um pouco das idéias anteriores, visto que a tipificação dos crimes cibernéticos classificados entre próprios ou puros, pelos outros autores, importaria na classificação como crime comum para o referido autor, independentemente do tipo de bem jurídico tutelado pelo Direito Penal, visto que a classificação de Albuquerque[125] centra-se no fato da conduta já estar tipificada ou não, opção que não parece ser a mais adequada.

Para Rustad[126], os crimes de computador podem ser classificados quanto ao tipo de dano, quanto à localização geográfica, quanto ao alvo e quanto ao criminoso. O autor relata que os danos causados por uma intrusão podem consistir em perda financeira, invasão à privacidade, furto de informações, destruição de segredos comerciais, danificação de discos rígidos e até, ameaças à saúde ou à segurança pública. As invasões podem originar-se nos Estados Unidos e em paraísos no exterior, atingindo instituições públicas e privadas, sendo que os ataques privados incluem ataques a sites corporativos ou redes de computadores[127]. Já os criminosos podem ser adolescentes entediados, funcionários descontentes, espiões corporativos ou redes de crime organizado[128].

Pode-se citar ainda a visão de Rosa[129], que separa o crime praticado com a utilização ou contra computadores, o crime comum (exemplo: estelionato) do crime de informática propriamente dito. Para o autor[130], a execução de crimes 'velhos' com o uso da Internet, já tipificados no Código Penal, não os caracteriza como 'crimes de informática'. Reza o autor[131]:

> O certo é que existem crimes comuns, ou seja, aquelas condutas previstas pela legislação penal; crimes comuns, porém, cometidos com o auxílio do computador, podendo-se, então, denominar crimes comuns praticados pelo uso ou contra o computador, mas que encontram aplicação na nossa legislação penal; e, por fim, certos comportamentos, certas condutas que ainda não estão tipificadas em nossa legislação penal, que necessitam do uso do computador para atingir sua finalidade, fazendo dele *conditio sine qua*

[123] ALBUQUERQUE, Op. Cit., p. 40-41.
[124] Id., Op. Cit., p. 40.
[125] ALBUQUERQUE, Op. Cit., p. 40.
[126] RUSTAD, Op. Cit., p. 65.
[127] Id., Op. Cit., p. 96.
[128] Id., Op. Cit., p. 96.
[129] ROSA, Op. Cit., p. 53.
[130] Id., Op. Cit., p. 73.
[131] Id., Op. Cit., p. 47.

> *non* para a empreitada: é aqui que podemos falar em "crimes de Informática" propriamente ditos.

Das classificações relatadas anteriormente, à semelhança do ocorrido quando considerado o conceito desses crimes e o seu bem jurídico, percebe-se uma convergência entre alguns autores, independentemente da nomenclatura utilizada, no esforço de diferenciar essencialmente duas espécies distintas de delitos, ou seja, aqueles em que as TICs são utilizadas como ferramentas para lesionar os mais variados bens jurídicos (honra, patrimônio etc) daqueles em que o alvo é justamente suas tecnologias. Estes seriam os delitos cibernéticos próprios ou puros, enquanto que aqueles, impróprios ou impuros[132].

Uma das interessantes questões é o estudo dos sujeitos, especialmente do ativo dessa criminalidade. Relativamente ao sujeito passivo desses delitos, ou seja, a vítima são as pessoas, físicas ou jurídicas, que são atingidas pela conduta (ação ou omissão) criminosa. À princípio, não se vislumbra qualquer dificuldade na sua identificação uma vez que se trata de indivíduos, empresas, entidades públicas, dentre tantos outros, cujos bens e/ou interesses são lesionados.

Lima[133] cita estudo da *Symantec* que aponta que 67% das empresas brasileiras já foi alvo de ataque nas suas redes, sendo que para 38% não foi a primeira vez que sofreram este tipo de investida. Na mesma esteira, Teixeira[134] menciona pesquisa da empresa *Attrition* que revela que as empresas comerciais nos Estados Unidos concentraram 45% dos ataques.

Como agentes da ação delituosa, encontra-se na doutrina uma ampla gama de descrições dos sujeitos ativos, tais como *hackers*, *white hats*, *black hats*, *insider hackers, outsider hackers*, *crackers*, *cyberpunks*, *phreakers*, *sniffers*, *carders*, *cyberterrorists*, *war drivers*, *lammers* e *spammers*[135].

Hackers são normalmente descritos como especialistas que acessam sistemas informáticos com a quebra de mecanismos de segurança. Silva[136] ensina que o termo surgiu no *MIT* para designar estudantes de computador, sendo "fuçador" a sua melhor tradução. Ainda que haja grande divergência sobre a sua atuação e especialidade, é possível identificar certo consenso no sentindo de que o seu objetivo é a invasão de computadores *per se*, sem

---

[132] Terminologia que a partir deste momento são utilizadas como sinônimo no presente trabalho.
[133] LIMA, Op. Cit., p. 67.
[134] TEIXEIRA, Tarcisio. *Direito Eletrônico***.** São Paulo: Juarez de Oliveira, 2007. 211 p. p. 49.
[135] Sobre o assunto, ver LIMA, Op. Cit., p. 69-78; SILVA, Op. Cit., p.77-82; BARROS, Op. Cit., p. 283; PINHEIRO, Op. Cit., p. 256-257; e ZANIOLO, Pedro Augusto. *Crimes modernos: o impacto da tecnologia no direito.* Curitiba: Juruá, 2007. 487 p. p. 366-367.
[136] SILVA, Op. Cit., p. 77-78.

visar à prática de outra conduta criminosa[137]. Na mesma linha, Lima[138] ensina que os *hackers* "estariam desafiando seus próprios conhecimentos técnicos e a segurança de sistemas informatizados de grandes companhias e organizações governamentais".

É possível, inclusive, perceber uma conotação positiva da expressão, conforme se extrai do fragmento abaixo da obra de Silva[139]:

> Hacker ético refere-se àquele sujeito que usa seus conhecimentos na busca de soluções de situações criadas pelos crackers. São capazes de entrar e sair de um computador sem que se perceba; mostrando-se como verdadeiros especialistas, "invadem sistemas, corrigem falhas de segurança e instalam uma porta única e controlada, com o propósito de garantir a exclusividade no acesso".

Pinheiro[140] divide os *hackers* em dois grandes grupos, classificando-os em *white* and *black hats*. Os *White Hats* seriam justamente os *hackers* éticos, pois visam invadir o sistema e após, comunicam ao dono as deficiências de segurança. Já os *Black Hats* seriam os *hackers* profissionais, ligados à espionagem industrial e governamental.

Ainda sobre os *hackers*, E. L. L. Ferreira[141] mostra a existência de outra categorização, distribuindo-os em *insiders* e *outsiders*, de acordo com a existência ou não de acesso legítimo. Sobre o assunto, Daoun e Blum[142] destacam que *insider* é o "*hacker* interno de uma empresa, é o próprio empregado que atua, geralmente movido por sentimento de vingança contra o empregador ou contra algum outro membro da empresa".

Especificamente sobre a metodologia usada pelos *hackers*, Vianna[143] explica que a atividade deles é sempre com o intuito de ganhar ou ampliar permissões de acesso a computadores interconectados. Para tanto, tentam descobrir a senha do usuário, tentam criar novo *login* e senha para determinado usuário ou, ainda, conseguem acesso após criar pane no sistema, permitindo acesso não autorizado. O autor [144] destaca ainda que os *hackers* tiram vantagem da postura do usuário, que representa a maior deficiência na estrutura de qualquer rede, elencando os seguintes métodos de atuação: dedução, engenharia social, tentativa e erro, utilização de "cavalos de tróia" e invasão de servidor.

---

[137] BARROS, Op. Cit., p. 283.
[138] LIMA, Op. Cit., p. 72.
[139] SILVA, Op. Cit., p. 78.
[140] PINHEIRO, Op. Cit., p. 256-257.
[141] FERREIRA, Érica, *Internet*, p. 107.
[142] DAOUN, Alexandre Jean; BLUM, Renato M. S. Ópice. Cybercrimes. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.). *Direito & Internet: aspectos jurídicos relevantes*. 2 ed. São Paulo: Quartier Latin, 2005. 543 p. p. 141-152. p. 147.
[143] VIANNA, *Dos Crimes*, p. 215.
[144] Id., *Dos Crimes*, p. 216-217.

Já os *crackers* são considerados '*hackers* do mal'[145], 'piratas da Internet'[146], pois além de acessar sistemas sem autorização, dolosamente adulteram, destroem, furtam e/ou apagam dados, sendo "os autores das grandes fraudes eletrônicas, causando expressivos prejuízos a vários usuários, instituições e, enfim, a toda a coletividade", segundo ensinamento de Lima[147].

Para E. L. L. Ferreira[148] *cyberpunks* são *crackers* que tem por finalidade destruir dados, programas e/ou sistemas. A autora também elucida que para os casos em que o alvo fraude são os sistemas de telecomunicações, especificamente, existe a denominação de *phreakers*[149]. Lima[150] acrescenta que a fraude recai usualmente sobre as linhas de telefonia fixa comutada e móvel, com o objetivo de utilizá-las sem arcar com os custos.

Os *Sniffers* buscam informações específicas por meio de programas rastreadores, acessando os discos rígidos de computadores conectados à rede mundial[151], configurando uma forma de invasão à privacidade dos usuários da Internet. *Carders* são descritos por Zaniolo[152] como especialistas "em fraudes envolvendo cartões de crédito".

Cyberterrorits são criadores de vírus perigosos com o objetivo de "sabotar redes de computadores e provocar a chamada *'DdoS - Denial of Service'* (a queda dos sistemas de grandes provedores) impossibilitando o acesso de usuários e causando enormes prejuízos", consoante explanação de Lima[153]. Recorda-se aqui as noções que fundamentam o conceito de terrorismo cibernético, já citadas anteriormente, possibilitando a definição destes terroristas como agentes que se utilizam das TICs ou buscam justamente atingí-las, com base em motivação política e/ou ideológica, causando violência contra pessoas ou interrupção e/ou prejuízo ao funcionamento de serviços essenciais para um determinado grupo de pessoas, instalando medo em determinada comunidade. A referência a uma ação política ou ideologicamente motivada, bem como ao sentimento de medo que gera na população, é importante para delimitar o enquadramento das práticas, sob pena de grande parte de ilícitos cometidos através do ambiente virtual passe a ser classificada como terrorismo.

---

[145] ZANIOLO, Op. Cit., p. 367.
[146] BARROS, Op. Cit., p. 283.
[147] LIMA, Op. Cit., p. 76.
[148] FERREIRA, Érica, *Internet*, p. 105.
[149] FERREIRA, Érica, *Internet*, p. 105.
[150] LIMA, Op. Cit., p. 77.
[151] FERREIRA, Érica, *Internet*, p. 105.
[152] ZANIOLO, Op. Cit., p. 367.
[153] LIMA, Op. Cit., p. 78.

Zaniolo[154] enquadra os *War Drivers* dentro da categoria de *crackers* que se utilizam das vulnerabilidades das redes sem fio.

Rossini[155] explica que *lammers* são indivíduos que não detêm conhecimentos suficientes, apesar de se identificarem como *crackers*, sendo que seu nome deriva da junção do termo inglês *lame* com a palavra *hacker*. Para finalizar, cabe mencionar os *spammers*, identificados por E. L. L. Ferreira[156] como aqueles que enviam milhares ou milhões de mensagens não solicitadas por correio eletrônico.

Percebe-se que os sujeitos ativos podem ser encaixados em dois grandes grupos: os *hackers* e os *crackers*, sendo que estes últimos recebem denominações diferentes de acordo com a técnica ou meio técnico utilizados (por exemplo, os *war drivers*) ou o fim visado (os *carders*).

Quanto aos meios utilizados para o ataque, são encontradas na literatura especializada as seguintes referências[157]: vírus, *worms, DoS, DDoS, trojan horses, spoofing, phishing, salami slicing, trap doors, logic bombs, scans, cybersquatting, DNS hijacking, hoaxes, spam, wiretapping, malware, superzapping, data didling, traching, cookies* etc[158].

Pinheiro[159] conceitua vírus informático como "programa ou parte de um programa de computador, normalmente malicioso, que se propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador". A autora ainda alerta que "depende da execução do programa ou arquivo hospedeiro para que possa tonar-se ativo e dar continuidade ao processo de infecção"[160].

Lima explica que *worms* são vírus que se disseminam com a geração de cópias funcionais de si mesmos, cuja difusão ocorre por conexão de rede ou anexos de mensagens de correio eletrônico[161]. Zaniolo[162] apresenta uma classificação para vírus, dividindo-os em inócuos: não geram perturbação ao sistema; humorísticos: não causam danos, limitando-se a mostrar mensagem ou imagem humorística; alteradores que provocam, como já indica o nome, modificação de dados em arquivos, sendo potencialmente danosos, pois nem sempre a

---

[154] ZANIOLO, Op. Cit., p. 367.
[155] ROSSINI, Op. Cit., p. 151.
[156] FERREIRA, Érica, *Internet*, p. 106.
[157] Enumeração meramente exemplificative, visto que todos os dias nascem novas técnicas em decorrência de evolução tecnológica e do increment das práticas e políticas de segurança que instigam a criação de novos métodos.
[158] Sobre o tema ver FERREIRA, Érica, *Internet*, p. 112-115; SILVA, Op. Cit., p. 72-75; ZANIOLO, Op. Cit.; LIMA, Op. Cit., p. 49-64; PINHEIRO, Op. Cit., FINKELSTEIN, Op. Cit., p. 417.
[159] PINHEIRO, Op. Cit., p. 376-377.
[160] Id., Op. Cit., p. 377.
[161] LIMA, Op. Cit., p. 51.
[162] ZANIOLO, Op. Cit., p. 261-262.

alteração é percebida; catastróficos, virus repentinos com prejuízos globais e imediatos, podendo apagar, destruir, inutilizar arquivos e/ou dispositivos, e os genéricos, sendo os mais contagiosos, restando invisíveis até sua execução, com a alteração ou destruição de arquivos.

DoS (Denial of Service) é um tipo de ataque que faz com que um computador ou um servidor da rede mundial não responda, pare de funcionar, por causa de uma sobrecarga de processos requisitados, conforme Pinheiro[163]. Já o *DDoS* (*Distributed Denial of Service*) representa uma evolução do ataque anterior, visto ser uma forma distribuída e coordenada da investida, pois ocorre a utilização de computadores vulneráveis de terceiros para gerar a sobrecarga que impedirá a resposta a outros pedidos, como destacado por Concerino[164].

Pinheiro[165] define *trojan horses*, os cavalos de tróia, como programas que, em geral, executam funções maliciosas e sem conhecimento do usuário, sendo recebidos através de cartões virtuais, jogos, protetores de tela etc. A autora também explica que a terminologia "código malicioso" é genérica, servindo para designar todos os tipos de programas (vírus, *worms*, *bots*, cavalos de tróia e *rootkits*) que executam rotinas maliciosas[166].

Doneda[167] salienta que *Spoofing* é uma técnica que mascara o verdadeiro remetente da comunicação a fim de que seja aceita. É uma das ferramentas utilizadas por *spammers*.

Phishing é descrito por Pinheiro[168] como,

> mensagem não solicitada que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou site popular, e que procura induzir usuários ao fornecimento de dados pessoais e financeiros. Inicialmente, esse tipo de mensagem induzia o usuário ao acesso a páginas fraudulentas na Internet. Atualmente, o termo também se refere à mensagem que induz o usuário à instalação de códigos maliciosos, além da mensagem que, no próprio conteúdo, apresenta formulários para o preenchimento e envio de dados pessoais e financeiros.

Salami Slicing, na explanação de Ferreira[169], configura uma alteração leve em um programa "para recortar dados insignificantes de contas correntes, saldos" etc, *v. g.*, a transferência eletrônica de um centavo de real de milhões de contas bancárias. Para a autora,

---

[163] PINHEIRO, Op. Cit., p. 356-357.
[164] CONCERINO, Arthur José. Internet e Segurança são Compatíveis? *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.). *Direito & Internet: aspectos jurídicos relevantes*. 2 ed. São Paulo: Quartier Latin, 2005. 543 p. p. 153-178. p. 163.
[165] PINHEIRO, Op. Cit., p. 351-352.
[166] Id., Op. Cit., p. 352-353.
[167] DONEDA, Danilo. Perspectivas para Combate ao Spam. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.). *Direito & Internet: aspectos jurídicos relevantes*. Vol. II. São Paulo: Quartier Latin, 2008. 718 p. p. 255-276. p. 263.
[168] PINHEIRO, Op. Cit., p. 368.
[169] FERREIRA, Érica, *Internet*, p. 114.

trap doors funda-se na "validação de 'portas' de acesso camufladas para a introdução de programas, com fim ilícito de aproveitamento" [170].

Bombas lógicas (*logic bombs*) designam, de acordo com Lima[171], um programa que começa sua rotina destrutiva após determinado intervalo de tempo ou hora previamente fixadas ou, ainda, após a ocorrência de determinado sinal.

Finkelstein[172] caracteriza *scans* como varreduras que captam senhas fracas para ataques, ressaltando que são responsáveis pela maioria das fraudes bancárias, sendo que os dados dos usuários são obtidos através de *keyllogers* (captura das teclas digitadas), *screenloggers* (captura das posições do mouse) ou telas sobrepostas[173].

Cybersquatting é o registro de domínios da Internet, utilizando marcas famosas ou nomes fantasia de empresas para posteriormente revendê-las por um preço exorbitante para os seus detentores, consistindo em prática ilegal e extorsiva para Pinheiro[174;175]. A autora também indica uma variante desta prática, que seria esse registro com erros de digitação, chamado de *typosquatting*[176].

DNS hijacking (sequestro de DNS)[177] é uma técnica que causa um desvio no endereçamento, fazendo o domínio digitado remeter à página diversa da registrada. Para exemplificar, cita-se a hipótese de um correntista que ao digitar corretamente o domínio do seu banco no seu navegador de Internet, é remetido para outra página. Neste caso, pode-se imaginar dois cenários. No primeiro, o usuário não tem interesse na página para onde foi remetido e não existem maiores transtornos, além daqueles decorrentes da não utilização do serviço desejado. Obviamente, pode ser extremamente prejudicial de acordo com a duração do incidente, com o tipo de serviço atingido e com a abrangência de pessoas prejudicadas. No entanto, ainda é possível imaginar um panorama de maior gravidade, o segundo cenário, no qual o usuário é remetido para uma página idêntica, porém falsa do seu banco e, dessa forma, todas as suas informações são captadas e imediatamente utilizadas para transferir todo o montante depositado em sua conta bancária.

---

[170] Id., Op. Cit., p. 114.
[171] LIMA, Op. Cit., p. 50.
[172] FINKELSTEIN, Op. Cit., p. 417.
[173] *Keyllogers* e screenloggers são técnicas já obsoletas em face dos avanços na área de segurança, especialmente no âmbito de serviços bancários.
[174] PINHEIRO, Op. Cit., p. 101.
[175] Sobre cybersquatting ver SMITH, Op. Cit., p. 291-296.
[176] Id., Op. Cit., p. 101.
[177] *DNS* é o acrônimo de *Domain Name Server*, que na Internet representa o sistema por meio do qual o nome de domínio digitado é vinculado a um endereço de IP, ou seja, a um determinado computador, fazendo com que se encontre a página procurada.

Hoaxes (boatos) são mensagens de correio eletrônico, cujo conteúdo é alarmante ou falso e, geralmente, atribuído a instituições com credibilidade (por exemplo: órgãos públicos ou grandes empresas), como salienta Zaniolo[178], podendo ser agrupados[179] em avisos de códigos maliciosos, ofertas de produtos gratuitos, correntes, lendas urbanas, ações de solidariedade, avisos inconsequentes, sátiras e outros.

No tocante ao *Spam*[180], Doneda[181] expõe os problemas de uma conceituação abstrata fechada, assentando quatro elementos básicos que caracterizam o *spam*, a saber: o caráter comercial, o envio em massa, a uniformidade de conteúdo e a ausência de solicitação por parte do destinatário. Assim, pode-se inferir com base nesses atributos que são mensagens não solicitadas enviadas a um grande número de pessoas, com o mesmo conteúdo e visando uma finalidade comercial, ainda que indireta. O próprio autor alerta que pode haver hipóteses em que nem todos os elementos estarão presentes, devendo-se avaliar no caso concreto se o *spam* decorre de algum interesse do remetente ou se pode causar dano, ainda que potencial[182].

Ainda sobre o *spam*, cabe ressaltar que o recente Anteprojeto de atualização do Código de Defesa do Consumidor[183], no proposto art. 45-E, contempla a vedação ao envio de mensagem eletrônica não solicitada, ainda que não a considere uma prática criminosa.

E. L. L. Ferrera[184] qualifica *wiretapping* como interceptação de dados e *malware* é, para Zaniolo[185], a combinação de dois ou mais tipos de vírus como *trojans* e *worms*.

Silva[186] esclarece que *superzapping* é a paralisação da memória do processador central, que impede o seu uso regular e viabiliza o acesso aos dados, penetrando no seu conteúdo. A autora ainda aclara que *data diddling* consiste na modificação de comandos para possibilitar a entrada em bancos de dados, seus registros e códigos e que *traching* é a busca nas lixeiras dos computadores de informações que permitam o acesso ao código de ingresso nos programas[187].

---

[178] ZANIOLO, Op. Cit., p. 130-134.
[179] Segundo classificação do sítio *HoaxBusters apud* ZANIOLO, *Op. Cit*., p. 130.
[180] Recorda-se aqui a citação inicial sobre a divergência sobre a caracterização do spam como prática criminosa. Vide nota de rodapé n.° 1.
[181] DONEDA, Op. Cit., p. 259-260.
[182] DONEDA, Op. Cit., *p.* 260.
[183] Texto do anteprojeto disponível na íntegra em: <http://www12.senado.gov.br/noticias/materias/2012/03/14/veja-a-integra-do-anteprojeto-que-atualiza-o-codigo-do-consumidor >. Acesso em: 26/03/2012.
[184] FERREIRA, Érica, *Internet,* p. 114.
[185] ZANIOLO, Op. Cit., 261.
[186] SILVA, Op. Cit., p. 73.
[187] Id., Op. Cit., p. 73.

Cookies[188] são "absorventes de textos com informações sobre o comportamento dos usuários na rede. Permitem que servidores gravem informações de seu interesse em outro microcomputador remoto", consoante lição de Pinheiro[189].

Pelas técnicas acima expostas, observa-se a existência de muitos recursos para a execução dos delitos, os quais, muitas vezes, consistem na aglutinação de mais de uma ferramenta, existindo uma extensa nomenclatura. A descrição efetuada pretendeu relatar algumas das mais relevantes e ocorrentes práticas, a fim de que se tenha alguma noção sobre como os crimes cibernéticos são cometidos. Não houve pretensão de relacionar exaustivamente todas as técnicas existentes, até mesmo pela impossibilidade prática, na medida em que todos os dias novos instrumentos são criados e descobertos.

Após o breve estudo que perpassa a caracterização dos crimes cibernéticos, abordando a terminologia empregada, o conceito, o contexto de seu surgimento, os bens jurídicos tutelados, os seus elementos e sua classificação, bem como a descrição dos sujeitos ativo e passivo e de suas técnicas, passa-se à análise de como esta criminalidade é enfrentada pelo Sistema Jurídico Brasileiro.

B: CRIMES CIBERNÉTICOS NO BRASIL

Ao falar-se de crimes em sentido amplo, deve-se ter presente que o combate dessas infrações obedece a uma cadeia específica de regras e princípios de estrita observância, cuja pedra de toque é o Princípio da Legalidade, uma vez que o Direito Penal é a *ultima ratio*, pois sua incidência pode implicar em restrição de um dos mais elementares direitos fundamentais, qual seja a liberdade. Aqui reside, justamente, a importância de se estudar o fenômeno denominado de criminalidade cibernética, a fim de verificar se essas condutas podem ser alvo da repressão pelo Direito Penal Brasileiro.

Nesse sentido, Silva[190] alerta:

> Três são os pontos de destaque: a necessidade de cuidado no tentar adaptar as leis existentes aos delitos que tenham sido praticados por intermédio do computador; a existência de casos, cujo uso do computador poderia ser circunstância a provocar aumento de pena; e outros casos que se vislumbrariam situações novas, nascendo a necessidade de se criar tipo novo.

---

[188] *Cookies* são uma técnica que não é necessariamente usada para o cometimento de delitos, sendo utilizada corriqueira e licitamente na utilizaç
[189] PINHEIRO, Op. Cit., p. 354.
[190] SILVA, Op. Cit., p. 51.

Primeiramente, deve-se ter presente que os crimes cibernéticos impuros, compreendidos pela utilização das TICs como instrumento para a prática de condutas típicas que lesionam os mais variados bens jurídicos, são objeto de repressão pelo nosso Sistema Criminal, incidindo no dispositivo penal que tutela o bem determinado. Dessa maneira, não se faz necessária a tipificação de novas condutas, pois constituem velhos crimes que se utilizam de um novo meio, cabendo o questionamento sobre a necessidade de adequação da pena em abstrato, em face da lesividade destes crimes. O Supremo Tribunal Federal (STF) já teve a oportunidade de se manifestar sobre essa criminalidade, restando assentado no HC 76689-PB, julgado em 20 de setembro de 1998, de Relatoria do Ministro Sepúlveda Pertence, que novo *modus operandi* não infringe o Princípio da Legalidade e não exclui a tipicidade, permitindo assim, a punição do agente. Transcreve-se aqui a ementa do julgado:

> 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.[191]

Além da jurisprudência favorável à aplicação dos tipos penais tradicionais aos crimes que se utilizam das TICs para sua execução, na doutrina também é possível encontrar essa orientação. Finkelstein[192] defende:

> [...] a *internet* é meramente uma nova forma de consecução de condutas criminosas já tipificadas. Em outras palavras, a conduta dos criminosos eletrônicos já está definida em nossa legislação penal. A *internet* é apenas uma ferramenta para o cometimento do crime. A conduta dos infratores pode, assim, ser encaixada em tipos penais já regulamentados há vários anos, tais como estelionato, dano ou fraude.

[191] Grifo nosso.
[192] FINKELSTEIN, Op. Cit., p. 428.

Cabe mencionar que existe divergência doutrinária sobre a possibilidade de caracterizar dados e informação como coisa, objeto tangível, fato que autorizaria a aplicação da proteção conferida ao patrimônio no Código Penal. Para Albuquerque[193] não é possível considerar os dados armazenados coisas móveis, podendo apenas ser objeto de crimes patrimoniais clássicos como furto, roubo, dano e apropriação indébita, nos casos em que "formarem uma unidade material com o respectivo suporte"[194]. Na mesma linha, Rossini[195] vislumbra a total impossibilidade de caracterizar conduta com tipo em que conste a elementar 'coisa', ressalvando que a tipicidade poderia ocorrer somente com equiparação legal. Dessa forma, para o autor não seriam todos os crimes contra o patrimônio que poderiam ser cometidos com o auxílio da informática, mas tão somente aqueles que possuem "compatibilidade típica com a informática/telemática, como é o caso do estelionato"[196].

Com opinião divergente em relação à restrita visão sobre dados dos autores citados anteriormente, Vianna[197], ao estudar a repressão penal de vírus de computador, sustenta que dados são coisas, pelo simples fato de existirem. Assim, gozariam da tutela penal, sendo que a conduta de criação e divulgação de vírus poderia ser enquadrada como crime de dano, fulcro no art. 163 do Código Penal, ainda que preferível a sua específica tipificação.

Não obstantes os tipos penais que tutelam os tradicionais bens jurídicos (honra, patrimônio, etc), o Brasil também possui tipos penais que, expressamente, prevêem a utilização das TICs para a execução do delito, bem como condutas típicas que buscam proteger essas tecnologias[198], no tocante a sua integridade, confiabilidade e disponibilidade. Podem ser mencionadas como exemplos as seguintes condutas criminalizadas no Código Penal: art. 153, § 1°- A (divulgação de segredo contido ou não em sistemas informáticos ou banco de dados da Administração Pública)[199]; art. 313 - A (inserção de dados falsos em sistema de informações ou banco de dados da Administração Pública)[200]; art. 313-B

[193] ALBUQUERQUE, Op. Cit., p. 44-46.
[194] Id., Op. Cit., p. 46.
[195] ROSSINI, Op. Cit., p. 217.
[196] ROSSINI, Op. Cit., p. 217-218.
[197] VIANNA, *Fundamentos*, p. 21-22.
[198] LIMA, Op. Cit., p. 159-163.
[199] Art. 153 - Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem: Pena - detenção, de um a seis meses, ou multa. § 1º Somente se procede mediante representação. § 1º-A. Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública: Pena - detenção, de 1 (um) a 4 (quatro) anos, e multa. § 2º Quando resultar prejuízo para a Administração Pública, a ação penal será incondicionada.
[200] Art. 313-A. 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

(modificação não autorizada de sistemas de informação por funcionário público) [201] e art. 325, § 1°, I e II (violação de sigilo profissional com facilitação de acesso não autorizado a sistemas informáticos ou banco de dados da Administração Pública ou uso indevido de acesso restrito, respectivamente[202]).

Outras legislações esparsas também tipificam delitos cibernéticos, tais como: art. 12 da Lei n.° 9.609/1998 (violação do direito do autor de programa de computador)[203]; art. 10 da Lei n.° 9.296/1996 (quebra de sigilo)[204]; art. 72 da Lei n.° 9.504/1997 (descreve condutas relacionadas ao acesso aos sistemas informáticos da Justiça Eleitoral para modificar o resultado, bem como de inserção de comando e/ou programa para alteração ou supressão de dados, dentre outras ações, e, por fim, de dano físico à urna eletrônica ou ao equipamento de totalização dos votos)[205], art. 2°, V, da Lei n.° 8.137/1990 (uso ou divulgação de programa que permita que o sujeito passivo de obrigação tributária obtenha informação contábil diversa da realidade)[206]; e arts. 241-A, 241-B, 241-C e 241-D do Estatuto da Criança e do Adolescente - ECA (tipos que buscam combater a pedofilia e a pornografia infantil, inclusive a posse deste material, notadamente na Internet)[207], acrescidos pela Lei n.° 11.829/2008[208].

---

fim de obter vantagem indevida para si ou para outrem ou para causar dano: Pena - reclusão, de 2 (dois) a 12 (doze) anos, e multa.

[201] Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente: Pena - detenção, de 3 (três) meses a 2 (dois) anos, e multa.

[202] Art. 325 - Revelar fato de que tem ciência em razão do cargo e que deva permanecer em segredo, ou facilitar-lhe a revelação: Pena - detenção, de seis meses a dois anos, ou multa, se o fato não constitui crime mais grave. § 1º Nas mesmas penas deste artigo incorre quem: I - permite ou facilita, 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; II - se utiliza, indevidamente, do acesso restrito.

[203] Art. 12. 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.

[204] Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei.

[205] Art. 72. Constituem crimes, puníveis com reclusão, de cinco a dez anos: I - obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de alterar a apuração ou a contagem de votos; II - desenvolver ou introduzir 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; III - causar, propositadamente, dano físico ao equipamento usado na votação ou na totalização de votos ou a suas partes.

[206] Art. 1° Constitui crime contra a ordem tributária suprimir ou reduzir tributo, ou contribuição social e qualquer acessório, mediante as seguintes condutas: [...] Art. 2° Constitui crime da mesma natureza: [...] V - utilizar ou divulgar 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. Pena - detenção, de 6 (seis) meses a 2 (dois) anos, e multa.

[207] Art. 241. Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: Pena – reclusão, de 4 (quatro) a 8 (oito) 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

Ainda não existe em nosso ordenamento uma legislação própria sobre os crimes cibernéticos, embora existam diversos Projetos de Lei (PL) em tramitação no Congresso Nacional referentes a esta temática. Nesse sentido, destaca-se o Projeto de Lei n° 84/1999 (apensador dos Projetos de Lei n.° 2.557, 2.558 e 3.796/2000. No Senado, recebeu a numeração 89/2003, apensando o Projeto de Lei do Senado - PLS n.° 137/2000, o qual já apensava o PLS n.° 76/2000), cujo substitutivo de autoria do Senador Eduardo Azeredo foi aprovado no Senado e encaminhado para Câmara. Em 5 de março de 2009, o substitutivo foi aprovado, no mérito, pela Comissão de Constituição e Justiça e de Cidadania (CCJC) da Câmara dos Deputados. Após mais de ano com trâmite paralisado, em agosto de 2010, foi apresentado parecer da Comissão de Segurança Pública e Combate ao Crime Organizado (CSPCCO), defendendo sua aprovação. Já em outubro do mesmo ano e em janeiro de 2011, a

---

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.

Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa. § 1º Nas mesmas penas incorre quem: I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo; II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo. § 2º As condutas tipificadas nos incisos I e II do § 1º deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo.

Art. 241-B. Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. § 1º A pena é diminuída de 1 (um) a 2/3 (dois terços) se de pequena quantidade o material a que se refere o caput deste artigo. § 2º Não há crime se a posse ou o armazenamento tem a finalidade de comunicar às autoridades competentes a ocorrência das condutas descritas nos arts. 240, 241, 241-A e 241-C desta Lei, quando a comunicação for feita por: I – agente público no exercício de suas funções; II – membro de entidade, legalmente constituída, que inclua, entre suas finalidades institucionais, o recebimento, o processamento e o encaminhamento de notícia dos crimes referidos neste parágrafo; III – representante legal e funcionários responsáveis de provedor de acesso ou serviço prestado por meio de rede de computadores, até o recebimento do material relativo à notícia feita à autoridade policial, ao Ministério Público ou ao Poder Judiciário. § 3º As pessoas referidas no § 2º deste artigo deverão manter sob sigilo o material ilícito referido.

Art. 241-C. Simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual: Pena – reclusão, de 1 (um) a 3 (três) anos, e multa. Parágrafo único. Incorre nas mesmas penas quem vende, expõe à venda, disponibiliza, distribui, publica ou divulga por qualquer meio, adquire, possui ou armazena o material produzido na forma do caput deste artigo.

Art. 241-D. Aliciar, assediar, instigar ou constranger, por qualquer meio de comunicação, criança, com o fim de com ela praticar ato libidinoso: Pena – reclusão, de 1 (um) a 3 (três) anos, e multa. Parágrafo único. Nas mesmas penas incorre quem: I – facilita ou induz o acesso à criança de material contendo cena de sexo explícito ou pornográfica com o fim de com ela praticar ato libidinoso; II – pratica as condutas descritas no caput deste artigo com o fim de induzir criança a se exibir de forma pornográfica ou sexualmente explícita.

[208] A edição da Lei n.° 11.829, de 25 de novembro de 2008, é fruto do trabalho da Comissão Parlamentar de Inquérito – CPI da Pedofilia do Senado Federal, cuja promulgação rendeu ao Presidente Luiz Inácio Lula da Silva o Prêmio Mundial das Telecomunicações e Sociedade da Informação 2009 da União Internacional de Telecomunicações – UIT. A temática escolhida para o Prêmio de 2009 foi justamente a proteção das crianças no ambiente virtual.

CCJC emitiu novos pareceres, de relatoria do Deputado Regis de Oliveira[209], restando a apreciação do Plenário da Casa.

Cabe a ressalva de que o último parecer do relator do PL na CCJC, apresentado em 25/01/2011, inovou com a introdução de diversas emendas supressivas, a fim de retirar do texto os termos "dispositivos de comunicação", com o intuito de reduzir a abrangência dos tipos penais e eliminar grande parte das críticas ao projeto.

Em 14/06/2011, foi apresentado o Parecer n.° 4 do relator na Comissão de Ciência e Tecnologia, Comunicação e Informática (CCTCI), de relatoria do Deputado Eduardo Azeredo (responsável pela redação do substitutivo aprovado no Senado Federal)[210], que, na mesma linha do parecer do Deputado Regis de Oliveira, sugere, em síntese, a aprovação do substitutivo com a supressão dos termos "dispositivos de comunicação" e/ou "redes de computador" a fim de reduzir o seu escopo de aplicação e buscar algum apoio para a aprovação do PL.

Relembra-se que a discussão em torno do projeto ressurgiu com força em face dos ataques *DOS* vivenciados por sites governamentais em junho de 2011, assumidos pelo grupo de hackers LulzSecBrazil, os quais tiraram do ar sites da presidência da república e do governo federal, reacendendo o debate no país sobre a necessidade de lei para punição destas práticas.

Assim, em que pese o atual trâmite do projeto, ainda na pauta da CCTCI, acredita-se remota a possibilidade do PL ser votado com o texto hoje vigente, mesmo com as emendas supressivas e de rejeição propostas, em face dos problemas de definição de alguns crimes, *v.g*. de acesso não autorizado e de código malicioso e a ausência de consenso sobre o tempo de manutenção dos *logs* de acesso pelos provedores[211;212].

A falha na descrição de alguns dos tipos propostos, bem como a polêmica no tocante à obrigação dos provedores de armazenar 'os rastros' dos usuários e de denunciar à polícia eventuais práticas ilícitas rendeu a esse Projeto a alcunha de "AI-5 Digital", sendo objeto de grande manifestação contrária da sociedade civil, da academia e da comunidade técnica, que

---

[209] Trâmite do PL pode ser consultado em: <http://www.camara.gov.br/internet/sileg/Prop_Detalhe.asp?id=15028>. Acesso em: 21/02/2011.

[210] Trâmite do PL e texto integral do parecer pode ser consultado em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=15028> . Acesso em: 24/11/2011.

[211] Nesse sentido ver CENTRO DE TECNOLOGIA E SOCIEDADE, ESCOLA DE DIREITO DO RIO DE JANEIRO DA FUNDAÇÃO GETULIO VARGAS. *Comentários e Sugestões sobre o substitutivo do Projeto de Lei de Crimes Eletrônicos (PL n. 84/99) apresentado pela Comissão de Constituição e Justiça e de Cidadania, nov. 2009.* Disponível em: <http://virtualbib.fgv.br/dspace/bitstream/handle/10438/7719/coment%c3%a1rios%20ao%20substitutivo%20PL%2088-99.pdf?sequence=1>. Acesso em: 16/11/2010. 38 p.

[212] Tendo em vista a incerteza sobre os rumos do PL, o presente trabalho não fará uma análise detalhada do Projeto e dos tipos penais ali contemplados.

sustentam que primeiramente deve ser assentado os direitos dos usuários na Internet, ou seja, o marco civil, para posteriormente, tratar-se da criminalização de condutas.

Nesse sentido, louva-se a o envio ao Congresso do Projeto de Lei n.° 2.126/2011[213], que trata do Marco Civil da Internet, abarcando os princípios do uso da Internet no Brasil, direitos dos usuários, responsabilidade dos provedores de acesso e de conteúdo, guarda de logs, etc, o qual foi construído após extenso e inovador processo de consulta pública que recebeu a contribuição, inclusive, de outros países.

Faz-se necessário mencionar que o prosseguimento da tramitação e discussão do PL n.° 84/1999, revigorado após os ataques sofridos pelas páginas governamentais em junho de 2011 relatados anteriormente, gerou a proposição de novo projeto de lei, o PL n.° 2.793/2011[214], proposto recentemente em 29/11/2011 como alternativa ao PL n.° 84/1999, no intuito de tipificar delitos informáticos, sem supostamente incorrer nos erros deste, criminalizando somente as condutas socialmente reconhecidas como ilegítimas e graves[215].

Ainda sobre propostas legislativas, o recente Anteprojeto de atualização do Código de Defesa do Consumidor propõe no art. 72-A, a inclusão de um crime cibernético próprio, garantindo tutela penal a confidencialidade de dados, informações ou identificadores pessoais[216].

Parte da doutrina advoga pela necessidade de edição de novas leis para dar o adequado tratamento a essas novas condutas criminosas. Na mesma linha Lima[217] salienta que a "legislação existente é mesmo incapaz de atender de forma eficaz todas as questões atinentes a essa prática criminosa", posição sustentada também por I. S. Ferreira[218], que ressalta a necessidade de reformulação da legislação a fim de acompanhar o crescimento da delinquência cibernética.

---

[213] Texto completo do PL disponível em:<http://www.planalto.gov.br/ccivil_03/Projetos/PL/2011/msg326-24ago2011.htm>. Acesso em: 24/11/2011.

[214] Projeto de Lei n.° 2.793/2011 de autoria dos Deputados Federais Paulo Teixeira, Luiza Erundina, Manuela D'Àvila, João Arruda, Brizola Neto e Emiliano José. Texto completo e informações sobre a tramitação disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=529011#>. Acesso em: 30/11/2011.

[215] Ver justificatição do PL n.° 2.793/2011, disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao? idProposicao=529011#>. Acesso em: 30/11/2011

[216] Texto do anteprojeto disponível na íntegra em: <http://www12.senado.gov.br/noticias/materias/2012/03/14/veja-a-integra-do-anteprojeto-que-atualiza-o-codigo-do-consumidor >. Acesso em: 26/03/2012. **Art. 72-A.** Veicular, hospedar, exibir, licenciar, alienar, utilizar, compartilhar, doar ou de qualquer forma ceder ou transferir dados, informações ou identificadores pessoais, sem a expressa autorização de seu titular e consentimento informado, salvo exceções legais. Pena – Reclusão, de um a quatro anos, e multa.

[217] LIMA, Op. Cit., p. 9.

[218] FERREIRA, Ivette, Op. Cit., p. 163.

No mesmo sentido, Gouvêa[219] confirma que crimes já tipificados não precisam de revisão, cabendo a promulgação de novas leis para tipificar condutas em que o sistema de informática seja lesionado.

Vianna[220] ressalta que uma "legislação penal moderna e bem elaborada" que tratasse adequadamente os crimes por computador, tornaria mais fácil a atuação dos operadores do Direito e o ideal seria que fosse regulada por um tratado internacional por ser um fenômeno transnacional. Outrossim, o autor sustenta que não se pode enxergar a edição de legislação como *conditio sine qua non* para a repressão desses crimes, punindo-se os já tipificados no nosso sistema.

Partilha-se do entendimento adotado por Cruz[221] que prescreve que "em determinadas hipóteses, é evidente a necessidade de novos preceitos penais; já em outras, basta apenas uma reinterpretação dos elementos normativos dos tipos penais tradicionais".

Dessa forma, não se faz necessária a inovação legislativa a fim de criminalizar condutas enquadradas como crimes cibernéticos pela utilização das TICs como ferramenta para a prática do crime, mas, tão somente, daquelas cujos alvos são as TIC, a criminalidade cibernética que é classificada como própria. Daoun[222] corrobora:

> [...] existem situações fáticas em que a inovação não está no meio empregado para o cometimento do crime. São hipóteses de que a tecnologia, o dado, a informação e o sistema informatizado estejam como finalidade almejada pelo agente no desempenho da conduta criminosa. Reiterando, são os crimes informáticos de natureza pura (ou próprios).
> Em tais situações, por não haver tutela expressa do bem jurídico na legislação penal brasileira e não se admitir a aplicação da analogia maléfica, *in malam partem*, permite-se elaborar, atentando-se para o princípio constitucional da reserva legal, uma regulamentação própria e específica por meio de tipos penais que contenham tal previsão.

Como exemplos das condutas que devem ser objeto de tipificação, Rosa[223] elenca um rol de treze novos comportamentos cometidos no ambiente informático que poderiam ou deveriam ser contemplados em legislação: fraude/falsidade informática; danos afetando dados ou programas informáticos/danificação de informações e/ou programas de computadores; pichação (colocação indevida de textos ou figuras em site de terceiros); sabotagem informática (inclusão, modificação ou exclusão de dados de programas com o objetivo de prejudicar seu funcionamento); acesso indevido/ilegal/não autorizado; utilização não

[219] GOUVÊA, Op. Cit., p. 138.
[220] VIANNA, *Dos Crimes*, p. 212.
[221] CRUZ, Op. Cit., p. 5.
[222] DAOUN, Crimes, p. 181-182.
[223] ROSA, Op. Cit., p. 65-66.

autorizada de um sistema informático; interceptação não autorizada; pirataria/reprodução não autorizada de um programa informático protegido; utilização não autorizada de um programa informático protegido; espionagem informática/fuga de dados; spam; furto de informações; e divulgação de informações sem autorização de autoridade competente ou de pessoa interessada, quando necessária.

Sustenta Vianna[224] que a tipificação de uma única conduta seria suficiente para o enfrentamento desta criminalidade a ser inserida no capítulo dos crimes contra a liberdade individual do Código Penal ou em lei especial, que seria o delito de violação de computadores, sugerindo a seguinte redação:

> 4.1. Violação de Computadores
> Devassar indevidamente computadores ligados em rede, acessando dados para os quais não possui permissões de acesso:
> Pena: De X a Y.
> 4.2. Forma qualificada
> § 1°. Se o agente modifica, apaga ou acrescenta dados no computador devassado:
> Pena: De X1>Y1 (em que X1>X e Y1>Y).
> 4.3. Aumento de pena
> § 2°. Aumenta-se a pena em Z, se o crime é cometido com o fim de se obter vantagem econômica de qualquer natureza, para si ou para outrem.
> 4.4. Ação penal
> § 3°. O crime que trata este artigo e seus parágrafos somente se procede mediante representação.

Sobre a proposição, o autor[225] também elucida que o bem jurídico é a liberdade individual e o consequente direito à inviolabilidade das informações que ficam armazenadas nos computadores e que a conduta é devassar, ou seja, olhar dentro, ter conhecimento, sendo que o elemento normativo 'indevidamente' pressupõe que a conduta seja ilegítima, sem autorização.

É louvável a proposta supracitada, datada de um trabalho apresentado em outubro de 2000 e certamente resolveria diversos casos em que não é possível enquadrar a conduta nos tipos penais existentes. No entanto, parece que melhor funcionaria como um tipo subsidiário a ser aplicado quando não for possível a configuração como outros delitos cibernéticos puros. Primeiro por que a evolução tecnológica e o uso criminal das TICs vivenciados na última década demonstram a necessidade de tipificação adequada de diversas condutas, a fim de que as ações sejam devidamente repreendidas, uma vez que o bem jurídico não se limita a liberdade individual. Ademais, a sugestão de qualificadora e majorante para a adequação da

[224] VIANNA, *Dos Crimes*, p. 217-218.
[225] VIANNA, *Dos Crimes*, p. 218.

pena não é suficiente para tornar proporcional o cálculo de pena em face do potencial lesivo de determinados crimes.

Menciona-se ainda a proposta de Silva Júnior[226] que fixa como tipo hipotético, também tutelando a inviolabilidade de dados de informação constantes em sistemas computacionais, a conduta de "acessar, inserir, retirar ou modificar, de forma indevida ou não autorizada, senhas, dados e informações constantes de um sisema computacional", aplicando-se à proposta do autor as mesmas observações à proposição de tipificação única defendida por Vianna[227].

Depois de ter descrito, ainda que superficialmente, como se dá o combate destes crimes no Brasil, cumpre, por fim, relatar a peculiar existência de um Termo de Ajustamento de Conduta firmado entre o GOOGLE e o Ministério Público Federal, sendo único no mundo.

A empresa Google Brasil Internet Ltda. (GOOGLE), integrante do grupo econômico *Google Inc.*, com sede nos Estados Unidos, é uma empresa provedora de serviço de valor adicionado, nos termos no art. 60, parágrafo da Lei n. 9.472, de 17 de julho de 1997, mais especificamente, provedora de conteúdo e dos serviços de correio eletrônico, de busca, de armazenamento de vídeos, de armazenamento de fotos, de páginas de relacionamentos, dentre outros. A empresa é notadamente conhecida pelas marcas Google, Gmail, Orkut, YouTube, Picasa etc.

Em 30 de junho de 2008, o GOOGLE (compromitente) assinou um Termo de Ajustamento de Conduta (TAC)[228] com a Procuradoria da República no Estado de São Paulo (compromissária), órgão do Ministério Público Federal (MPF), que constitui título executivo extrajudicial, nos termos do art. 5º**,** § 6.°, da Lei 7.347/1985. O TAC impõe diversas obrigações de fazer à entidade, grande parte destas sem amparo em leis que lhe imputassem tais deveres, prevendo que o seu descumprimento substancial implica multa no valor de R$ 25.000,00 (vinte e cinco mil reais) por dia de atraso, sem prejuízo da execução judicial para cumprimento da obrigação, consoante cláusula nona.

---

[226] SILVA JÚNIOR, Op. Cit., p. 332.
[227] VIANNA, *Dos Crimes*, p. 217-218.
[228] Cópia integral do TAC disponível em: <http://www.prsp.mpf.gov.br/crimes-ciberneticos/TACgoogle.pdf>. Acesso em: 21/01/2010.

Em síntese, o TAC, no qual a SaferNet Brasil[229], organização não governamental cujo foco é a proteção de crianças e adolescentes no ambiente virtual e que hoje é responde pelo recebimento de denúncias de alguns crimes cibernéticos[230] (especialmente aqueles relacionados a violações aos Direitos Humanos como pornografia infantil e pedofilia, discriminação racial, intolerância religiosa etc) integra como interveniente anuente ao TAC, obriga o GOOGLE, em relação ao ORKUT, a guardar os registros dos *logs* de acesso[231], que abrangem, em essência, dados relativos ao endereço do IP (*Internet Protocol*) [232] utilizado e as datas e os horários de início e de término do acesso, aponta BARROS[233].

Além da guarda desses registros, que somente será fornecida mediante ordem judicial, o TAC também contempla, como obrigação do GOOGLE, a preservação desses *logs;* a comunicação ao MPF das ocorrências de pornografia infantil denunciadas no Centro Nacional para Crianças Desaparecidas e Exploradas, relacionadas às ocorrências realizadas a partir do território brasileiro; a comunicação ao MPF de ocorrências de pornografia infantil; a retirada de conteúdo ilícito a pedido de ordem da Justiça, MP ou autoridade policial do ORKUT, bem como sua preservação para fins de investigação; verificação de conteúdo postado por usuários do ORKUT, inclusive aqueles definidos pelo próprio usuário como restrito, a fim de identificar em quais existem indícios de materialidade do crime tipificado no art. 241 do Estatuto da Criança e do Adolescente (pornografia infantil) [234] ou foram denunciadas no

---

[229] Mais informações sobre a entidade podem ser obtidas no seu site disponível em: <http://www.safernet.org.br>. Acesso em: 28/10/2009. Ressalta-se que em 12/11/2010 o Ministério Público Federal rescindiu unilateral e parcialmente o TAC celebrado com a entidade, em razão da constatação de falhas na análise dos conteúdos notificados através da "Central Nacional de Denúncias", sendo que o conteúdo da Nota Técnica do MPF que comunica a rescisão está disponível em:<http://www.prsp.mpf.gov.br/sala-de-imprensa/noticias_prsp/12-11-10-nota-publica-mpf-rescinde-termo-de-cooperacao-com-safernet/>. Acesso em: 23/05/2011. Em contrapartida, a SaferNet também publicou nota técnica contestando o parecer técnico do MPF, a qual encontra-se disponível em: <http://www.safernet.org.br/site/noticias/nota-p%C3%BAblica-safernet-contesta-parecer-t%C3%A9cnico-mpf-sp>. Acesso em: 23/05/2011.

[230] *Hotline* de denúncias brasileiras, disponível em: <http://www.denunciar.org.br>. Acesso em: 21/01/2010.

[231] Definido por PINHEIRO, *Op. Cit*., p. 365, como "registro de atividades gerado por programas de computador".

[232] Definido por PINHEIRO, *Op. Cit*., p. 358, como "é o endereçamento real de uma máquina na Internet. Consiste em uma série de números separados por pontos. Cada máquina conectada à rede tem um endereço IP. Os Domain Name Servers servem para relacionar os 'endereços com letras' com o endereço IP". A autora ainda define IP na mesma obra, p. 364, como "protocolo responsável pelo percurso de pacotes entre dois sistemas que utilizam a família de protocolos TCP/IP desenvolvida e utilizada na Internet".

[233] BARROS, Marco Antonio de. Tutela Punitiva Tecnológica. *In*: PAESANI, Liliana Minardi (Coord.). *O Direito na Sociedade da Informação*. São Paulo: Editora Atlas, 2007. 333 p. p. 275-300. p. 292.

[234] Art. 241. Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa. Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa. § 1º Nas mesmas penas incorre quem: I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo; II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo. § 2º As condutas

Centro Nacional para Crianças Desaparecidas e Exploradas; desenvolver filtro de detecção automática de imagens caracterizadas como pornografia infantil; manter lista atualizada de URLs (*uniform resourse locator*)[235] contendo pornografia infantil, a fim de possibilitar a rápida detecção e remoção desses links do ORKUT; detectar e remover outras contas Google pertencentes a usuários já excluídos por manipulação de pornografia infantil e revisar, manualmente, páginas suspeitas mais acessadas ou relacionadas a usuários que já tenham, confirmadamente, manipulado pornografia infantil[236].

---

tipificadas nos incisos I e II do § 1º deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo. Art. 241-B. Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. § 1º A pena é diminuída de 1 (um) a 2/3 (dois terços) se de pequena quantidade o material a que se refere o caput deste artigo. § 2º Não há crime se a posse ou o armazenamento tem a finalidade de comunicar às autoridades competentes a ocorrência das condutas descritas nos arts. 240, 241, 241-A e 241-C desta Lei, quando a comunicação for feita por: I – agente público no exercício de suas funções; II – membro de entidade, legalmente constituída, que inclua, entre suas finalidades institucionais, o recebimento, o processamento e o encaminhamento de notícia dos crimes referidos neste parágrafo; III – representante legal e funcionários responsáveis de provedor de acesso ou serviço prestado por meio de rede de computadores, até o recebimento do material relativo à notícia feita à autoridade policial, ao Ministério Público ou ao Poder Judiciário. § 3º As pessoas referidas no § 2º deste artigo deverão manter sob sigilo o material ilícito referido. Art. 241-C. Simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual: Pena – reclusão, de 1 (um) a 3 (três) anos, e multa. Parágrafo único. Incorre nas mesmas penas quem vende, expõe à venda, disponibiliza, distribui, publica ou divulga por qualquer meio, adquire, possui ou armazena o material produzido na forma do caput deste artigo. Art. 241-D. Aliciar, assediar, instigar ou constranger, por qualquer meio de comunicação, criança, com o fim de com ela praticar ato libidinoso: Pena – reclusão, de 1 (um) a 3 (três) anos, e multa. Parágrafo único. Nas mesmas penas incorre quem: I – facilita ou induz o acesso à criança de material contendo cena de sexo explícito ou pornográfica com o fim de com ela praticar ato libidinoso; II – pratica as condutas descritas no caput deste artigo com o fim de induzir criança a se exibir de forma pornográfica ou sexualmente explícita. Art. 241-E. Para efeito dos crimes previstos nesta Lei, a expressão "cena de sexo explícito ou pornográfica" compreende qualquer situação que envolva criança ou adolescente em atividades sexuais explícitas, reais ou simuladas, ou exibição dos órgãos genitais de uma criança ou adolescente para fins primordialmente sexuais.

[235] Recurso Localizador Uniforme – "localizador que permite identificar e acessar um serviço na rede Web", conforme definição do Glossário da Associação de Software Livre disponível em: <http://wiki.softwarelivre.org/bin/viewfile/PCLivre/GlossariO?rev=1;filename=glossario-6.pdf>. Acesso em: 21/01/2010.

[236] Traz-se à colação fragmentos mais importantes do TAC. "***Cláusula Segunda.*** Em relação ao ORKUT, a COMPROMITENTE obriga-se a: a) **assegurar, a partir de 1º de Julho de 2008, a retenção e a acessibilidade** nos servidores, pelo prazo mínimo de 180 (cento e oitenta) dias, dos seguintes dados que detiver das **conexões efetuadas por usuários a partir do Brasil**: e-mail de acesso (login), número IP de criação, logs de acesso, data, hora e referência GMT das conexões. **A retenção desses dados se dará de forma automática e sem necessidade de qualquer pedido específico por parte das autoridades competentes**; b) **fornecer, mediante ordem judicial**, as evidências referidas na alínea anterior, de forma padronizada e clara, conforme padrão atualmente utilizado, constante do anexo I do presente Termo; c) **assegurar a preservação**, a partir de 1º de julho de 2008, por prazo de até 180 (cento e oitenta) dias, ou até fornecidas as informações, o que ocorrer antes, **dos dados referidos na alínea "a" acima**, **além do conteúdo especificamente requerido pelas autoridades competentes para a investigação do crime de pornografia infantil, tipificado no art. 241 do Estatuto da Criança e do Adolescente (Lei Federal 8.069/90).** Referido conteúdo poderá incluir scraps, mensagens, tópicos, imagens e fotos existentes nos servidores no momento do recebimento do pedido. O prazo de 180 (cento e oitenta) dias poderá, em relação a uma evidência sobre a qual haja o risco de perda no curso de uma investigação devidamente identificada e individualizada, ser prorrogado por um período adicional de 180 (cento e oitenta) dias, mediante solicitação que deverá, preferencialmente e sem prejuízo dos meios regulares de notificação, ser enviada através de e-mail específico disponibilizado pela COMPROMITENTE; d) fornecer, a partir de 1.º de julho de 2008**,** mediante ordem judicial, as informações referidas nas alíneas acima em meio

Não se pretende juridicamente discutir o conteúdo do TAC assinado, limitando-se o trabalho a descrever o termo de cooperação sobre a atuação do GOOGLE no território brasileiro. Da mesma forma, não é objeto desta pesquisa o exame valorativo dos deveres assumidos pela empresa, que se enquadram num debate muito mais amplo de segurança *versus* privacidade. Repisa-se que o Brasil é o único país no mundo no qual o grupo firmou tal

---

magnético, papel ou qualquer outro meio de prova válido, conforme determinado pelo juízo competente; e) **informar à COMPROMISSÁRIA**, por via eletrônica ou outro meio de comunicação inequívoco, e independentemente de solicitação específica, **as ocorrências de pornografia infantil reportadas ao National Center for Missing and Exploited Children - NCMEC que digam respeito a conexões efetuadas em território brasileiro, incluindo a informação de identificação associada ao relatório da ocorrência, o que permitirá à COMPROMISSÁRIA** obter ordem judicial específica para fornecimento dos dados referidos no item "c" acima; f) **informar à COMPROMISSÁRIA, sem prejuízo do disposto na alínea anterior, por via eletrônica ou outro meio de comunicação inequívoco, e independentemente de solicitação específica, a ocorrência de qualquer das condutas tipificadas no art. 241 do Estatuto da Criança e do Adolescente** (Lei Federal 8.069/90). A COMPROMITENTE declara, neste ato, que o envio de informações sobre a possível existência de pornografia infantil em seus serviços é feito no intuito exclusivo de colaborar com as autoridades públicas na identificação dos autores do delito. Assim, a avaliação da COMPROMITENTE sobre qualquer conteúdo em que se alegue a existência de pornografia infantil é feita de boa-fé e não constitui, em relação à COMPROMITENTE, nenhum juízo de valor a respeito dos conteúdos notificados; g) **mediante ordem judicial, requerimento escrito de autoridade policial, ministerial ou ao seu critério, promover a retirada de conteúdos alegadamente ilícitos hospedados no ORKUT e assegurar, a partir de 1º de julho de 2008, mediante requerimento específico, a preservação e acessibilidade por 180 (cento e oitenta) dias dos dados e conteúdo que detiver referidos nas alíneas "a" e "c" acima, conforme o objeto da ordem ou requerimento. Se houver controvérsia em relação à ilicitude do conteúdo, as partes reconhecem que caberá ao juízo competente decidir se o conteúdo deve ou não ser removido**. Se a COMPROMISSARIA ou outra autoridade requerente julgar que uma evidência sobre a qual haja o risco de perda no curso de uma investigação devidamente identificada e individualizada deva ter seu tempo de retenção prorrogado, ela poderá, mediante solicitação escrita, solicitar um período adicional de retenção de 180 (cento e oitenta) dias; [...] **Cláusula Quarta.** Também em relação ao ORKUT, a COMPROMITENTE se obriga a: a) **quanto aos conteúdos postados por usuários a partir de conexões efetuadas no Brasil - inclusive conteúdos definidos por esses usuários como de acesso restrito a sua própria rede de relacionamentos – implementar, em conjunto com** a INTERVENIENTE ANUENTE, a partir de 1º de Julho de 2008, um processo que permitirá a esta última encaminhar à COMPROMITENTE - com cópia para a COMPROMISSÁRIA - uma lista diária com até 500 URL`s em relação às quais a COMPROMITENTE se obriga a: **i) verificar e informar à INTERVENIENTE ANUENTE – ou, em sua falta, diretamente à COMPROMISSÁRIA - quais dentre essas URL's continham indícios da materialidade do delito tipificado no art. 241 do Estatuto da Criança e do Adolescente e/ou foram objeto de comunicação ao National Center for Missing and Exploited Children – NCMEC, bem como a respectiva informação de identificação junto a esse órgão.** A COMPROMITENTE declara, neste ato, que o envio de informações sobre a possível existência de pornografia infantil em seus serviços é feito no intuito exclusivo de colaborar com as autoridades públicas na identificação dos autores do delito. Assim, a avaliação da COMPROMITENTE sobre qualquer conteúdo em que se alegue a existência de pornografia infantil é feita de boa-fé e não constitui, em relação à COMPROMITENTE, nenhum juízo de valor a respeito dos conteúdos notificados; ii) **com relação às demais URL's, verificar e informar à INTERVENIENTE ANUENTE – ou, em sua falta, diretamente à COMPROMISSÁRIA - quais foram retiradas do ar;** iii) em qualquer dos casos acima, quando a COMPROMITENTE tenha retirado o respectivo conteúdo do ar, assegurar a preservação e acessibilidade dos respectivos dados de usuário e conteúdos existentes nas URL's notificadas por 180 dias contados a partir do recebimento, pela COMPROMITENTE, da notificação encaminhada pela INTERVENIENTE ANUENTE, e que serão fornecidos às autoridades brasileiras mediante ordem judicial; [...] b) **assegurar a implementação, a partir de 1.º de julho de 2008, de uma nova tecnologia de filtros destinada a: 1) detecção automática de imagens conhecidas de pornografia infantil inseridas nas páginas do ORKUT; 2) manutenção de uma lista regularmente atualizada de URL's contendo pornografia infantil, incluindo URL's fornecidas pela INTERVENIENTE ANUENTE e outras organizações de proteção à infância, para possibilitar a rápida detecção e remoção desses links das páginas do ORKUT; 3) detecção automática e remoção de outras contas Google pertencentes a usuários já excluídos por manipulação de pornografia infantil; d) revisões manuais de páginas suspeitas mais acessadas ou relacionadas a usuários que já tenham confirmadamente manipulado pornografia infantil;** [...]" (Grifo nosso).

acordo e que inexiste qualquer dispositivo legal que obrigue a empresa a adotar tais condutas. Parece que justamente a ausência de lei e a existência de jurisprudência não uniforme sobre a responsabilidade de provedores tenham funcionado como incentivos à adesão do GOOGLE ao TAC.

O Livro Verde sobre Segurança Cibernética[237] no Brasil, organizado sob a coordenação do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República, destina um dos seus capítulos a apresentar uma visão do país face aos marcos recentes, elencando as oportunidades e os desafios relacionados à segurança cibernética, nos vetores político-estratégico, econômico, social e ambiental, ciência e tecnologia, educação, legal, cooperação internacional e segurança das infraestruturas críticas, destacando-se aqui alguns itens do aspecto legal e de cooperação[238]:

> LEGAL
> OPORTUNIDADES
> [...];
> O Código Penal do Brasil tem Artigos que atendem a determinados crimes com uso de computador;
> [..].
> DESAFIOS
> Ausência de legislação nacional e internacional específica de segurança cibernética, em especial contra crimes cibernéticos;
> [...].
> COOPERAÇÃO INTERNACIONAL
> OPORTUNIDADES
> [...];
> Grupo de trabalho instituído em 2010, no âmbito da ONU, para elaborar proposta de uma nova Convenção, de caráter global, contra o crime cibernético, sob a coordenação do Embaixador do Brasil em Viena.
> DESAFIOS
> [...];
> Ausência de instrumentos internacionais específicos contra crimes cibernéticos para ação policial transfronteiras;

---

[237] Para fins de compreensão do termo no presente trabalho, adota a definição ampla de segurança cibernética proposta pelo Setor de Normalização da União Internacional de Telecomunicações, na Recomendação n. ° X.1205, disponível em: <http://www.itu.int/rec/T-REC-X.1205-200804-I>. Acesso em: 04/04/2011. Segundo o documento, Segurança Cibernética é o conjunto de ferramentas, políticas, conceitos de segurança, salvaguardas de segurança, diretrizes, abordagens de gestão de riscos, ações de treinamento, melhores práticas, garantias e tecnologias que podem ser usados para proteger o ambiente cibernético e ativos de usuários e de organizações. Ativos de usuários e organizações incluem dispositivos de computação conectados, pessoal, infraestrutura, aplicações, serviços, sistemas de telecomunicações, e a totalidade das informações transmitidas e/ou armazenadas no ambiente virtual. A Segurança Cibernética se esforça para assegurar a obtenção e a manutenção das propriedades de segurança de ativos dos usuário e das organizações contra relevante riscos de segurança no ambiente cibernético. Os objetivos gerais de segurança incluem: disponibilidade, integridade e confidencialidade (Tradução nossa).

[238] BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. *Livro verde: segurança cibernética no Brasil*. Brasília: GSIPR/SE/DSIC, 2010. 63 p. p. 39-40. Disponível em: <http://dsic.planalto.gov.br/documentos/publicacoes/1_Livro_Verde_SEG_CIBER.pdf>. Acesso em: 06/03/2011.

> Articulação, ainda incipiente, em termos de definição de ações transnacionais de segurança cibernética, com foco em crimes cibernéticos; [...].

Na visão proposta pela publicação supracitada[239], a inexistência de legislação específica para o enfrentamento dos crimes cibernéticos, tanto na esfera nacional quanto na esfera internacional, é vista como um dos grandes desafios, ressaltando a oportunidade que se vislumbra de negociação de uma convenção no âmbito das Nações Unidas, fato a ser estudado na segunda parte deste trabalho, quando do exame do papel de destaque do Escritório das Nações Unidas sobre Drogas e Crime.

Agora que já se tem um panorama sobre o quê são crimes cibernéticos e como são repreendidos e prevenidos no sistema penal brasileiro, passa-se para o exame de como são enfrentados na conjuntura regional e internacional, sob o viés da atuação das organizações que são os principais atores: COE, OCDE e agências e órgãos da Organização das Nações Unidas (AGNU, UNODC e UIT) motivo pelo qual se subdivide esta parte do texto em duas, uma concentrada do trabalho realizado no seio da ONU e a outra, destinada às demais organizações.

[239] BRASIL. Presidência da República, *Livro*, p. 39-40.

PARTE II: ENFRENTAMENTO DA CRIMINALIDADE CIBERNÉTICA NO ÂMBITO REGIONAL E INTERNACIONAL

A discussão sobre os crimes cibernéticos na esfera regional e internacional tem sido conduzida, essencialmente pelo Conselho da Europa, pela Organização para a Cooperação e Desenvolvimento Econômico e por agências e órgãos da ONU (Assembléia Geral, Escritório das Nações Unidas sobre Drogas e Crime e União Internacional de Telecomunicações), razão pela qual se abordará, inicialmente a atuação dos órgãos e agências integrantes do Sistema das Nações Unidas e posteriormente, de outras organizações, destacando-se o seu mandato e as atividades por elas desempenhadas.

A: ÂMBITO DO SISTEMA DAS NAÇÕES UNIDAS

A.1 Assembléia Geral das Nações Unidas (AGNU)

A Assembléia Geral das Nações Unidas (AGNU) é um dos principais órgãos das Nações Unidas pelo disposto no art. 7° da Carta das Nações Unidas, assinada em 26 de junho de 1945 em São Francisco, com vigência a partir de 24 de outubro do mesmo ano[240]. De acordo com o art. 9° da Carta, a Assembléia será composta de todos os Estados-Membros das Nações Unidas, com até cinco representantes e com direito a um voto (art. 18).

Quanto às funções e aos poderes, cabe destacar que o artigo 10 estabelece o mandato geral do órgão, atribuindo à Assembléia Geral a possibilidade de discutir quaisquer questões e assuntos relacionados ao escopo da Carta ou relativo aos poderes e funções de quaisquer órgãos previstos na Carta, assim como fazer recomendações sobre tais questões e assuntos aos Estados-Membros, Conselho de Segurança ou a ambos. Já no artigo 11 é salientado o papel do órgão quanto às questões relacionadas à manutenção da paz e segurança internacionais e no art. 13 está disposto que a Assembléia deve iniciar estudos e fazer recomendações com as seguintes finalidades: promoção da cooperação internacional no campo político e encorajamento do progressivo desenvolvimento do direito internacional e sua codificação;

[240] Texto completo da Carta das Nações Unidas disponível em: <http://www.un.org/en/documents/charter/chapter4.shtml>. Acesso em: 28/03/2011.

promoção da cooperação internacional nos campos econômico, social, cultural, educacional e de saúde, bem como apoiar a realização dos direitos humanos e das liberdades fundamentais para todos, sem distinção de raça, sexo, língua ou religião.

No tocante ao quórum de deliberação, por força do art. 18, "b", as questões simples (definidas por exclusão) são decididas pela maioria dos membros presentes e votantes e as questões importantes por maioria de 2/3 dos membros presentes e votantes, categoria que inclui, por exemplo, decisão sobre recomendações relacionadas à manutenção da paz e da segurança internacionais, eleição dos membros não permanentes do Conselho de Segurança, eleição dos membros do Conselho Econômico e Social, admissão de novo membro nas Nações Unidas etc.

A AGNU não ficou alheia à preocupação da utilização das TICs para o cometimento de crimes e o tema da segurança cibernética e, mais especificamente, dos crimes cibernéticos foi objeto de diversas resoluções, as quais assentam a posição de destaque do assunto na agenda diplomática internacional, reconhecem a gravidade do problema e a importância de combate a esta criminalidade e sustentam a necessidade imperativa de cooperação internacional para uma luta eficaz.

Dessa forma, após superficial descrição do órgão, busca-se descrever as Resoluções da Assembléia Geral que norteiam a atuação das Nações Unidas e dos Estados-Membros na matéria, notadamente as Resoluções n.° 53/70, 54/49, 55/28, 55/63, 56/19, 56/121, 57/53, 57/239, 58/32, 58/199, 59/61, 60/45, 61/54, 62/17, 63/37, 64/25, 64/211 e 65/41. Outras resoluções que tangenciam o tema serão abordadas quando, a seguir, do estudo da União Internacional de Telecomunicações e do Escritório das Nações Unidas sobre Drogas e Crime, tendo em vista a pertinência temática.

Inicia-se com a Resolução n.° 70, aprovada na 53° Sessão da Assembléia Geral das Nações Unidas, em 4 de dezembro de 1998, intitulada "Os avanços na Informação e nas Telecomunicações no Contexto da Segurança Internacional"[241]. A Resolução reconhece os benefícios dos avanços tecnológicos e científicos e sua necessidade de manutenção e encorajamento, assim como observa o considerável progresso que pode ser obtido com o desenvolvimento e a aplicação das últimas tecnologias e meios de telecomunicações. Além disso, destaca que os avanços inserem-se em um processo mais amplo de oportunidades positivas para o desenvolvimento da civilização, de oportunidades de cooperação para o bem

[241] Resolução n.° 53/70, "Os avanços na Informação e nas Telecomunicações no Contexto da Segurança Internacional", texto disponível em: <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N99/760/03/PDF/N9976003.pdf?OpenElement> . Acesso em 29/03/2011.

comum de todos os países, de aumento do potencial criativo da humanidade e de melhoria adicional na circulação de informações na comunidade global; constata ainda que a disseminação e o uso das tecnologias e meios de informação afetam os interesses de toda comunidade internacional; expressa preocupação com o fato de que estes meios e tecnologias possam ser potencialmente usados para finalidades que são inconsistentes com os objetivos de manutenção da estabilidade e segurança internacional e podem afetar adversamente a segurança dos países e considera necessário prevenir o abuso ou exploração dos recursos e tecnologias de informação para fins criminais e terroristas.

Assim sendo, solicita aos Estados-Membros a promoção em nível multilateral do exame das existentes e potenciais ameaças no âmbito da segurança da informação; convida aos Estados-Membros a informar o Secretário-Geral das suas opiniões e observações sobre as seguintes questões: (a) apreciação geral dos problemas de segurança da informação, (b) definição das noções básicas relacionadas à segurança da informação, incluindo interferência não autorizada ou abuso dos sistemas de informação e telecomunicações e dos recursos de informação e (c) conveniência de desenvolver princípios internacionais que aumentem a segurança global dos sistemas de informação e telecomunicações e ajudem na luta contra o terrorismo e a criminalidade na esfera da informação. Por fim, o documento roga ao Secretário-Geral para submeter um relatório à AGNU em sua 54° Sessão e decide incluir em sua agenda o tópico dos avanços na informação e nas telecomunicações no contexto da segurança internacional.

Em continuidade, na 54° Sessão o tema é retomado e é aprovada a Resolução n.° 49, em 1° de dezembro de 1999, com o mesmo título da resolução anterior[242], que repisa os apontamentos do documento anterior; observa a contribuição dos Estados-Membros que submeteram suas avaliações sobre as questões relacionadas à segurança da informação em atendimento aos parágrafos 1° e 3° da Resolução n.° 53/70, bem como o relatório do Secretário-Geral sobre tais avaliações e acolhe a oportuna iniciativa da Secretaria e do Instituto das Nações Unidas para a Pesquisa sobre o Desarmamento (UNIDIR) quanto à celebração de uma reunião internacional de *experts* em Genebra em Agosto de 1999 sobre os avanços na informatização e nas telecomunicações no contexto da segurança internacional.

Dessa forma, considerando que as avaliações dos Estados-Membros contidas no relatório do Secretário-Geral e que a supracitada reunião de *experts* contribuíram para um

[242] Resolução n.° 54/49, "Os Avanços na Informação e nas Telecomunicações no Contexto da Segurança Internacional", texto disponível em: <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N99/777/13 PDF/N9977713.pdf?OpenElement>. Acesso em: 29/03/2011.

melhor entendimento da substância das questões referentes à segurança da informação internacional, noções relacionadas e possíveis medidas para limitar as ameaças emergentes neste campo, a Assembléia Geral resolve ratificar a parte dispositiva da resolução anterior sobre o tema, no sentido de instar os Estados-Membros a continuar a discussão multilateral sobre o tópico e de convidá-los a continuar a remeter suas impressões sobre o assunto ao Secretário-Geral, destacando-se a manifestação sobre conveniência da elaboração de princípios internacionais que aumentem a segurança da informação e ajudem na luta contra os crimes e o terrorismo que dela se utilizam.

Para finalizar, solicita ao Secretário-Geral que submeta relatório na 55° Sessão e inclui na agenda provisória o item intitulado "Os Avanços na Informação e nas Telecomunicações no Contexto da Segurança Internacional".

Assim, o tema retorna a 55° Sessão, sendo canalizado na Resolução n.° 28, aprovada em 20 de novembro de 2000[243], a qual recorda as duas resoluções anteriores (Resoluções n.° 53/70 e 54/49) e toda sua fundamentação, ressaltando as contribuições dos Estados- Membros sobre a matéria, para instá-los a continuar considerando em nível multilateral a ameaças neste campo, assim como as possíveis medidas para limitar as ameaças no campo e para considerar que a finalidade destas medidas poderia ser atendida com o exame dos conceitos internacionais destinados a fortalecer a segurança da informação e dos sistemas de telecomunicações globais. Ademais, convida os Estados-Membros a continuar remetendo informações, suas opiniões sobre o tema, especialmente sobre a análise de conceitos internacionais que podem reforçar a segurança da informação, as quais devem ser apresentadas pelo Secretário-Geral, como já anteriormente contemplado nas resoluções anteriores, e inclui o tópico na agenda da próxima sessão.

Ainda na 55° Sessão tem-se a aprovação de uma das resoluções mais importantes para o tema, a Resolução n° 63, em 4 de dezembro de 2000, intitulada "Combatendo o Uso Criminoso das Tecnologias de Informação"[244]. A Resolução expressa a preocupação com o fato da evolução tecnológica ter criado novas possibilidades para a atividade delitiva, particularmente, com o uso criminoso das TICs; constata a necessidade de prevenção do uso criminoso das tecnologias da informação e que a confiança nestas resultou em aumento substancial da cooperação e coordenação global e o resultado do uso criminoso delas pode

[243] Resolução n.° 55/28, "Os Avanços na Informação e nas Telecomunicações no Contexto da Segurança Internacional", texto disponível em: <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N00/561/07/PDF/N0056107.pdf?OpenElement >. Acesso em: 29/03/2011.

[244] Resolução n.° 55/63, "Combatendo o Uso Criminoso das Tecnologias de Informação". Texto disponível em: <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N00/563/17/PDF/N0056317.pdf? OpenElement>. Acesso em: 25/03/2011.

causar grave impacto a todos os países; reconhece a necessidade de cooperação entre os países e o setor privado para combate do problema; salienta a necessidade de cooperação e coordenação entre os países no enfrentamento desta criminalidade, enfatizando o papel que pode ser assumido pelas Nações Unidas e pelas organizações regionais; e observa, dentre outros, o trabalho realizado pelo Conselho da Europa (que à época trabalhava na minuta da Convenção sobre Crimes Cibernéticos) e pelo G8.

Na parte dispositiva do documento, após destacar a apreciação pelos esforços anteriormente citados, constata o valor, *inter alia*, das seguintes medidas para o combate desta criminalidade: a) os países devem assegurar que sua legislação e práticas eliminem portos seguros para estes criminosos; b) a cooperação para investigação e persecução dos casos internacionais deve ser coordenada entre todos os países interessados; c) as informações relativas aos problemas no combate destes delitos deve ser compartilhadas pelos países; d) os recursos humanos dos órgãos de segurança pública devem receber treinamento e equipamentos para enfrentar esses crimes; e) os sistemas legais devem proteger a confidencialidade, integridade e disponibilidade dos dados e sistemas informáticos da ingerência não autorizada e assegurar que o abuso criminal seja penalizado; f) os sistemas legais devem permitir a preservação e o acesso rápido a dados eletrônicos pertencentes a determinadas investigações; g) regimes de assistência mútua devem garantir investigações e a coleta e troca de evidências tempestivas nesses casos; h) o público em geral deve ser sensibilizado da necessidade de prevenir e reprimir esses delitos; i) as tecnologias de informação, na medida do possível, devem ser projetadas para ajudar a prevenir e detectar a utilização criminosa, rastrear criminosos e coletar evidências e, j) a luta contra o uso criminoso dessas tecnologias exige o desenvolvimento de soluções que considerem a proteção das liberdades individuais e da privacidade, assim como a preservação da capacidade dos governos de combater sua utilização criminosa.

Além disso, convida os países a levar em consideração as medidas mencionadas acima nos seus esforços para combater o uso criminoso das tecnologias de informação e decide manter este assunto na agenda da sua Sessão 56°, realizada em 2001.

Assim, na 56° Sessão, tem-se a aprovação, como na sessão anterior, de duas resoluções envolvendo o assunto. A Resolução n.° 19, aprovada em 29 de novembro de 2001[245], limita-se a atualizar o texto anterior das resoluções sobre os avanços na informação e

[245] Resolução n.° 56/19, "Os Avanços na Informação e nas Telecomunicações no Contexto da Segurança Internacional", texto disponível em: <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N01/476/28/PDF/N0147628.pdf?OpenElement>. Acesso em: 29/03/2011.

nas telecomunicações no contexto da segurança internacional, sem grandes alterações substantivas, ressalvando-se que o texto inova ao solicitar ao Secretário-Geral a considerar as existentes e potenciais ameaças na esfera da segurança da informação e possíveis medidas de cooperação para combatê-las e a conduzir estudos sobre os conceitos internacionais destinados a fortalecer a segurança da informação e dos sistemas de telecomunicações globais, com a assistência de um grupo governamental de experts a ser formado em 2004, apontados pelo Secretário, respeitando a distribuição geográfica equitativa e com a ajuda dos Estados-Membros em posição de prestar o auxílio, devendo submeter o resultado na 60° Sessão, a ser realizada em 2005.

O segundo texto aprovado na 56° Sessão foi a Resolução n.° 121[246], que ratifica o embasamento da Resolução n.° 55/63, destacando-se agora a já existente Convenção sobre Crimes Cibernéticos do COE, e convida os Estados-Membros a considerar, se apropriado, o trabalho e os resultados da Comissão sobre Prevenção ao Crime e Justiça Criminal e de outras organizações regionais e internacionais, quando do desenvolvimento de legislação, política e práticas nacionais de combate ao uso criminoso das tecnologias da informação. Além disso, a Assembléia toma nota do valor das medidas consagradas na Resolução n.° 55/63 para reforçar o convite aos Estados-Membros a considerá-las nos seus esforços de combate ao uso criminoso destas tecnologias. Por fim, difere a análise do assunto na pendência do trabalho previsto no Plano de Ação Contra Crimes Informáticos e de Alta Tecnologia da Comissão sobre Prevenção ao Crime e Justiça Criminal.

Na 57° Sessão, realizada no ano de 2002, à semelhança das duas sessões anteriores de 2000 e 2001, foram aprovadas duas resoluções que são pertinentes ao estudo. A Resolução n.° 53[247]mantém novamente o assunto dos avanços da informação e das telecomunicações no contexto da segurança internacional em pauta, atualizando o texto anterior e assegurando a inclusão do tema na próxima sessão da Assembléia. Já com Resolução n.° 239, intitulada "Criação de uma Cultura Global de Segurança Cibernética"[248], tem-se novo marco no trabalho da AGNU ao mencionar, pela primeira vez em suas resoluções, o termo "segurança cibernética" e abordar o aspecto cultural do problema que afronta a segurança da informação.

---

[246] Resolução n.° 56/121, "Combatendo o Uso Criminoso das Tecnologias de Informação". Texto disponível em: <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N01/482/04/PDF/N0148204.pdf?OpenElement>. Acesso em: 29/03/2011.

[247] Resolução n.° 57/53, "Os Avanços na Informação e nas Telecomunicações no Contexto da Segurança Internacional", texto disponível em: <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N02/541/45/PDF/N0254145.pdf?OpenElement>. Acesso em: 02/04/2011.

[248] Resolução n.° 57/239, "Criação de uma Cultura Global de Segurança Cibernética", texto disponível em: <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N02/555/22/PDF/N0255522.pdf?OpenElement>. Acesso em 02/04/2011.

Nesta resolução, a Assembléia Geral constata a crescente dependência dos Governos, das empresas, de outras organizações e dos usuários individuais em relação às tecnologias de informação para a provisão de bens e serviços essenciais, para a condução dos negócios e para a troca de informações; reconhece a necessidade do aumento da segurança cibernética tendo em vista que os países aumentam sua participação na Sociedade da Informação; relembra todas as resoluções supracitadas; conscientiza-se que a efetiva segurança cibernética não é assunto limitado às práticas de governo e de ordem pública, mas deve ser alcançada através da prevenção e do suporte de toda sociedade e que a tecnologia por si só não assegura segurança cibernética, devendo ser priorizados o planejamento e a gestão de segurança cibernética por todas as sociedades e reconhece que governos, setor privado, outras organizações, usuários e proprietários individuais das tecnologias de informação, cada um em seu respectivo papel, devem estar cientes dos riscos de segurança e das medidas preventivas e devem assumir a responsabilidade por adotar as ações para aumentar a segurança das tecnologias de informação.

Outrossim, reconhece ainda que disparidades no acesso e no uso dessas tecnologias pelos países podem diminuir a efetivação da cooperação internacional no combate ao uso criminoso das mesmas e da criação de uma cultura global de segurança cibernética, apontando a necessidade de facilitação da transferência de tecnologia da informação, particularmente para países em desenvolvimento; reconhece a importância de cooperação internacional para alcançar segurança cibernética através do suporte dos esforços nacionais destinados ao reforço da capacidade humana, ao aumento das oportunidades de aprendizagem e de emprego, à melhoria dos serviços públicos e a melhoria da qualidade de vida por tirar proveito das avançadas, confiáveis e seguras redes e TICs e à promoção do acesso universal; constata que, em face do aumento da interconectividade, as redes e os sistemas informáticos estão agora mais expostos ao crescente número e maior variedade de ameaças e vulnerabilidades, as quais levantam novas questões de segurança para todos e observa ainda, o trabalho de relevantes organizações internacionais e regionais no aumento da segurança cibernética e na segurança das tecnologias da informação.

Dessa maneira, a Assembléia leva em considerações os elementos citados em seu anexo para a criação de uma cultura global de segurança cibernética; convida às relevantes organizações internacionais a considerar, dentre outros, os elementos citados no anexo em qualquer trabalho futuro sobre segurança cibernética; convida os Estados-Membros a considerar, dentre outros, os elementos citados no anexo nos seus esforços para desenvolver em suas sociedades a cultura de segurança cibernética na aplicação e no uso das tecnologias

de informação; convida os Estados-Membros e todas as relevantes organizações internacionais a levar em conta estes elementos, dentre outros e a necessidade de uma cultura global de segurança cibernética na sua preparação para a Cúpula Mundial sobre a Sociedade da Informação, a ser realizada em Genebra em 2003 e em Túnis em 2005 e salienta a necessidade de facilitar a transferência da tecnologia da informação e da capacitação para países em desenvolvimento, a fim de ajudá-los a adotar medidas em segurança cibernética.

No referido anexo, estão relacionados nove elementos para a criação de uma cultura de segurança cibernética, ressaltando que os rápidos avanços na tecnologia da informação mudaram a maneira como a segurança cibernética deve ser abordada pelos governos, setor privado, outras organizações e usuários individuais que desenvolvem, tem, fornecem, gerenciam, mantêm e usam as redes e os sistemas informáticos (chamados de participantes), sendo que tal cultura exigirá que todos participantes considerem os elementos complementares relacionados. Os nove elementos são: conscientização, responsabilidade, resposta, ética, democracia, avaliação do risco, implementação e desenho de segurança, gestão de segurança e reavaliação.

Nota-se que os nove elementos, ainda que a resolução não mencione expressamente o trabalho da OCDE, são exatamente os nove princípios constantes das Diretrizes da OCDE para a Segurança das Redes e Sistemas de Informação: em Direção à Cultura de Segurança, de 2002, as quais já existiam desde 1992, com a última atualização do documento em 2002, consoante relatado na parte do trabalho destinada à organização. A descrição dos elementos na resolução é uma versão resumida do conteúdo dos princípios das diretrizes.

Da mesma forma que nas anteriores, a 58° Sessão realizada em 2003 abrange novamente a temática dos avanços das TICs e segurança, garantindo sua inclusão na sessão a ser realizada em 2004[249] e dá continuidade à discussão sobre a criação de uma cultura de segurança cibernética, com a Resolução n.° 199, aprovada em 23 de dezembro de 2003[250], acrescendo a questão da proteção das Infraestruturas Críticas da Informação (ICI) [251].

---

[249] Resolução n.° 58/53, "Os Avanços na Informação e nas Telecomunicações no Contexto da Segurança Internacional", texto disponível em: <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N03/454/83/PDF/N0345483.pdf?OpenElement>. Acesso em: 02/04/2011.

[250] Resolução n.° 58/199, "Criação de uma Cultura Global de Segurança Cibernética e a Proteção de Infraestruturas Críticas de Informação", texto disponível em: <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N03/506/52/PDF/N0350652.pdf?OpenElement>. Acesso em 02/04/2011.

[251] Adota-se a seguinte definição de Infraestruturas Críticas de Informação: "As Infraestruturas Críticas da Informação (ICI) são assim definidas como o subconjunto de Ativos de Informação - meios de armazenamento, transmissão e processamento, sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso - que afetam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade". Definição da publicação: BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. *Guia de Referência para a*

Além de repisar os apontamentos anteriores sobre criação de uma cultura de segurança cibernética constante da Resolução n.° 57/239, com a edição da resolução, a AGNU reconhece a crescente interdependência das estruturas críticas de cada país (geração, transmissão e distribuição de energia, transporte aéreo e marítimo, serviços bancários e financeiros, comércio eletrônico, fornecimento de água, distribuição de alimentos e saúde pública) e as infraestruturas críticas de informação e como resultado da crescente interconectividade, as ICI estão expostas a maior variedade de ameaças e vulnerabilidades que aumentam e geram novas preocupações relacionadas à segurança.

Ademais, ressalta que sua proteção efetiva inclui, dentre outras medidas, a identificação das ameaças e a redução da sua vulnerabilidade, a minimização dos danos e do tempo de resposta em caso de ataque e a identificação da causa do dano ou fonte do ataque. No mesmo sentido, reconhece que essa proteção demanda comunicação e cooperação nacional e internacional entre todos os atores, sendo que os esforços nacionais devem ser apoiados por efetiva e substantiva cooperação regional e internacional.

Deste modo, a Assembléia reconhece que esforços para proteger as ICI devem ser empreendidos, levando em consideração as leis nacionais relativas à proteção da privacidade e legislação relevante; toma nota dos elementos relacionados no anexo à resolução para proteção destas infraestruturas; convida a todas as relevantes organizações internacionais, incluindo os órgãos das Nações Unidas, a considerarem, quando apropriado e dentre outras medidas, os referidos elementos em qualquer trabalho futuro sobre segurança cibernética ou proteção de infraestrutura crítica; convida aos Estados-Membros a considerarem esses elementos, dentre outros, em suas estratégias para redução dos riscos às ICI de acordo com suas leis e regulação nacionais; convida aos Estados-Membros e às relevantes organizações a considerarem esses elementos e a necessidade de proteção das ICI na sua preparação para a Segunda Fase da Cúpula Mundial para a Sociedade da Informação, a ser realizada em 2005; incentiva aos Estados-Membros e às relevantes organizações regionais e internacionais que, ao desenvolverem estratégias para lidar com segurança cibernética e com a proteção das ICI compartilhem suas melhores práticas e medidas, auxiliando outros Estados-Membros nos seus esforços para a obtenção de segurança cibernética e salienta a necessidade de esforços reforçados para acabar com o hiato digital, para proteger as ICI através da facilitação da transferência de tecnologia e capacitação, em particular, para os países em desenvolvimento, e

---

Segurança das Infraestruturas Críticas da Informação. Versão 1. Brasília: GSIPR/SE/DSIC, 2010. 151 p. p. 28. Disponível em: <http://dsic.planalto.gov.br/documentos/publicacoes/2_Guia_SICI.pdf>. Acesso em: 06/03/2011.

especialmente, para os países menos desenvolvidos, assim todos os países poderão beneficiar-se das TICs para seu desenvolvimento sócio-econômico.

Por fim, cabe mencionar os onze elementos para proteção das ICI constantes do anexo: existência de redes de alertas de emergência relacionadas às vulnerabilidades, ameaças e incidentes cibernéticos; conscientização para facilitar a compreensão dos atores da natureza e extensão das suas ICI e o papel que cada um deve desempenhar na sua proteção; exame das infraestruturas e identificação das interdependências entre elas, melhorando assim sua proteção; promoção de parcerias entre os atores, públicos e privados, para trocar e analisar ICI com o intuito de prevenir, investigar e responder aos danos ou ataques por elas sofridos; criação e manutenção de redes de comunicação para casos de crise e teste dos mesmos a fim de assegurar que a sua segurança e estabilidade em situações de emergência; garantia que as políticas de disponibilidade de dados considerem a necessidade de proteção das ICI; facilitação do rastreamento dos ataques às ICI e, quando apropriado, a divulgação da informação a outros países; condução de treinamento e exercício para aumento da capacidade de resposta e teste dos planos de continuidade e contingência em caso de ataque às ICI e incentivo aos atores a engajar-se em atividades similares; existência de leis materiais e processuais adequadas e pessoal treinado para possibilitar aos Estados investigar e processar os ataque às ICI e a coordenar tais investigações com outros países, quando apropriado; incentivo de cooperação internacional, quando apropriado, para proteger as ICI, incluindo o desenvolvimento e coordenação de sistemas de alerta de emergência, trocando e analisando informações concernente às vulnerabilidade, às ameaças e aos incidentes e coordenando investigações dos ataques de acordo com leis domésticas; e promoção de pesquisa, desenvolvimento e aplicação, em âmbito nacional e internacional, das tecnologias de segurança para atender aos padrões internacionais.

Todas as próximas sessões da Assembléia Geral continuarão a abordar o assunto. As 59° e 60° Sessões, realizadas em 2004 e 2005, respectivamente, mantém na pauta os avanços na informatização e nas telecomunicações no contexto da segurança internacional[252], sendo que Assembléia de 2004 nota com satisfação que o Secretário Geral está considerando as existentes e potenciais ameaças e possíveis medidas para enfrentar o problema e está conduzindo o grupo governamental de experts, em conformidade com a Resolução n.° 58/32,

[252] Resolução n.° 59/61, "Os Avanços na Informação e nas Telecomunicações no Contexto da Segurança Internacional", texto disponível em: <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N04/479/92/PDF/N0447992.pdf?OpenElement>. Acesso em: 02/04/2011; Resolução n.° 60/45, "Os Avanços na Informação e nas Telecomunicações no Contexto da Segurança Internacional", texto disponível em: <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N05/490/30/PDF/N0549030.pdf?OpenElement>. Acesso em: 02/04/2011.

sendo que a primeira previsão ao grupo consta da Resolução n.° 56/19. Em 2005, já com base no resultado do trabalho do grupo de *experts*, solicita ao Secretário-Geral, com o auxílio de um grupo governamental de experts a ser formado em 2009, a continuar a conduzir estudos sobre existentes e potenciais ameaças na esfera da segurança da informação e possíveis medidas de cooperação para combatê-las e sobre os conceitos internacionais destinados a fortalecer a segurança da informação e dos sistemas de telecomunicações globais, devendo apresentá-los na 65° Sessão, a ser realizada em 2010.

Em 2006, 2007 e 2008, a temática é mantida nas agendas das 61°, 62° e 63° Sessões, sem qualquer inovação substantiva no texto, apenas, sua atualização[253]. Em 2009 tem-se a edição de duas resoluções. A primeira continua a discussão dos avanços das TICs e a segurança internacional[254], fazendo referência à realização em novembro de 2009 da primeira reunião do grupo governamental de experts estabelecido pelo Secretário-Geral, em atendimento à Resolução n.° 63/37, já tendo sido previsto inicialmente na Resolução n.° 60/45.

O segundo documento, editado em 2009 com pertinência temática ao presente estudo é a Resolução n.° 64/211[255], que traz à pauta, novamente, o tópico da criação de uma cultura de segurança cibernética e da proteção das ICI. A Resolução relembra todas as resoluções que abordam o tópico das TICs e seus reflexos nas questões de segurança, bem como, os resultados das primeira e segunda fases da Cúpula Mundial sobre a Sociedade da Informação, destacando-se, dentre outros apontamentos, o reconhecimento que a confiança e a segurança no uso das TICs estão entre os principais pilares da Sociedade da Informação e que uma robusta cultura global de segurança cibernética necessita ser encorajada, promovida, desenvolvida e vigorosamente implementada; o reconhecimento da crescente contribuição dessas tecnologias para muitas funções essenciais da vida cotidiana, comércio e provisão de bens e serviços, pesquisa, inovação e empreendedorismo e para a livre circulação de

---

[253] Resolução n.° 61/54, "Os Avanços na Informação e nas Telecomunicações no Contexto da Segurança Internacional", texto disponível em: <http://daccess-dds-y.un.org/doc/UNDOC/GEN/N06/497/67/PDF/N0649767.pdf?OpenElement>. Acesso em: 02/04/2011; Resolução n.° 62/17, "Os Avanços na Informação e nas Telecomunicações no Contexto da Segurança Internacional", texto disponível em: <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N07/464/79/PDF/N0746479.pdf?OpenElement >. Acesso em: 02/04/2011; e Resolução n.° 63/37, "Os Avanços na Informação e nas Telecomunicações no Contexto da Segurança Internacional", texto disponível em: <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N08/473/01/PDF/N0847301.pdf?OpenElement >. Acesso em: 02/04/2011.

[254] Resolução n.° 64/25, "Os Avanços na Informação e nas Telecomunicações no Contexto da Segurança Internacional", texto disponível em: <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N09/463/33/PDF/N0946333. pdf?OpenElement>. Acesso em: 02/04/2011

[255] Resolução n.° 64/211, "Criação de uma Cultura Global de Segurança Cibernética e o Balanço dos Esforços Nacionais de Proteção de Infraestruturas Críticas de Informação", texto disponível em: <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N09/474/49/PDF/N0947449.pdf?OpenElement>. Acesso em 11/04/2011.

informação entre indivíduos e organizações, governos, empresas e sociedade civil; o reconhecimento, ainda que de acordo com seus papéis, governos, empresas, organizações e proprietários e usuários das TICs devem assumir sua responsabilidade e adotar medidas para aumentar a segurança dessas tecnologias.

Ademais, afirma que a segurança da ICI é uma responsabilidade que poder público deve tratar de forma sistêmica, liderando nacionalmente na área, em coordenação com os principais atores, os quais devem estar conscientes dos riscos relevantes, medidas preventivas e respostas efetivas de acordo com seus respectivos papéis; reconhece que os esforços nacionais devem ser apoiados pela troca de informação e colaboração internacionais, no intuito de combater a crescente natureza transnacional das ameaças; considera o relevante trabalho das organizações regionais e internacionais no aumento da segurança cibernética, reiterando seu papel no encorajamento dos esforços nacionais e na promoção da cooperação internacional e ainda salienta o trabalho da União Internacional de Telecomunicações, consubstanciado no relatório sobre segurança das redes de informação e comunicação e melhores práticas para o desenvolvimento de uma cultura de segurança cibernética.

Dessa forma, a AGNU convida os Estados-Membros a usar, se e quando apropriado, a ferramenta de autoavaliação dos esforços nacionais para proteção das ICI, constante do anexo à resolução e encoraja os Estados-Membros e relevantes organizações regionais e internacionais que, ao desenvolveram estratégias para lidar com a segurança cibernética e proteção das ICI, compartilhem suas melhores práticas e medidas que podem auxiliar outros Estados-Membros em seus esforços de alcançar segurança cibernética através do fornecimento das informações ao Secretário-Geral para compilação e disseminação entre os mesmos.

No anexo que trata da ferramenta voluntária de autoavaliação dos esforços nacionais de proteção das ICI, estão abarcados dezoito itens relacionados ao balanço das necessidades e estratégias em matéria de segurança cibernética; funções e responsabilidades dos atores; processos políticos e participação; cooperação entre os setores público e privado; gestão de incidentes e recuperação; arcabouço legal; e desenvolvimento de uma cultura global de segurança cibernética.

No tocante ao marco legal, a ferramenta de avaliação apresenta cinco pontos. Aponta a revisão e atualização da legislação (incluindo a relacionada aos crimes cibernéticos, à privacidade, à proteção de dados, às leis comerciais, à assinatura digital e à criptografia) que pode estar desatualizada ou obsoleta como resultado da rápida incorporação e dependência das novas TICs e a utilização das convenções regionais e internacionais, acordos e

precedentes nestas revisões, verificando assim se o país desenvolveu a legislação necessária para a investigação e persecução dos crimes cibernéticos, salientando os marcos existentes, por exemplo, as Resoluções da AGNU n.° 55/63 e 56/121 que tratam da combate ao uso criminosos destas tecnologias e iniciativas regionais, incluindo, a Convenção do Conselho da Europa sobre Crimes Cibernéticos.

Igualmente, indica a determinação do status atual das autoridades e procedimentos nacionais no tocante aos crimes cibernéticos, incluindo a autoridades legais e unidades nacionais de combate aos crimes cibernéticos, bem como o nível de compreensão das questões dessa criminalidade entre membros do Ministério Público, juízes e legisladores; a avaliação da adequação dos códigos penais atuais e das autoridades para o enfrentamento dos atuais e futuros desafios dos delitos cibernéticos e do espaço cibernético, em geral; o exame da participação nacional nos esforços internacionais para combater estas infrações penais, como a Rede 24/7 de Pontos de Contato sobre Crimes Cibernéticos e a determinação dos requisitos para os órgãos nacionais de segurança pública cooperarem com órgãos homólogos internacionais com a finalidade de investigar crimes cibernéticos transnacionais nos casos em que a infraestrutura está situada ou o criminoso reside dentro do território nacional e as vítimas residem em outro lugar.

Por fim, no ano de 2010, a AGNU manteve em sua agenda a discussão sobre os avanços das TICs e segurança[256], repisando e atualizando o texto anterior, garantindo a inclusão do tema na próxima sessão da Assembléia, em 2011, solicitando ao Secretário-Geral, com o auxílio de um grupo governamental de experts a ser formado em 2012 a levar em consideração as avaliações e as recomendações constantes do relatório do grupo de experts estabelecido em 2009, a continuar conduzindo estudos sobre existentes e potenciais ameaças na esfera da segurança da informação e possíveis medidas de cooperação para combatê-las e sobre os conceitos internacionais destinados a fortalecer a segurança da informação e dos sistemas de telecomunicações globais, devendo apresentá-los na 68° Sessão, a ser realizada em 2013.

Percebe-se pelo exposto que, desde 1998, as repercussões da evolução tecnológica e da massiva utilização das TICs na segurança têm sido uma constante na pauta do principal órgão deliberativo das Nações Unidas, fato que reflete sua importância e emergência e a necessidade de que seja abordado pela comunidade internacional, visto que as ameaças,

[256] Resolução n.° 65/41, "Os Avanços na Informação e nas Telecomunicações no Contexto da Segurança Internacional", texto disponível em: <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N10/515/00/PDF/N1051500.pdf?OpenElement>. Acesso em: 11/04/2011.

incidentes e crimes cibernéticos são essencialmente transnacionais. Também resta assentado que a discussão sobre uma luta efetiva contra essa nova categoria criminal é eminentemente interdisciplinar, envolvendo assim a problemática da cultura de segurança cibernética e da proteção das ICI.

Além da AGNU, outras agências e órgãos do Sistema das Nações Unidas também têm direcionado esforços para o enfrentamento do problema, especialmente, a União Internacional de Telecomunicações e o Escritório das Nações Unidas sobre Drogas e Crime, cujas atribuições e iniciativas continuam a ser descritas a seguir.

A.2 União Internacional de Telecomunicações (UIT)

Antes de descrever as ações da União Internacional de Telecomunicações (UIT) no tocante aos crimes cibernéticos, faz-se necessário descrever a organização, visto que não é uma das organizações internacionais mais familiares aos operadores do Direito. Além disso, também se impõe explicar como a temática foi atribuída à UIT, para que se possa, então, apreciar suas atividades específicas na matéria.

A UIT é a Agência Especializada das Nações Unidas para assuntos ligados às TICs, cobrindo uma diversa e extensa pauta de atribuições que inclui desde a coordenação e divisão do espectro radioelétrico até a interconectividade das redes de telecomunicações, passando pela normalização de padrões técnicos e regulatórios, inclusive com foco no atendimento dos desafios da sociedade contemporânea, por exemplo, a segurança no uso dessas tecnologias.

As atividades desenvolvidas cotidianamente por indivíduos em qualquer um dos continentes envolvem, necessariamente, o trabalho realizado pela UIT ou nela construído. O programa de rádio que se escuta no deslocamento para o trabalho, a novela assistida no final do dia, as mensagens eletrônicas trocadas no exercício da atividade profissional e as ligações efetuadas para familiares, bem como todos os equipamentos e tecnologias envolvidos na prestação e/ou operação desses serviços, abarcam, em maior ou menor grau, as competências da UIT.

A UIT é regida, essencialmente, pela sua Constituição e Convenção, e o seu preâmbulo consagra um dos seus fundamentos balizadores de toda sua atuação, que justamente o fato de que as telecomunicações servem como alavanca para o desenvolvimento econômico e social dos países. Reza o preâmbulo:

> Embora reconhecendo plenamente o direito de cada Estado Soberano para regular suas telecomunicações, e considerando a crescente importância das telecomunicações para a preservação da paz e para desenvolvimento socioeconômico de todos os Estados, os Estados Partes dessa Constituição, como instrumento básico da União Internacional de Telecomunicações, e da Convenção da União Internacional de Telecomunicações (adiante designada referida como "Convenção"), que a complementa, com o objetivo de facilitar as relações pacíficas, a cooperação internacional entre os povos e o desenvolvimento socioeconômico por meio de serviços de telecomunicações eficientes, acordaram o seguinte:[257]

A UIT é uma organização intergovernamental[258] e conta, atualmente, com 191 Estados-Membros e mais de 700 Membros de Setores e Associados, ressaltando que além dos países, o setor privado também tem assento na entidade, assim como entidades regionais e internacionais de telecomunicações, de fomento e de pesquisa e desenvolvimento de TICs e outras instituições que tratem de assuntos relacionados às TICs[259]. É justamente a composição heterogênea dessa Agência que a diferencia, nos termos das suas próprias publicações, que assim sustentam[260]:

> **La UIT es única** entre las organizaciones internacionales, ya que sus miembros son gobiernos y empresas del sector privado. Estas últimas pueden adherirse a la UIT como Miembros de Sector o Asociados. Son miembros de la UIT poderes públicos y organismos reguladores, operadores de redes, fabricantes de equipos, creadores de equipos y programas informáticos, organizaciones regionales de normalización e instituciones financieras. La UIT es pues el lugar de encuentro mundial de los sectores de las TIC y las telecomunicaciones.

---

[257] "*While fully recognizing the sovereign right of each State to regulate its telecommunications and having regard to the growing importance of telecommunication for the preservation of peace and the economic and social development of all States, the States Parties to this Constitution, as the basic instrument of the International Telecommunication Union, and to the Convention of the International Telecommunication Union (herein after referred to as "the Convention") which complements it, with the object of facilitating peaceful relations, international cooperation among peoples and economic and social development by means of efficient telecommunication services, have agreed as follows*:". Texto original disponível em: <http://www.itu.int/net/about/basic-texts/constitution/preamble.aspx>. Acesso em: 18/01/2010 (Tradução nossa).

[258] Consoante *caput* do Art. 2 "*The International Telecommunication Union is an intergovernmental organization in which Member States and Sector Members, having well-defined rights and obligations, cooperate for the fulfilment of the purposes of the Union. It shall, having regard to the principle of universality and the desirability of universal participation in the Union, be composed of: [...].*

[259] UNIÓN INTERNACIONAL DE TELECOMUNICACIONES. *UIT. Miembros*. Genebra: UIT, 2008. 36 p. 6 e 27. Disponível em: <http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-MEMB-2008-PDF-S.pdf.>. Acesso em: 18/01/2010.

[260] UNIÓN INTERNACIONAL DE TELECOMUNICACIONES. *UIT*, *Op. Cit.*, p. 8.

A UIT foi fundada em Paris em 1865, então denominada de União Internacional do Telégrafo, sendo que o nome atual, União Internacional de Telecomunicações, foi adotado em 1934 e, em 1947, a UIT tornou-se uma agência especializada das Nações Unidas[261].

Os seus objetivos e atribuições estão insculpidos nos art. 1°, §§ 1° e 2°, respectivamente, da Constituição, dispondo da seguinte forma:

> Art. 1° Objetivos da União:
> 1. Os objetivos da União são:
> a) manter e alargar a cooperação internacional entre todos os seus Estados-Membros para a melhoria e uso racional de todos os tipos de telecomunicações;
> a bis) promover e aumentar a participação das entidades e organizações nas atividades da União e fomentar proveitosa cooperação e parceria entre elas e os Estados-Membros para o cumprimento dos objetivos gerais consagrados no âmbito da União;
> b) promover e oferecer assistência técnica aos países em desenvolvimento no campo das telecomunicações e também promover a mobilização dos recursos materiais, humanos e financeiros necessários à sua execução, bem como o acesso à informação;
> c) promover o desenvolvimento dos meios técnicos e a sua operação mais eficiente, com vista a melhorar a eficiência dos serviços de telecomunicações, aumentando a sua utilidade e fazê-los, na medida do possível, amplamente disponíveis ao público;
> d) promover a extensão dos benefícios das novas tecnologias de telecomunicações a todos os habitantes do mundo;
> e) promover a utilização de serviços de telecomunicações com o objetivo de facilitar relações pacíficas;
> f) harmonizar as ações dos Estados-Membros e promover cooperação frutífera e construtiva e parceria entre os Estados-Membros e Membros do Setor da realização desses fins;
> g) promover, a nível internacional, a adoção de uma abordagem mais ampla para as questões das telecomunicações na economia e na sociedade global da informação, através da cooperação com outras organizações intergovernamentais internacionais e regionais e com organizações não-governamentais relacionadas às telecomunicações.
> 2. Para o alcance desses fins, a União deve, particularmente:
> a) efetuar a alocação das bandas do espectro de radiofrequência, a atribuição de frequências de rádio e de registro de radiofrequência atribuídas, e, para os serviços espaciais, de qualquer posição orbitral associada à órbita de satélites geoestacionários ou de quaisquer características associadas de satélites de outras órbitas, a fim de evitar interferências prejudiciais entre as estações de rádio de diferentes países;
> b) coordenar os esforços para eliminar as interferências prejudiciais entre as estações de rádio de diferentes países e para melhorar a utilização do espectro de radiofrequências para serviços de radiocomunicações e de satélites geoestacionários e outros satélites órbitrais;
> c) Facilitar a padronização mundial das telecomunicações, com uma qualidade satisfatória de serviço;

[261] UNIÓN INTERNACIONAL DE TELECOMUNICACIONES. *UIT – La Visión: Ayudamos al Mundo a Comunicarse*. Genebra: UIT, 2007. 20 p. 4. Disponível em: <http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-HLPW-2007-PDF-S.pdf>. Acesso em: 18/01/2010.

> d) promover a cooperação e a solidariedade internacionais na prestação de assistência técnica aos países em desenvolvimento e a criação, desenvolvimento e melhoria de equipamentos de telecomunicações e redes eM países em desenvolvimento por todos os meios ao seu dispor, inclusive através da sua participação nos programas pertinentes das Nações Unidas e da utilização de seus recursos próprios, conforme o caso;
> e) coordenar os esforços para harmonizar o desenvolvimento de instalações de telecomunicações, especialmente daquelas utilizando técnicas espaciais, com vista a aproveitar ao máximo as suas possibilidades;
> f) fomentar a colaboração entre os Estados-Membros e Membros do Setor com vista à criação de tarifas em níveis tão baixos quanto possíveis, consistente com um serviço eficiente e levando em conta a necessidade de manutenção de administração financeira independente de telecomunicações em uma base sólida;
> g) promover a adoção de medidas para garantir a segurança da vida através da cooperação dos serviços de telecomunicações;
> h) realizar estudos, regular, aprovar resoluções, formular recomendações e opiniões, coletar e publicar informações relativas a assuntos de telecomunicações;
> i) promover, com organismos financeiros internacionais e de desenvolvimento, o estabelecimento de linhas preferenciais e favoráveis de crédito a ser utilizada para o desenvolvimento de projetos sociais que visem a expandir serviços de telecomunicações para as zonas mais isoladas nos países.
> j) promover a participação das entidades envolvidas nas atividades da União e cooperação com organizações regionais e outras para o cumprimento dos objetivos da União.[262]

O Brasil é um dos Países-Membros da União e os atos finais da Conferência Adicional dos Plenipotenciários de 1992 (Genebra) e da Conferência de Plenipotenciários de 1994 (Quioto) foram aprovados pelo Congresso Nacional, por meio do Decreto Legislativo n° 67, de 1998, sendo a Constituição e a Convenção da UIT promulgadas pelo Decreto n° 2.962, de 23 de fevereiro de 1999. Os atos finais das Conferências de 1998 (Minneapolis) e 2002 (Marraqueche) foram aprovados pelos Decretos Legislativos n.° 34, de 2002, e n.° 987, de 2009, respectivamente, restando pendentes de aprovação os atos finais das Conferências de 2006 (Antalya) e 2010 (Guadalajara).

A Estrutura da União é estabelecida pelo art. 7° da Constituição e compreende a Conferência de Plenipotenciários, órgão supremo da União; o Conselho, que age em nome da Conferência dos Plenipotenciários; Conferências Mundiais de Telecomunicações; o Setor de Radiocomunicação (UIT-R); o Setor de Normalização das Telecomunicações (UIT-T); o Setor de Desenvolvimento das Telecomunicações (UIT-D) e a Secretaria-Geral. O organograma é fruto da reorganização institucional da Agência, ocorrida em 1992, decorrente da Conferência Adicional dos Plenipotenciários, realizada em Genebra, na Suíça, com

[262] Tradução nossa.

vigência a partir de 1° de julho de 1994, quando foram aprovadas a Constituição e a Convenção da UIT, alteradas, posteriormente, pelas Conferências dos Plenipotenciários de 1994, 1998, 2002, 2006 e 2010.

Nos termos do art. 8°, a Conferência dos Plenipotenciários deve ser composta pelas delegações representando os Estados-Membros e deve ser realizada a cada quatro anos. Existe a possibilidade de edição excepcional e extraordinária da Conferência, no intervalo entre duas conferências ordinárias, para o tratamento de questões específicas, conforme art. 8°, §3°, da Constituição. O art. 9°, §1°, obriga a Conferência dos Plenipotenciários a observar, em quaisquer eleições, a distribuição equânime de vagas por todas as regiões, sendo que o Secretário-Geral, seu vice e os diretores dos *bureaus* dos setores (UIT-R, UIT-T, UIT-D) são eleitos entre os candidatos nacionais propostos pelos Estados-Membros, também garantindo distribuição geográfica equânime das vagas por todas as regiões do mundo, consoante art. 9°, § 2°.

O Conselho da UIT será composto pelos Estados-Membros eleitos pela Conferência dos Plenipotenciários e deve atuar como o órgão que governa a União nos intervalos entre as Conferências, em nome dela agindo, dentro dos limites dos poderes por ela delegados[263]. A Secretaria-Geral da União será dirigida pelo Secretário-Geral, representante legal da União[264].

A UIT-R, em síntese, possui duas grandes funções: a) de assegurar o uso do espectro de radiofrequência pelos serviços de radiocomunicações de forma racional, equitativa, eficiente e econômica, inclusive dos serviços que utilizam satélites geoestacionários ou outros satélites orbitrais e b) de realizar estudos sem limite de alcance de frequência e de adotar recomendações em matéria de radiocomunicações[265].

Em paralelo, a UIT-T é responsável por atender as finalidades da Agência no tocante à normalização das telecomunicações, por meio do estudo de questões técnicas, de operação e de tarifação e da adoção de recomendações sobre elas, no intuito de normalização das telecomunicações em nível mundial [266].

Ainda que a UIT-R e a UIT-T, assim como a UIT como um todo, devam considerar as necessidades particulares dos países em desenvolvimento na execução das suas atribuições, é justamente na UIT-D que essa preocupação se solidifica, pois toda sua atuação tem, por principais destinatários, os países em desenvolvimento, classificação que abarca os países menos desenvolvidos, as economias em transição e os pequenos países insulares. Dentro de

[263] Art.10, 1, "1)", e 3 da Constituição da UIT.
[264] Art.11, 1 "1)" da Constituição da UIT.
[265] Art.12 da Constituição da UIT.
[266] Art.17, 1 "1)" da Constituição da UIT.

suas atribuições, destaca-se: sensibilizar os tomadores de decisões sobre o papel das telecomunicações na economia nacional e no programa social de desenvolvimento, fornecendo informações e aconselhando sobre opções estruturais e de políticas a serem desenvolvidas; promover parcerias para o desenvolvimento, expansão e operação de redes e serviços de telecomunicações, particularmente nos países em desenvolvimento; aumentar o crescimento das telecomunicações através da cooperação com organizações regionais e globais; encorajar a participação da indústria no desenvolvimento dos países em desenvolvimento; ativar a mobilização de recursos para fornecer assistência da área de telecomunicações para os países em desenvolvimento; promover e coordenar programas de transferência de tecnologia para países em desenvolvimento à luz das mudanças e do desenvolvimento das redes dos países desenvolvidos; realizar ou financiar estudos sobre aspectos técnicos, econômicos, financeiros, gerenciais, regulatórios e de políticas no campo das telecomunicações[267].

Além disso, a atividade da UIT-D também é marcada pelo fato da UIT, como agência especializada das Nações Unidas e agência de execução, de implementação de projetos no seio do Sistema de Desenvolvimento das Nações Unidas ou de outros fundos, ser responsável por facilitar e aumentar o desenvolvimento das telecomunicações por meio da oferta, organização e coordenação técnica de atividades de cooperação e assistência[268].

O rol de competências da UIT, dentro das especificidades de cada um dos seus órgãos, demonstra a ampla gama de atribuições desta entidade, com sede em Genebra, na Suíça, contando atualmente com mais de 700 funcionários[269] para viabilizar o desempenho das suas funções. No exercício de 2008, seu orçamento foi de 169,1 milhões de francos suíços[270], dos quais 81% decorrem das contribuições dos seus membros, sendo 69%, especificamente, da contribuição dos Estados-Membros[271].

Após esse breve resumo sobre a UIT, passa-se à análise dos resultados da Cúpula Mundial sobre a Sociedade da Informação e seus reflexos na UIT.

---

[267] As atribuições estão relacionadas no art. 21, § 2°, 2, a-i, da Constituição da UIT.
[268] Artigo 21, §1,1 da Constituição da UIT.
[269] Informação referente a 1° de janeiro de 2009, disponível no sítio oficial da entidade, podendo ser visualizada na página: <http://www.itu.int/employment/index.html>. Acesso em 18/01/2010.
[270] Equivalente a 157,5 milhões de dólares utilizando-se a cotação das duas moedas no fechamento do exercício de 2008 (31/12/2008), fornecida pelo Banco Central do Brasil, disponível em: <http://www4.bcb.gov.br /pec/conversao /Resultado.asp?idpai=convmoeda >. Acesso em: 24/01/2010.
[271] UNIÓN INTERNACIONAL DE TELECOMUNICACIONES. *UIT, Informe Anual de la Unión, 2008.* Genebra: UIT, 2009. 88 p. 12. Disponível em: <http://www.itu.int/publ/S-CONF-AREP-2008/en>. Acesso em: 18/01 /2010.

Conforme descrito anteriormente, a UIT existe há mais de 140 anos e desde sua fundação tratou de temas relacionados às telecomunicações, remontando àquela época ao telégrafo, com a preponderância para questões de ordem técnica, notadamente interconexão, coordenação do espectro de radiofrequência e normalização.

O ano de 1989 marca o início da preocupação dessa Agência para com o desenvolvimento, visto que a Conferência dos Plenipotenciários, realizada em Nice, agregou, às competências da UIT, a assistência técnica aos países em desenvolvimento, criando o *Bureau* de Desenvolvimento das Telecomunicações (BDT). A necessidade de alavancar o desenvolvimento, aliada ao fenômeno da globalização e à liberalização do mercado das telecomunicações, até então, uma atividade essencialmente estatizada, culminou na reorganização institucional, promovida pela Conferência Adicional dos Plenipotenciários de 1992[272].

O advento da era da Sociedade da Informação provocou nova ampliação do seu escopo de atuação, fazendo com que a UIT, por exemplo, seja uma referência no combate à criminalidade cibernética, conforme se verá a seguir.

A Conferência dos Plenipotenciários da União Internacional de Telecomunicações, realizada em Minneápolis, nos Estados Unidos, em 1998, é o marco histórico para a realização da Cúpula Mundial sobre a Sociedade da Informação (CMSI), uma vez que nela foi aprovada a Resolução n°73[273], que instruiu o Secretário-Geral da UIT a colocar a questão da possibilidade de realização dessa Cúpula na Agenda do Comitê Administrativo de Coordenação das Nações Unidas, destacando a sua consciência no tocante: (a) ao fato de que a globalização das telecomunicações deve ter em conta uma evolução harmoniosa de políticas, regulamentação, redes e serviços em todos os Estados-Membros e (b) ao surgimento do conceito de sociedade da informação, no qual as telecomunicações desempenham um papel-chave.

Vislumbrando essa decisão no âmbito da UIT como alavanca para o debate sobre a Sociedade da Informação, faz-se necessária uma explicação sobre qual conjuntura essa nomenclatura busca retratar. Para tanto, utiliza-se a definição adotada pelo Programa da Sociedade da Informação, que assim a descreve[274]:

> Representa uma profunda mudança na organização da sociedade e da economia, havendo quem a considere um ***novo paradigma técnico-***

[272] Nesse sentido ver histórico da UIT disponível em:<http://www.itu.int/net/about/history.aspx>. Acesso em: 18/01/2010.
[273] Texto completo da Resolução disponível em: <http://www.itu.int/wsis/docs/background/resolutions/73_.html>. Acesso em: 10/10/2010.
[274] BRASIL. Ministério da Ciência e Tecnologia, *Sociedade,* p. 5.

> ***econômico***. É um ***fenômeno global,*** com elevado potencial transformador das atividades sociais e econômicas, uma vez que a estrutura e a dinâmica dessas atividades inevitavelmente serão, em alguma medida, afetadas pela infra-estrutura de informações disponível. É também acentuada sua ***dimensão político-econômica***, decorrente da contribuição da infra-estrutura de informações para que as regiões sejam mais ou menos atraentes em relação aos negócios e empreendimentos.
> Sua importância assemelha-se à de uma boa estrada de rodagem para o sucesso econômico das localidades. Tem ainda marcante ***dimensão social***, em virtude do seu elevado potencial de promover a integração, ao reduzir as distâncias entre pessoas e aumentar o seu nível de informação.

Continuando a breve exposição dos antecedentes históricos, ressalta-se que o Conselho da UIT, com a aprovação da Resolução n° 1.158/2000[275], instrui o Secretário-Geral da Agência a coordenar, juntamente com outras organizações internacionais, a realização da Cúpula para o ano de 2003. Dando continuidade às atividades de preparação da conferência, o Conselho aprovou a Resolução n° 1.179/2001[276], endossando a proposta do Secretário-Geral da UIT sobre a organização da Cúpula em duas fases, acolhendo o oferecimento da Suíça e da Tunísia para sediar a primeira e a segunda fases, respectivamente, nos anos de 2003 e 2005. Dessa maneira, a CMSI começou a tomar forma e foi sedimentada pela Resolução n.° 183, aprovada na 56ª Sessão da Assembléia Geral das Nações Unidas (AGNU)[277], em 21 de dezembro de 2001, ratificando a decisão tomada pelo Conselho da UIT e convidando essa Agência a assumir a liderança gerencial na Secretaria da Cúpula e no seu processo preparatório.

Na sequência dos trabalhos preparatórios, a Resolução n° 238, da 57ª Sessão da AGNU[278], de 20 de dezembro de 2002, encoraja o engajamento do setor privado e de entidades não governamentais nesse processo, convidando os países a enviar representantes políticos do alto escalão para a Conferência.

Dessa forma, de 10 a 12 de dezembro de 2003, ocorreu a primeira fase da Cúpula, em Genebra, na Suíça. Reuniram-se cerca de cinquenta Chefes de Estado ou de Governo e Vice-Presidentes e mais de onze mil delegados, participando nas mais de trezentas atividades

---

[275] Texto completo da Resolução disponível em <http://www.itu.int//wsis/docs/background/resolutions/1158.html>. Acesso em: 10/10/2009.
[276] Texto completo da Resolução disponível em <http://www.itu.int/wsis/docs/background/resolutions/1179.html>. Acesso em: 10/10/2009.
[277] Texto completo da Resolução disponível em <http://www.itu.int/wsis/docs/background/resolutions/56_183_unga_2002.pdf >. Acesso em: 20/10/2009.
[278] Texto completo da Resolução disponível em <http://www.itu.int/wsis/docs/background/resolutions/57-238.pdf>. Acesso em: 10/10/2009.

relacionadas à Cúpula em Genebra, organizadas por diversas agências que compõem o Sistema das Nações Unidas e por outras organizações regionais e internacionais[279].

Como resultados dessa primeira fase têm-se a Declaração de Princípios de Genebra e o Plano de Ação de Genebra. A Declaração inicia com a descrição da visão comum sobre a Sociedade da Informação (SI) pelos representantes de todos os povos reunidos por ocasião da CMSI, salientando o desejo e comprometimento na SI, baseada nas seguintes premissas:

> [...] construir una Sociedad de la Información centrada en la persona, integradora y orientada al desarrollo, en que todos puedan crear, consultar, utilizar y compartir la información y el conocimiento, para que las personas, las comunidades y los pueblos puedan emplear plenamente sus posibilidades en la promoción de su desarrollo sostenible y en la mejora de su calidad de vida, sobre la base de los propósitos y principios de la *Carta de las Naciones Unidas* y respetando plenamente y defendiendo la *Declaración Universal de Derechos Humanos*[280].

Outrossim, a Declaração também destaca o desafio de canalizar as TICs para promover os objetivos de desenvolvimento da Declaração do Milênio, observando-se a questão da sustentabilidade pregada pela Declaração e Plano de Ação de Johannesburgo, pelo Consenso de Monterrey e pelos resultados de outras Cúpulas pertinentes das Nações Unidas. Repisa-se como fundamento essencial da SI, a liberdade de opinião e expressão de todos os indivíduos, sendo a comunicação um processo social fundamental, uma necessidade humana básica e o fundamento de toda organização social, constituindo o seu alicerce central. A Declaração reforça o direito de todos de participarem da SI e que ninguém pode ficar excluído dos benefícios que oferece[281]. Cumpre referir que o documento faz expressa menção sobre a desigual distribuição das vantagens decorrentes da revolução tecnológica da informação, e contempla o comprometimento de conversão do hiato digital numa oportunidade digital para todos[282].

Como base da SI, foram elencados os seguintes princípios[283]: colaboração dos governos e das partes interessadas para promoção das TICs para o desenvolvimento; ampliação da infraestrutura; acesso à informação e ao conhecimento; fomento da capacitação; reforço da confiança e da segurança na utilização das TICs; criação de um ambiente propício

---

[279] INTERNATIONAL TELECOMMUNICATION UNION. *ITU Building the Information Society.* Genebra: UIT, 2007. 44 p. 11. Disponível em: <http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-BIS-2007-PDF-E.pdf>. Acesso em: 07/10/2009.

[280] UNIÓN INTERNACIONAL DE TELECOMUNICACIONES. *CMSI: Documentos Finales*. Genebra: UIT, 2006. 102p. 11. Disponível em: <*http://www.itu.int/wsis /outcome/booklet-es.pdf*>. Acesso em: 10/10/2009.

[281] Parágrafos 2° e 4° da Declaração de Princípios de Genebra, cujo texto integral pode ser visualizado em: <http://www.itu. int/wsis/docs/geneva/official/dop-es.html >. Acesso em: 18/01/2010.

[282] Parágrafo 10 da Declaração.

[283] Parágrafo 19 e seguintes da Declaração.

em todos os níveis para a SI; desenvolver e ampliar a utilização das TICs; promoção e respeito à diversidade cultural; reconhecimento do papel dos meios de comunicação; abordagem das dimensões éticas da SI e incentivo à cooperação internacional e regional.

Como consequência prática, a 1ª Fase da CMSI gerou o Plano de Ação de Genebra[284], que traduz a visão de SI e os seus princípios em linhas de ação concreta, cada uma correspondendo a cada um dos onze princípios, nas quais são listados diversos objetivos e metas para alcançar o desenvolvimento que foi acordado na Declaração de Princípios, assim como na Declaração do Milênio e diversos outros instrumentos internacionais.

Cabe transcrever a Linha de Ação C.5, que trata justamente da efetivação do Princípio de Criação da Confiança e da Segurança na Utilização das TICs, sendo que o § 12. b) grifado abaixo trata do enfrentamento do problema da criminalidade cibernética nos seguintes termos:

> C5. Creación de confianza y seguridad en la utilización de las TIC
> *12.* La confianza y la seguridad son unos de los pilares más importantes de la Sociedad de la Información.
> *a)* Propiciar la cooperación entre los gobiernos dentro de las Naciones Unidas, y con todas las partes interesadas en otros foros apropiados, para aumentar la confianza del usuario y proteger los datos y la integridad de la red; considerar los riesgos actuales y potenciales para las TIC, y abordar otras cuestiones de seguridad de la información y de las redes.
> ***b)* Los gobiernos, en cooperación con el sector privado, deben prevenir, detectar, y responder a la ciberdelincuencia y el uso indebido de las TIC, definiendo directrices que tengan en cuenta los esfuerzos existentes en estos ámbitos; estudiando una legislación que permita investigar y juzgar efectivamente la utilización indebida; promoviendo esfuerzos efectivos de asistencia mutua; reforzando el apoyo institucional a nivel internacional para la prevención, detección y recuperación de estos incidentes; y alentando la educación y la sensibilización.**
> *c)* Los gobiernos y otras partes interesadas deben fomentar activamente la educación y la sensibilización de los usuarios sobre la privacidad en línea y los medios de protección de la privacidad.
> *d)* Tomar medidas apropiadas contra el envío masivo de mensajes electrónicos no solicitados ("spam") a nivel nacional e internacional.
> *e)* Alentar una evaluación interna de la legislación nacional con miras a superar cualquier obstáculo al uso efectivo de documentos y transacciones electrónicas, incluido los medios electrónicos de autenticación.
> *f)* Seguir fortaleciendo el marco de confianza y seguridad con iniciativas complementarias y de apoyo mutuo en los ámbitos de la seguridad en el uso de las TIC, con iniciativas o directrices sobre el derecho a la privacidad y la protección de los datos y de los consumidores.
> *g)* Compartir prácticas óptimas en el ámbito de la seguridad de la información y la seguridad de las redes, y propiciar su utilización por todas las partes interesadas.
> *h)* Invitar a los países interesados a establecer puntos de contacto para intervenir y resolver incidentes en tiempo real, y desarrollar una red

[284] Texto disponível na sua integralidade em: <http://www.itu.int/wsis/docs/geneva/official/poa-es.html>. Acesso em: 18/01/2010.

> cooperativa entre estos puntos de contacto de forma que se comparta información y tecnologías para intervenir en caso de estos incidentes.
> *i)* Alentar el desarrollo de nuevas aplicaciones seguras y fiables que faciliten las transacciones en línea.
> *j)* Alentar a los países interesados a que contribuyan activamente en las actividades en curso de las Naciones Unidas tendentes a crear confianza y seguridad en la utilización de las TIC[285].

Já a segunda fase da CMSI foi realizada de 16 a 18 de novembro em Túnis, na Tunísia, com a presença de 45 Chefes de Estado ou de Governo e Vice-Presidentes e mais de 19 mil delegados, sendo 5.800 delegados representando mais de 174 Estados-Membros; 1.500 representantes de 92 organizações internacionais; 6.200 delegados, representando organizações não governamentais e a sociedade civil e 4.816, do setor privado, além de 1.222 jornalistas credenciados[286], números que demonstram o sucesso do evento e a mobilização de todos os interessados. Assim como na primeira fase, registrou-se a ocorrência de mais de 300 eventos relacionados à Cúpula em Túnis.

Como resultados mensuráveis da segunda fase têm-se o Compromisso de Túnis[287] e a Agenda de Túnis para a Sociedade da Informação[288]. Além de reiterar a Declaração de Princípios de Genebra e o Plano de Ação de Genebra, a Cúpula em seus documentos aborda três questões essenciais: os mecanismos de financiamento para a redução do hiato digital; a governança da Internet com a criação do Fórum de Governança da Internet[289] e a implementação e seguimento dos resultados e compromissos da CMSI, com a indicação das possíveis agências especializadas do Sistema das Nações Unidas que poderiam atuar como mediadoras e/ou facilitadoras em cada uma das linhas constantes do Plano de Ação de Genebra[290].

Outro aspecto relevante é a provisão contida no §111 da Agenda de Túnis, no sentido de que a AGNU faça uma apreciação em 2015 da implementação dos resultados da CMSI, estimulando a efetivação dos compromissos acordados pelas delegações e impactando no trabalho desenvolvido pelas organizações designadas como mediadoras e/ou facilitadoras das linhas de ação, visto que compõe o Sistema das Nações Unidas, do qual a AGNU é o órgão deliberativo e representativo.

---

[285] Grifo nosso.
[286] INTERNATIONAL TELECOMMUNICATION UNION, *ITU Building*, p. 14.
[287] Texto integral disponível para consulta em: <http://www.itu.int/wsis/docs2/tunis/off/7-es.html>. Acesso em: 18/01/2010.
[288] Texto integral disponível para consulta em: <http://www.itu.int/wsis/docs2/tunis/off/6rev1-es.html>. Acesso em 18/01/2010.
[289] Criação determinada pelo § 72 da Agenda de Túnis para a Sociedade de Informação. Seu mandato, características e funcionamento foram provisionados nos §§ 73 a 78.
[290] INTERNATIONAL TELECOMMUNICATION UNION, *ITU Building*, p. 12.

À UIT é atribuído o papel de mediadora e/ou facilitadora de oito linhas de ação, de um total de onze, dentre as quais duas são de sua competência exclusiva, notadamente as Linhas de Ação 2 e 5, que versam sobre infraestrutura de informação e comunicação e criação de confiança e segurança no uso das TICs, respectivamente. As três linhas de ação para as quais a UIT não recebeu o papel de mediadora e/ou facilitadora dizem respeito aos princípios da promoção e do respeito à diversidade cultural; do reconhecimento do papel dos meios de comunicação e da abordagem das dimensões éticas da SI, destacando-se, nesses casos, o papel da UNESCO, Organização das Nações Unidas para a Educação, a Ciência e a Cultura.

Percebe-se que a UIT recebeu uma extensa e complexa gama de atribuições, envolvendo questões que vão da infraestrutura de telecomunicações à segurança cibernética, do acesso à informação e ao conhecimento à capacitação dos agentes; do desenvolvimento de aplicações para as TICs ao estímulo ao engajamento dos Governos no uso das TICs para o desenvolvimento, até à cooperação regional e internacional, dentre outras.

No tocante à Agenda de Túnis, é pertinente citar a preocupação apontada, expressa por diversas vezes no texto do documento, quanto à segurança cibernética, ao combate da criminalidade cibernética e do terrorismo cibernético, trazendo-se à colação os seguintes parágrafos:

> **39. Pretendemos** crear confianza de los usurarios y seguridad en la utilización de las TIC fortaleciendo el marco de confianza. **Reafirmamos** la necesidad de continuar promoviendo, desarrollando e implementando en colaboración con todas las partes interesadas una cultura mundial de ciberseguridad, como se indica en la Resolución 57/239 de la Asamblea General de las Naciones Unidas y en otros marcos regionales relevantes. Esta cultura requiere acción nacional y un incremento de la cooperación internacional para fortalecer la seguridad mejorando al mismo tiempo la protección de la información, privacidad y datos personales. El desarrollo continuo de la cultura de ciberseguridad debería mejorar el acceso y el comercio y debe tener en cuenta el nivel de desarrollo social y económico de cada país y respetar los aspectos orientados al desarrollo de la Sociedad de la Información.
> **40. Destacamos** la importancia de enjuiciar la ciberdelincuencia, incluida la que se produce en una jurisdicción pero repercute en otra. **Destacamos además** la necesidad de concebir instrumentos y mecanismos nacionales e internacionales eficaces y eficientes, para promover la cooperación internacional, entre otros, de los organismos encargados de aplicar la ley en materia de ciberdelincuencia. **Instamos a los gobiernos** a que, en cooperación con otras partes interesadas, promulguen leyes que hagan posible la investigación y enjuiciamiento de la ciberdelincuencia, respetando los marcos vigentes, por ejemplo, las Resoluciones de la Asamblea General de las Naciones Unidas 55/63 y 56/121 sobre la "Lucha contra la utilización de la tecnología de la información con fines delictivos" y el *Convenio sobre el Delito Cibernético* del Consejo de Europa.
> [...]

> **44. Asimismo, subrayamos** la importancia de combatir el terrorismo, en todas sus formas y manifestaciones, en Internet, respetando los derechos humanos y en consonancia con las obligaciones contraídas en virtud del derecho internacional, según se indica en la Resolución de la Asamblea General de las Naciones Unidas A/60/L.1, donde se hace referencia al Artículo 85 del Documento Final de la Cumbre Mundial 2005.[291]

Demonstrada a alteração da missão institucional da UIT, essencialmente, em decorrência de sua designação como uma das organizações líderes no processo de implementação dos compromissos assumidos na CMSI bem como da efetivação dos Princípios por ela assentados, a título de entidade mediadora e/ou facilitadora, inclusive no tocante à criminalidade cibernética, cabe verificar-se como essa Agência vem desempenhando esse papel.

Nesse sentido, em cumprimento ao mandato atribuído pela CMSI, em especial pela Agenda de Túnis para a Sociedade da Informação, que lhe designou o papel de mediadora e facilitadora de 8 das 11 linhas de ação do Plano de Genebra, sendo exclusivo para as Linhas de Ação C.2. e C.5 (que buscam dar efetividade aos princípios de ampliação de infraestrutura das TICs e criação de confiança e segurança no uso destas tecnologias), a UIT vem desenvolvendo inúmeras atividades, dentre as quais se destaca aquelas em cumprimento à Linha de Ação C.5, Criação de Confiança e Segurança no uso das TICs.

Essa linha de ação foi contemplada no §12 do Plano de Ação de Genebra, já transcrito anteriormente, a qual empresta aos valores confiança e segurança a condição de um dos pilares mais importantes da SI. Esse parágrafo desmembra-se em dez passos a serem trilhados, a saber: favorecimento, no âmbito das Nações Unidas, da cooperação entre Governos e, em outros foros, da cooperação deles com as partes interessadas na efetivação desse princípio; prevenção e repressão da criminalidade cibernética pelos governos, em cooperação com o setor privado; fomento pelos governos e pelas partes interessadas da educação e sensibilização dos usuários com relação à privacidade; combate nacional e internacional do *spam*; avaliação da legislação interna de cada país, a fim de disseminar as práticas de documentos e transações eletrônicos; fortalecimento do marco de confiança e segurança com iniciativas complementares ou diretrizes na temática da proteção de dados e o direito a privacidade, por exemplo; compartilhamento de melhores práticas nesse campo e convite aos países interessados em estabelecer pontos de contato para o tratamento imediato de incidentes e em desenvolver rede cooperativa; estímulo ao desenvolvimento de novas

[291] Grifo do original.

aplicações mais seguras e confiáveis; e estímulo dos países interessados para continuarem a participar ativamente nas ações pertinentes das Nações Unidas.

Antes de tratar especificamente das ações adotadas pela UIT a fim de concretizar esse mandato, cabe menção de que a União realizou três grandes Conferências com a participação dos seus Estados-Membros, as quais forneceram o arcabouço normativo inicial para que a Agência instrumentalizasse os resultados da CMSI. Em 2006, foi realizada a Conferência Mundial de Desenvolvimento das Telecomunicações (CMDT), no âmbito da UIT-D, em Doha, no Quatar, cujos resultados são sintetizados em dois principais documentos: Declaração de Doha e o Plano de Ação de Doha[292].

Além disso, nessa Conferência também foi aprovada a Resolução n°45 que trata de mecanismos para o aumento da cooperação em segurança cibernética, incluindo o combate ao *spam*[293]. Em resumo, o documento aborda: a necessidade de confrontar os desafios e as ameaças decorrentes do abuso da tecnologia, inclusive para fins criminais e terroristas, respeitando os direitos humanos; a persecução penal dos crimes cibernéticos nos níveis nacional e regional; a necessidade de uma abordagem holística, incluindo cooperação internacional, para enfrentamento dos problemas associados à segurança cibernética, incluindo *spam*; e que o crescimento do problema dos crimes cibernéticos deve alarmar a toda comunidade internacional, incluindo a UIT.

A segunda conferência supramencionada, Conferência dos Plenipotenciários de Antalya, foi realizada em 2006, na Turquia quando foram aprovadas as Resoluções n°s130 e 149, as quais versam, respectivamente, sobre o fortalecimento do papel da UIT na criação da confiança e segurança no uso das TICs e sobre o estudo de definições e terminologias pertinentes à temática[294].

Já na Assembléia Mundial de Normalização das Telecomunicações, da UIT-T, realizada em Johannesburgo, na África do Sul, em 2008, tem-se a edição de três resoluções: Resolução 50[295], sobre segurança cibernética; Resolução 52[296], que trata do combate ao *spam*

---

[292] Nesse sentido, ver INTERNATIONAL TELECOMMUNICATION UNION, *ITU Building*, p. 16.

[293] Texto da Resolução disponível em: <http://www.itu.int/ITU-D/e-strategies/Cybersecurity/Meetings /Geneva 2006/Documents/Res%2045.pdf>. Acesso em: 25/05/2009.

[294] Textos das Resoluções disponíveis, respectivamente em: <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/security-related-extracts-pp-06.pdf> e <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/security-related-extract-pp-06.pdf>**.** Acesso: 21/01/2010.

[295] Texto Integral da Resolução disponível em: <http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.50-2008-PDF-E.pdf>. Acesso em: 21/01/2010.

[296] Texto Integral da Resolução disponível em: <http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.52-2008-PDF-E.pdf>. Acesso em: 21/01/2010.

e Resolução 58[297], que encoraja a criação de Grupos de Resposta a Incidentes de Segurança pelos países em desenvolvimento, especialmente.

Posteriormente, a CMDT de 2010, realizada em Hiderabade na Índia, e a Conferência dos Plenipotenciários de 2010, de Guadalajara no México, corroboraram o papel da UIT para a implementação dos compromissos da CMSI, revisando resoluções pertinentes e editando novas[298], sendo a segurança cibernética um dos temas centrais e mais controversos das duas conferências.

Dos documentos resultantes da Conferência dos Plenipotenciários, ganha destaque a Resolução n.° 174 da Conferência dos Plenipotenciários de Guadalajara[299], sobre questões de políticas públicas internacionas relacionadas ao risco do uso ilícito das TICs, a qual considera o papel da UIT de facilitadora e moderadora da Linha de Ação C.5, para instruir o Secretário-Geral a adotar as medidas necessárias para sensibilizar os Estados-Membros sobre a temática e manter o papel da UIT de cooperar com outros órgãos das Nações Unidas na matéria. Além disso, a resolução também solicita ao Secretário-Geral a organizar encontro dos Estados-Membros e relevante atores dos setor das TICs para discutir abordagens alternativas para enfrentar e prevenir a aplicação ilícita das TICs; convida os Estados-Membros e relevantes atores dos setor das TICs para buscar o dialogo nacional e regional no intuito de encontrar soluções mútuas aceitáveis; e convida o Secretário-Geral a coletar as melhores práticas a fim de assistir aos Estados-Membros interessados.

No tocante aos documentos da CMDT de Hiderabade, 2010, deve-se salientar a revisão da Resolução n.° 45 de Doha, 2006, que trata de mecanismos para aumentar a cooperação em segurança cibernética, incluindo o combate ao *spam*, a qual reconhece a necessidade de lidar com o crescente problema do spam, assim como crimes cibernéticos e outras ameaças, convidando ao Secretário-Geral, em coordenação com os diretores dos três setores da união a preparar documento relacionado a possível Memorando de Entendimento entre Estados-Membros para aumentar a segurança e combater as ameaças cibernéticas. Esse memorando nada mais é que uma tentativa de formalizar a cooperação dos países,

---

[297] Texto Integral da Resolução disponível em: <http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.58-2008-PDF-E.pdf>. Acesso em: 21/01/2010.

[298] Texto das resoluções aprovadas pela Conferência dos Plenipotenciários de 2010 disponível em: <http://www.itu.int/pub/S-CONF-PLEN-2011/en>. Acesso em: 29/11/2011. Referentemente à segurança cibernética e à Linha de Ação C.5, destaca-se as Resoluções 71, plano estratégico da UIT para 2012-2015; 130, fortalecimento do papel da UIT na criação de confiança e Segurança no uso das TICs; 174, papel da UIT relacionada às questões de políticas públicas internacionais referentes ao risco do uso ilícito das TICs; 179, papel da UIT na proteção das crianças na Internet; e 181, definição de segurança cibernética.

[299] Resolução n.° 174 (Guadalajara, 2010), com texto disponível em: <http://www.itu.int/pub/S-CONF-PLEN-2011/en>. p. 606.

especialmente dos países em desenvolvimento, que não estão amparados, em sua grande maioria, por iniciativas regionais.

Também não se pode olvidar que a UIT estabeleceu a salvaguarda das redes como uma das suas sete metas e orientações estratégicas, no seguinte sentido:

> *Meta estratégica cuatro*[300]
> Elaborar instrumentos baseados en las contribuciones de los Miembros, para promover la confianza de los usuarios y salvaguardar la eficacia, seguridad, integridad e interoperabilidad de las redes.*
> ** El concepto de eficacia y seguridad de las redes de información y comunicación abarca amenazas que comprenden, entre otras, el correo basura (spam), la ciberdelincuencia, los virus, los gusanos y los ataques de denegación de servicio.*[301]

No desempenho desse papel central de implementação da Linha de Ação ligada à segurança cibernética, existem diversas atividades realizadas, ou em andamento, pela UIT, abrangendo questões de estudos nos Grupos de Estudo da UIT-T e da UIT-D, simpósios e conferências sobre o assunto; publicações de materiais explicativos, guias, melhores práticas e diretrizes para o enfrentamento do problema; assistência técnica; parcerias de cooperação nos níveis nacional, regional e internacional; e iniciativas, dentre as quais se destaca a Agenda Global de Segurança Cibernética (AGSC)[302], que consolida várias ações e o Programa Proteção das Crianças *Online* [303].

A AGSC[304], que foi lançada em 17 de maio de 2007 pela UIT, em cumprimento ao seu papel de facilitadora da Linha de Ação C.5, fornece um arcabouço dentro do qual a resposta internacional aos crescentes desafios em segurança cibernética pode ser coordenada e direcionada. Destaca a Agência no seu Relatório Anual de 2008[305]:

> La *Agenda sobre ciberseguridad global (GCA)* es un marco mundial para el diálogo y la cooperación a fin de coordinar la respuesta internacional a las dificultades crecientes de ciberseguridad. Trata de aprovechar trabajos existentes para elaborar un marco mundial de coordinación, en colaboración con algunos de los mayores expertos en la materia. Está basada en cinco temas de trabajo, a saber, medidas jurídicas, medidas técnicas y procesales, estructuras orgánicas, creación de capacidad y cooperación internacional [...].

---

[300] UNIÓN INTERNACIONAL DE TELECOMUNICACIONES, *UIT, Informe*, p. 52-61.
[301] Grifo original.
[302] Sobre a AGSC – Global Cybersecurity Agenda (CGA) ver material disponível em: <http://www.itu.int/osg/csd /cybersecurity/gca/new-gca-brochure.pdf>. Acesso em: 25/10/2009.
[303] Sobre a Iniciativa Proteção das Crianças *Online* (Child Online Protection – COP) ver material disponível em: <http://www.itu.int/osg/csd/cybersecurity/gca/cop/cop-brochure.pdf>. Acesso em: 21/01/2010. Ressalta-se a existência na página da iniciativa na Internet, <http://www.itu.int/cop>, de material específico destinado aos tipos de público alvo, tais como crianças; pais e educadores; setor privado; e poder público.
[304] Ver página oficial da Iniciativa disponível em: <http://www.itu.int/osg/csd/cybersecurity/gca/>. Acesso em: 25/10/2009.
[305] UNIÓN INTERNACIONAL DE TELECOMUNICACIONES, *UIT, Informe*, p. 54.

A AGSC utilizou o trabalho do Grupo de *Experts* de Alto Nível (GEAN)[306], um grupo de aconselhamento criado em 2007 e integrado por 100 renomados e conhecidos *experts* de diversos países, setores (público, privado e academia) e áreas do conhecimento, que trabalhou a partir de outubro de 2007 e durante todo primeiro semestre de 2008 com a finalidade de propor medidas no intuito de combater as ameaças e a criminalidade cibernética, assim como promover a segurança cibernética. Como fruto do seu esforço, cita-se a Série de Propostas Estratégicas, com um informe de autoria do presidente do grupo e o Relatório de Estratégia Global do GEAN[307].

As propostas versam justamente sobre os cinco pilares da AGSC: medidas legais, medidas técnicas e procedimentais, estrutura organizacional, capacitação dos agentes e cooperação internacional. Esses pilares englobam, respectivamente: desafios legais e harmonização das legislações nacionais, no sentido de torná-las compatíveis internacionalmente, bem como elaboração de lei contra criminalidade cibernética modelo; técnicas e procedimentos para o tratamento de vulnerabilidades em softwares; resposta estratégica e institucional para prevenção, detecção e reação a ataques cibernéticos, bem como gerenciamento de crise e proteção de infraestrutura crítica de sistemas de informação de cada país; ações concretas de capacitação dos atores no sentido de sensibilização, transferência de conhecimento e criação de uma política nacional de segurança cibernética; estratégia envolvendo todos os interessados para cooperação, diálogo e coordenação internacional, uma vez que os crimes cibernéticos são transnacionais e, portanto, o seu combate também deve ser no mesmo âmbito de abrangência[308].

No âmbito da AGSC, foi lançada a Parceria Internacional Multilateral contra Ameaças Cibernéticas, denominada de *Impact (International Multilateral Partnership Against Cyber Threats),* da qual o Brasil é parte, criada em 2009 e com sede na Malásia, que espera fornecer aos seus membros o estado da arte em recursos na luta contra essas ameaças[309], funcionando como centro de resposta global, laboratório de treinamento e centro para cooperação internacional.

---

[306] Nesse sentido, ver *UIT, Informe*, p. 54, e UNIÃO INTERNACIONAL DE TELECOMUNICAÇÕES. *Cybersecurity for All : ITU's work for a safer world.* Genebra: UIT, 2008. 32 p. 8. Disponível em: <http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-CYBER-2008-PDF-E.pdf>. Acesso em: 25/10/2009.

[307] Relatório disponível em: <http://www.itu.int/osg/csd/cybersecurity/gca/docs/Report_of_the_Chairman_of_HLEG_to_ITU_SG_03_sept_08.pdf>. Acesso em: 24/11/2011.

[308] INTERNATIONAL TELECOMMUNICATION UNION, *Cybersecurity*, p. 8-10.

[309] Informações sobre o Impact na página da iniciativa disponível em: <http://www.impact-alliance.org/>. Acesso em: 28/10/2009.

Merece destaque, ainda, o Portal de Segurança Cibernética, criado pela UIT na Internet[310], que agrega uma grande quantidade informações, incluindo todos os programas desenvolvidos pela UIT, os trabalhos desenvolvidos no âmbito dos seus setores, os materiais produzidos, relação de eventos pertinentes e uma preciosa base de dados sobre a legislação que dispõe sobre crimes cibernéticos em 38 países, dentre eles, Alemanha, Austrália, China, Estados Unidos, Índia etc.

Nessa esteira, o portal da UIT tornou-se a mais importante referência não somente para a pesquisa de Direito Comparado no assunto, pelos dados sobre leis nacionais que possui, mas também para o Direito Internacional, pois possui uma coletânea de documentos regionais e internacionais pertinentes, alocados no item referente às medidas legais da AGSC.

Com relação aos diversos materiais produzidos ou financiados pela UIT, disponíveis no Portal, cabe citar o "Guia de Legislação sobre Crimes Cibernéticos da UIT"[311]; a publicação "Entendendo os Crimes Cibernéticos: um Guia para Países em Desenvolvimento"[312]; o Guia para Promoção de uma Cultura de Segurança Cibernética da UIT; o Guia de Autoavaliação sobre Proteção de Infraestrutura Crítica de Informação etc.

Faz-se necessário o apontamento quanto às diversas recomendações de segurança expedidas na esfera da UIT-T, que possui um Grupo de Estudo exclusivo para a pesquisa nesse campo, que conta com diversas questões de estudos, abordando, por exemplo, gerenciamento de segurança, serviços de comunicação seguros e contenção de *spam* por meios técnicos.

Por fim, recorda-se, na UIT-D, a existência da Questão de Estudo 22 no Grupo 1 desde 2006 intitulada: "Segurança nas Redes de Informação e Comunicação: Melhores Práticas para o Desenvolvimento de uma Cultura de Segurança Cibernética", cujo trabalho do primeiro ciclo de estudos, realizado de 2006-2010, gerou um relatório[313], dividido em cinco partes, respectivamente: desenvolvimento e obtenção de um consenso acerca da estratégia nacional de segurança cibernética; estabelecimento de colaboração nacional entre governo e indústria; combate aos crimes cibernéticos; criação de capacidade de

---

[310] Página disponível no endereço: <http://www.itu.int/cybersecurity/gateway>. Acesso em: 25/10/2009.

[311] Disponível em: <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf>. Acesso em: 25/10/2009.

[312] Disponível: em: <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf>. Acesso em: 25/10/2009.

[313] INTERNATIONAL TELECOMMUNICATION UNION. *Question 22-1: Securing information and communication networks: best practices for developing a culture of cybersecurity*. Final Report. 72 p. Disponível em: <http://www.itu.int/dms_pub/itu-d/opb/stg/D-STG-SG01.22-2010-PDF-E.pdf>. Acesso em: 05/03/2011.

gerenciamento nacional de incidentes; e promoção de uma cultura nacional de segurança cibernética.

Especificamente no tocante à luta contra os crimes cibernéticos, o relatório final aponta que segurança cibernética pode ser melhorada, dentre outras medidas, com o estabelecimento e modernização de elementos de apoio, legislação criminal e processual penal e políticas para prevenir, impedir, responder e processar os crimes cibernéticos[314].

Dessa forma, o documento esclarece que a meta é a promulgação e aplicação de um conjunto compreensivo de leis relacionadas à segurança cibernética e aos respectivos delitos, sendo que este objetivo pode ser alcançado com os seguintes passos: avaliação pelos países de seus códigos penais e processuais penais a fim de determinar se está adequado para enfrentar os problemas atuais e futuros; elaboração e adoção de políticas e leis materiais, processuais e de assistência mútua para enfrentar os crimes cibernéticos, recomendando a participação ativa dos países no desenvolvimento da legislação necessária, levando em consideração iniciativas regionais, por exemplo, a Convenção de Budapeste; estabelecimento ou identificação de unidades nacionais de combate aos crimes cibernéticos; desenvolvimento de relações de cooperação com outros elementos da infraestrutura nacional de segurança cibernética e o setor privado; promoção da compreensão das questões referentes aos crimes cibernéticos entre integrantes do Ministério Público, juízes e legisladores; e participação na Rede 24/7 de Pontos de Contato sobre Crimes Cibernéticos[315].

A CMDT de 2010 garantiu mais um período de estudo à questão, ampliando seu campo de pesquisa, a fim de aprofundar os temas analisados no primeiro ciclo, com destaque para a proteção das crianças e adolescentes na Internet, produzir material para capacitação na área em países em desenvolvimento e produzir um compêndio de melhores práticas na temática, contando com a contribuição brasileira.

Por todo o exposto, percebe-se que é inquestionável, indispensável e extremamente relevante o trabalho que a UIT tem realizado, fazendo com que se torne uma referência para estudo, pesquisa e cooperação nessa temática. Claro que é importante se evitar a duplicação e sobreposição de esforços em órgãos e agências do Sistema das Nações Unidas, sendo necessária a delimitação precisa do seu campo de atuação, pois como será visto a seguir, o tópico também vem sendo tratado no Escritório das Nações Unidas sobre Drogas e Crime.

Nesse sentido, comemora-se as decisões da última Conferência dos Plenipotenciários, realizada em 2011, que limitou a atuação da UIT nesta esfera, conforme Resolução n.° 130

[314] INTERNATIONAL TELECOMMUNICATION UNION, *Question*, p. 14.
[315] Id, Op. Cit., p. 14-18

revista em Gualadajara, 2010[316], assentando a necessidade de evitar duplicação de trabalho entre os setores da União ou de trabalho que recaia mais apropriadamente no mandato de outros órgãos intergovernamentais ou internacionais, e que a UIT deve atuar na sua área de *expertise* técnica, excluindo assuntos relacionados à aplicação de lei referentes à segurança nacional, à defesa nacional, ao conteúdo e aos crimes cibernéticos, fato que não exclui as atribuições da União no tocante ao desenvolvimento de recomendações de aspectos técnicos e ao auxílio aos Estados-Membros, particularmente países em desenvolvimento, na elaboração de medidas legais relacionadas à proteção contra ameaças cibernéticas e nas atividades desenvolvidas no âmbito da Questão de Estudo 22, supramencionada.

Passa-se agora para a análise do trabalho desenvolvido pelo Escritório das Nações Unidas sobre Drogas e Crime e órgãos relacionados, que responde pelos esforços do Sistema das Nações Unidas na matéria, juntamente com a AGNU e com a UIT.

A.3 Escritório das Nações Unidas sobre Drogas e Crime

O Escritório das Nações Unidas sobre Drogas e Crime (UNODC) é o órgão vinculado à Secretaria das Nações Unidas[317], responsável pela luta contra os crimes internacionais e contra as drogas. Foi estabelecido em 1997 com a junção do Programa das Nações Unidas de Controle de Drogas e do Centro para Prevenção de Crimes Internacionais[318], tornando-se encarregado da implementação de ações baseadas nas três convenções internacionais de

---

[316] Texto da resolução disponível em: <http://www.itu.int/pub/S-CONF-PLEN-2011/en>. Acesso em 29/11/2011. p. 450-461. *"(...) resolves (...) 2 to give high priority to the work in ITU described in bearing in mind above, in accordance with its competences an areas of expertise, while being mindful of the need to avoid duplicating work among the Bureaux or the General Secretariat or work which more appropriately falls within the manates of other relevant international bodies; 3 that ITU shall focus resources and programmes on those areas of cybersecurity within its core mandate and expertise, notably the technical and development spheres, and not including areas related to Member States' application of legal or policy principles related to national defence, national security, content and cybercrime, which are within their sovereign rights, although this does not however exclude ITU from carrying out its mandate to develop technical recommendations designed to reduce vulnerabilities in the ICT infrastructure, nor from providing all the assistance that was agreed upon at WTDC-10, including Programme 2 activities such as "assisting Member States, in particular developing countries, in the elaboration of appropriate and workable legal measures relating to protection against cyberthreats" and in activities under Question 22-1/1*".

[317] Informações sobre a estrutura da Secretaria das Nações Unida disponíveis em: <http://www.un.org/en/mainbodies/secretariat/>. Acesso em: 23/02/2011.

[318] Informações sobre a UNDOC obtidas no site oficial da agência, disponível em: <http://www.unodc.org/unodc/en/about-unodc/index.html?ref=menutop>. Acesso em: 22/02/2011 e nas publicações UNITED NATIONS OFFICE ON DRUGS AND CRIME. *Making the World Safer from Crime, Drugs and Terrorism*. Eslováquia: UNODC, 2007. 4 p. Disponível em: <http://www.unodc.org/pdf/unodc_brochure_2007.pdf>. Acesso em: 23/02/2011, e UNITED NATIONS OFFICE ON DRUGS AND CRIME. *2010 Report*. 74 p. Disponível em: http://www.unodc.org/documents/frontpage/UNODC_Annual_Report_2010_LowRes.pdf>. Acesso em: 23/02/2011.

controle de drogas e nas convenções contra o crime organizado transnacional e contra a corrupção. Dessa maneira, seu campo de atuação foca-se em três áreas: saúde, segurança pública e justiça, as quais abrangem temáticas como o combate às drogas, ao tráfico de pessoas, ao terrorismo, à corrupção e à lavagem de dinheiro, dentre outras[319].

Inclui-se no seu mandato a assistência aos Estados-Membros na luta contra as drogas, crimes e terrorismo, sendo que, na Declaração do Milênio das Nações Unidas, os Estados-Membros resolveram intensificar os esforços para o combate aos crimes transnacionais em todas suas dimensões, a fim de redobrar os esforços para implementar o compromisso de combate ao problema mundial das drogas e para tomar medidas coordenadas contra o terrorismo internacional[320].

O UNODC possui escritórios de campo, nacionais e regionais, abarcando mais de 150 países e seu orçamento provém de contribuições voluntárias, sendo que 90% das contribuições são oriundas dos Estados-Membros[321].

O trabalho do escritório é baseado em três pilares[322]:

> **Trabalho normativo**, para ajudar os Estados na ratificação e na implementação dos tratados internacionais, e no desenvolvimento de suas legislações nacionais em matérias de drogas, criminalidade e terrorismo, além de oferecer serviços técnicos e operacionais para órgãos de execução e controle estabelecidos pelos tratados internacionais.
> **Pesquisa e análise**, para aumentar o conhecimento e a compreensão dos problemas relacionados às drogas e à criminalidade e para ampliar a definição de políticas e de estratégias com base em critérios baseados em evidências.
> **Assistência técnica**, por meio de cooperação internacional, para aumentar a capacidade dos Estados-membros em oferecer uma resposta às questões relacionadas às drogas ilícitas, ao crime e ao terrorismo.

O Escritório tem importante papel na preparação e realização dos Congressos das Nações Unidas sobre a Prevenção ao Crime e Justiça Criminal, os quais são realizados a cada cinco anos, desde 1955, e funcionam como órgão consultivo do Programa das Nações Unidas sobre Prevenção ao Crime e Justiça Criminal, de acordo com as provisões do parágrafo 29 do Anexo à Resolução n.° 152, aprovada na 46° Sessão da AGNU, em 18 de dezembro de 1991. A Comissão sobre Prevenção ao Crime e Justiça Criminal é o órgão responsável pelo

---

[319] Nesse sentido ver site da oficina regional da UNDOC no Brasil, disponível em: <http://www.unodc.org/southerncone/pt/sobre-unodc/index.html>. Acesso em: 22/02/2011.
[320] Informações sobre a UNDOC obtidas no site oficial da agência, disponível em: <http://www.unodc.org/unodc/en/about-unodc/index.html?ref=menutop>. Acesso em: 22/02/2011.
[321] Informações sobre a UNDOC obtidas no site oficial da agência, disponível em: <http://www.unodc.org/unodc/en/about-unodc/index.html?ref=menutop>. Acesso em: 22/02/2011.
[322] Nesse sentido ver site da oficina regional da UNDOC no Brasil, disponível em: <http://www.unodc.org/southerncone/pt/sobre-unodc/index.html>. Acesso em: 22/02/2011.

desenvolvimento, monitoramento e revisão da implementação do programa, cabendo também à Comissão a preparação dos congressos, consoante parágrafo 26 da resolução supracitada, ressaltando-se, por fim, que a comissão é órgão vinculado ao Conselho Econômico e Social das Nações Unidas, por força do parágrafo 23 do Anexo à Resolução 46/152[323].

Ainda com relação aos congressos, deve-se mencionar que a Resolução n.° 119, aprovada na 56° Sessão da AGNU, em 19 de dezembro de 2001, estabelece o seu papel, sua função, sua periodicidade e duração, determinando que, a partir de 2005, os congressos devam obedecer a diversas diretrizes, conforme parágrafo 2°, dentre as quais, destacam-se: a) discussão de tópicos específicos, incluindo um tema central, quando apropriado, determinados pela Comissão sobre Prevenção ao Crime e Justiça Criminal; b) inclusão de processo prévio de consulta; c) inclusão de segmento de alto nível no qual os Estados serão representados por delegados do mais alto nível possível, os quais terão a oportunidade de fazer declarações sobre os temas do congresso; d) facilitação pela Secretária-Geral da organização de encontros auxiliares de organizações não governamentais e profissionais nos congressos; e) adoção de uma declaração única contendo recomendações das deliberações do segmento de alto nível, das mesas redondas e dos *workshops* e f) realização de encontros regionais de preparação, quando necessário[324].

O último congresso, o Décimo-Segundo Congresso das Nações Unidas sobre Prevenção ao Crime e Justiça Criminal, foi realizado em Salvador, Brasil, de 12 a 19 de abril de 2010 e a utilização das TICs para práticas criminosas e as dificuldades de persecução destes delitos esteve presente nas discussões, em atendimento à Resolução n.° 193, aprovada na 63° Sessão da AGNU, em 18 de dezembro de 2008, que estabeleceu que o tema central do congresso seria "Estratégias Amplas para Desafios Globais: Sistemas de Prevenção ao Crime e Justiça Criminal e seus Desenvolvimentos em um Mundo em Transformação". Um dos tópicos específicos foi justamente os recentes desenvolvimentos no uso da ciência e tecnologia por criminosos e pelas autoridades competentes na luta contra o crime, incluindo o caso dos crimes cibernéticos, nos termos do parágrafo 5° da Resolução n.° 193, que aprovou a agenda provisional do congresso, finalizada pela Comissão sobre Prevenção ao Crime e Justiça Criminal[325].

---

[323] Resolução n.° 152, aprovada na 46° Sessão da AGNU, e seu respectivo anexo disponível em: <http://daccess-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/582/40/IMG/NR058240.pdf?OpenElement>. Acesso em: 23/02/2011.

[324] Resolução n.° 119, aprovada na 56° Sessão da AGNU, e seu respectivo anexo disponível em: <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N01/481/61/PDF/N0148161.pdf?OpenElement>. Acesso em: 23/02/2011.

[325] Resolução n.° 193, aprovada na 63° Sessão da AGNU, e seu respectivo anexo disponível em: < http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N08/482/37/PDF/N0848237.pdf?OpenElement>. Acesso em: 23/02/2011.

Em decorrência da adoção do tópico específico para discutir o uso nas TICs em condutas criminosas e pelas autoridades competentes no combate à criminalidade, foi preparado um documento de trabalho pela Secretaria[326], em que são ressaltados os limites da Convenção de Budapeste, relatando que a experiência demonstra a relutância de países em ratificar ou aderir a tratados dos quais não participaram das negociações e fazendo a ressalva de que, em todos os quatros encontros regionais de preparação, foi levantada a necessidade de uma convenção internacional sobre crimes cibernéticos[327].

O resultado das discussões da matéria foi condensado na Declaração de Salvador sobre "Estratégias Amplas para Desafios Globais: Sistemas de Prevenção ao Crime e Justiça Criminal e seus Desenvolvimentos em um Mundo em Transformação", contemplando recomendações sobre o assunto nos seguintes itens:

> [...]
> 39. Registramos que o desenvolvimento das tecnologias de informação e comunicação e o crescente uso da Internet abrem novas oportunidades para os criminosos e facilitam o crescimento de crimes.
> 40. Reconhecemos a vulnerabilidade das crianças e conclamamos a iniciativa privada a promover e apoiar esforços para prevenir o abuso sexual e a exploração de crianças através da internet.
> 41. Recomendamos **que o Escritório das Nações Unidas sobre Drogas e Crime forneça, caso solicitado e em cooperação com os Estados Membros, organizações internacionais envolvidas e setor privado, assistência técnica e qualificação aos Estados para aperfeiçoar as legislações nacionais e capacitar as autoridades nacionais com o intuito**

[326] Texto do documento de trabalho disponível em: <http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_9/ V1050382e.pdf>. Acesso em: 23/02/2011.

[327] Fragmento original do Documento de Trabalho: *"[…] 34. Another aspect of the role of regional frameworks as instruments for a global harmonization is the ability of non-members to participate. Despite the transnational dimension of cybercrime, the impact in the different regions of the world is different. This is especially relevant for developing countries. The regional approaches mentioned in paragraph 32 above do not offer a possibility for a broad involvement of non-members. While the Convention on Cybercrime is currently the instrument with the broadest membership,* ***even it limits the possibility of non-members to participate****. In article 37 of the Convention, it is stipulated that accession requires States to consult with and obtain the unanimous consent of the contracting States to the Convention. In addition, participation in the debate about possible future amendments is limited to parties of the Convention (art. 44). 35.* ***Experience has shown that States are generally reluctant to ratify or accede to conventions that they have not contributed to developing and negotiating. This has been true regardless of the topic of the conventions****. 36.* ***At all four regional preparatory meetings for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, calls were made for the development of an international convention on cybercrime****. 37.* ***Another such call was made at the meetings of the Heads of National Law Enforcement Agencies, Africa, the Near and Middle East and Europe, at which discussions were held on the Internet, electronic evidence gathering, legislation etc****. At meetings held in other regions, participants concluded that law enforcement agencies and judiciaries were poorly prepared and had insufficient capacity to address developments in cybercrime and to gather and use evidence from cybertechnologies in the preparation of prosecutions. There was universal agreement that national laws were not keeping pace and that amendments were needed to support the investigation, prosecution and conviction of offenders on the basis of evidence captured through cybertechnology. There is an urgent need for common rules and cooperation between States so that authorities can act effectively across jurisdictions to bring offenders to justice.* ***Calls for an international instrument have also come from academia.*** *[…]"*(Grifo nosso). Texto disponível em: <http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_9/ V1050382e.pdf>. Acesso em: 23/02/2011.

> **de combater o crime cibernético, incluindo a prevenção, detecção, investigação e persecução de tal modalidade criminosa em todas as suas formas, bem como de aumentar a segurança das redes de computadores**. 42. **Convidamos a Comissão sobre Prevenção ao Crime e Justiça Criminal** a considerar a convocação de um grupo aberto intergovernamental de experts para conduzir um estudo aprofundado da questão do crime digital e sobre as respostas dos Estados Membros, da comunidade internacional e da iniciativa privada, incluindo o compartilhando informações legislação nacional, boas práticas, assistência técnica e cooperação internacional, **com o propósito de considerar as opções para o fortalecimento das existentes e para propor novas legislações nacionais e internacionais e outras respostas ao crime cibernético**.
> [...][328].

A Declaração de Salvador foi endossada pelo Conselho Econômico e Social das Nações Unidas, na Resolução n.° 18 de 2010[329], que recomenda à AGNU, a adoção de minuta de resolução referente ao Décimo-Segundo Congresso das Nações Unidas sobre Prevenção ao Crime e Justiça Criminal, aprovada na Resolução n.° 230 da 65° Sessão da AGNU. O texto das resoluções requer a implementação do parágrafo 42 da Declaração, o qual convida a Comissão sobre Prevenção ao Crime e Justiça Criminal a convocar um grupo aberto intergovernamental de experts para conduzir um estudo aprofundado sobre os crimes cibernéticos. Ademais, as resoluções também solicitam que o UNODC, no desenvolvimento e na implementação dos programas de assistência técnica, objetive resultados sustentáveis e de longa duração na prevenção, persecução e punição da criminalidade, particularmente pela criação, modernização e fortalecimento dos sistemas de justiça criminal, assim como a promoção do Estado do Direito e desenhe programas para atingir todos os componentes do sistema de justiça criminal, de maneira integrada e com perspectiva de longa duração, aumentando assim a capacidade dos países solicitantes para prevenir e suprimir os vários tipos

---

328 "[...] *39. We note that the development of information and communications technologies and the increasing use of the Internet create new opportunities for offenders and facilitate the growth of crime. 40. We realize the vulnerability of children, and we call upon the private sector to promote and support efforts to prevent child sexual abuse and exploitation through the Internet. 41. We recommend that the United Nations Office on Drugs and Crime, upon request, provide, in cooperation with Member States, relevant international organizations and the private sector, technical assistance and training to States to improve national legislation and build the capacity of national authorities, in order to deal with cybercrime, including the prevention, detection, investigation and prosecution of such crime in all its forms, and to enhance the security of computer networks. 42. We invite the Commission on Crime Prevention and Criminal Justice to consider convening an open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime.* [...]" (Tradução e grifos nossos). disponível em: <http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/Salvador_Declaration/Salvador_Declaration_E.pdf>. Acesso em 18/01/2011.

329 Texto oficial disponível em: <http://www.un.org/en/ecosoc/docs/2010/res%202010-18.pdf>. Acesso em 24/02/2011.

de crimes que afetam a sociedade, incluindo o problema do crime organizado e dos crimes cibernéticos.

Em atendimento ao parágrafo 42 da Declaração, foi convocado o Grupo de Experts sobre Crimes Cibernéticos, que realizou sua primeira reunião em Viena, na Áustria, em janeiro de 2011. Neste encontro, que contou com a participação de mais de 300 delegados, representando 78 países e diversas entidades, incluindo academia[330], discutiu-se o objeto de estudo do grupo de experts, bem como a metodologia a ser utilizada[331], a qual prevê a finalização do trabalho com a submissão do estudo à Comissão sobre Prevenção ao Crime e Justiça Criminal em sua 22° Sessão, a ser realizada em abril de 2013. A metodologia atribui ao UNODC a responsabilidade pelo desenvolvimento de estudo, incluindo a elaboração de questionário, a coleta e a análise dos dados e a preparação a minuta de texto do estudo. Além de contar com sua expertise interna, o trabalho da UNODC será auxiliado por grupos regionais compostos de até seis experts, provenientes dos governos, os quais serão consultados pela secretaria de maneira *ad hoc*.

Seguindo o calendário de trabalho proposto na metodologia supracitada, a identificação dos experts que auxiliarão a UNODC na condução do estudo foi prevista para o mês de abril de 2011. No mesmo mês, na Vigésima Sessão da Comissão sobre Prevenção ao Crime e Justiça Criminal, ocorreu a divulgação da minuta de questionário a ser disseminado entre os Estados-Membros, Organizações Intergovernamentais, Setor Privado e Academia, o qual consiste em uma única pesquisa, baseada nos apontamentos do Documento de Trabalho da 1° Reunião do Grupo de Experts e em suas recomendações, ficando a minuta em consulta até junho de 2011. Em julho de 2011 foi prevista a finalização do questionário e a remessa aos interessados, destacando-se a garantia de confidencialidade e de anonimato dos dados recebidos, especialmente, para o setor privado. Até dezembro de 2011, objetivou-se a coleta e classificação dos dados, sendo marcada para o mesmo mês a 2° Reunião do Grupo de Experts.

Dando continuidade aos trabalhos, de janeiro a julho de 2012, está prevista a análise dos dados e elaboração da minuta do texto resultante do estudo, sendo que, em abril de 2012, será apresentado relatório de progresso à Comissão sobre Prevenção ao Crime e Justiça Criminal, em sua Vigésima Primeira Sessão. O mês de agosto de 2012 está destinado para a

---

[330] O Brasil foi representado no encontro por 8 delegados, incluindo integrantes do Ministério da Justiça, Polícia Federal, Ministério das Relações Exteriores e da Missão permanente do Brasil junto às Nações Unidas em Viena, conforme lista oficial de participantes disponível em: <http://www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/UNODC_CCPCJ_EG4_2011_INF_2_Rev1.pdf>. Acesso em: 24/02/2011.

[331] Descrita no documento disponível em: <http://www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/Working_Papers/Methodology_timeline_REV-7.pdf> . Acesso em 24/02/2011.

divulgação da minuta de texto do estudo aos Membros do Grupo de *Experts*, a fim de garantir a tempestiva preparação para a 3° Reunião do Grupo de *Experts*, a ser realizada em outubro de 2012, cuja agenda inclui a revisão, correção e adoção da minuta do estudo. Finalmente, conforme relatado anteriormente, em abril de 2013 o estudo será submetido à Comissão sobre Prevenção ao Crime e Justiça Criminal, em sua Vigésima Segunda Sessão[332].

Quanto ao objeto, o documento de trabalho de proposta de tópicos para análise no compreensivo estudo sobre o impacto e a resposta aos crimes cibernéticos prevê o exame de 12 temas, agrupados em 5 áreas-chave, com o objetivo de compreender extensivamente cada um deles. Os 12 tópicos são: a) fenômeno dos crimes cibernéticos, b) estatísticas e c) desafios (agrupados na área-chave do problema dos crimes cibernéticos); d) abordagens comuns para legislação, e) criminalização, f) poderes de investigação, g) cooperação internacional, h) evidências eletrônicas e i) papel e responsabilidade dos provedores de serviço e do setor privado (respostas legais aos crimes cibernéticos); j) prevenção ao crime e capacitação da justiça criminal e outras respostas aos crimes cibernéticos; k) organizações internacionais; e l) assistência técnica[333].

O Livro Verde sobre segurança cibernética no Brasil do DSIC, ao tratar das potenciais diretrizes estratégicas que deveriam ser abarcadas no estabelecimento de uma Política Nacional de Segurança Cibernética, ressalta no tocante ao vetor marco legal, as seguintes visões de curto (2 - 3 anos) e médio prazos (5 – 7 anos) [334]:

> **COLABORAR** estritamente para a atualização e por vezes para a **construção do marco legal, nacional e internacional**, contra ataques e **crimes cibernéticos, no curto e médio prazo**;
> **PROTAGONIZAR a articulação e a elaboração de Convenção global, sobre crime cibernético, no âmbito da ONU, no curto e médio prazo**.[335]

Ressalva-se que a menção à Convenção Global no âmbito da ONU refere-se justamente ao trabalho sobre Crimes Cibernéticos que vem sendo desenvolvido na Comissão sobre Prevenção ao Crime e Justiça Criminal, visto que decorre das conclusões do Décimo-Segundo Congresso das Nações Unidas sobre Prevenção ao Crime e Justiça Criminal, realizado em 2010 no Brasil, consubstanciadas na Declaração de Salvador. Cabe uma crítica à menção ao médio prazo para a construção do marco internacional, em face da urgência da

---

[332] Nesse sentido ver a documento de metodologia, disponível em: <http://www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/Working_Papers/Methodology_timeline_REV-7.pdf>. Acesso em 24/02/2011.

[333] Texto completo do documento de trabalho, incluindo a descrição detalhada de cada tópico do estudo, disponível em: <http://www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/Working_Papers/UNODC_CCPCJ_EG4_2011_2_rev1_-_amended_-_final.pdf>. Acesso em 24/02/2011.

[334] BRASIL. Presidência da República, *Livro*, p. 45.

[335] Grifo nosso.

temática e da facilidade com que o estudo pode tornar-se desatualizado e obsoleto, decorrente da evolução tecnológica inerente ao tema. Recorda-se aqui que a desatualização da Convenção e Budapeste pelos avanços tecnológicos é um dos argumentos relacionados na publicação do DSIC, "Livro Verde: segurança cibernética no Brasil", para justificar a necessidade de um tratado internacional[336]. O período de três anos, prazo classificado como meta de curto prazo, parece ser um bastante razoável para a negociação de uma convenção no plano internacional, sendo que a análise final do estudo conduzido pelo Grupo de *Experts* está marcada para abril de 2013, o qual será o ano emblemático para uma decisão da comunidade internacional com relação ao marco dos crimes cibernéticos.

Desta forma, existe a possibilidade concreta que o estudo aprofundado acabe por impulsionar o nascimento de um instrumento internacional entre os Estados interessados no seio do Sistema das Nações Unidas, mais especificamente no âmbito da Comissão sobre Prevenção ao Crime e Justiça Criminal do Conselho Econômico e Social e da UNODC, tendo o Brasil como um dos países protagonistas da discussão e negociação.

B: OUTRAS ORGANIZAÇÕES

B.1 Conselho da Europa

O Conselho da Europa (*Council of Europe* - COE)[337] foi fundado em 5 de maio de 1949 pela união de dez países[338] e, atualmente, é formado por 47 Estados-Membros[339],

[336] BRASIL. Presidência da República, *Livro*, p. 23.
[337] Informações obtidas na página oficial da organização na Internet, disponível em: <http://www.coe.int/about Coe/ index.asp?page=quisommesnous&l=en>. Acesso em: 21/01/2010.
[338] Países fundadores: Bélgica, Dinamarca, França, Itália, Irlanda, Luxemburgo, Noruega, Países Baixos, Reino Unido e Suécia.
[339] Os 37 países restantes e suas respectivas datas de adesão ao Conselho são: Grécia (9 de agosto de 1949), Turquia (9 de agosto de 1949), Islândia (9 de março de 1950), Alemanha Ocidental (13 de julho de 1950), Áustria (16 de abril de 1956), Chipre (24 de maio de 1961), Suíça (6 de maio de 1963), Malta (29 de abril de 1965), Portugal (22 de setembro de 1976), Espanha (24 de novembro de 1977), Liechtenstein (23 de novembro de 1978), São Marinho (16 de novembro de 1988), Finlândia (5 de maio de 1989), Hungria (6 de novembro de 1990), Polónia (26 de novembro de 1991), Bulgária (7 de maio de 1992), Estônia (14 de maio de 1993), Lituânia (14 de maio de 1993), Eslovênia (14 de maio de 1993), República Tcheca (30 de junho de 1993), Eslováquia (30 de junho de 1993), Romênia (7 de outubro de 1993), Andorra (10 de outubro de 1994), Letônia (10 de fevereiro de 1995), Albânia (13 de julho de 1995), Moldávia (13 de julho de 1995), Macedónia (9 de novembro de 1995), Ucrânia (9 de novembro de 1995), Rússia (28 de fevereiro de 1996), Croácia (6 de novembro de 1996), Geórgia (27 de abril de 1999), Arménia (25 de janeiro de 2001), Azerbaijão (25 de janeiro de 2001), Bósnia e Herzegovina (24 de abril de 2002), Sérvia (3 de abril de 2003), Mónaco (5 de outubro de 2004) e Montenegro

correspondendo a quase a totalidade dos países do continente europeu. A organização, com sede em Estrasburgo na França, tem por finalidade o desenvolvimento de Princípios Comuns e Democráticos pela Europa, baseados na Convenção Européia dos Direitos Humanos e outros textos de referência na proteção dos indivíduos[340]. Não se confunde com a União Européia (organização supranacional) nem com o Conselho Europeu, órgão daquela que reúne Chefes de Estados ou de Governo dos Estados-Membros, para o planejamento da política da União[341]. Cabe mencionar que todos os países que formam a União Européia integram o Conselho da Europa, que concedeu o *status* de Membros Observadores aos Estados Unidos, Canadá, Japão, México e Santa Sé[342].

No âmbito do Conselho da Europa foi gestada a Convenção sobre Crimes Cibernéticos (*Council of Europe Convention on Cybercrime*), Convenção n.° 185[343], assinada em Budapeste, na Hungria, em 23 de novembro de 2001, contando com a adesão de 47 países[344], dos quais 32 já a ratificaram[345]. Sua vigência iniciou em 1° de julho de 2004 com sua ratificação por 5 países, incluindo 3 países membros do Conselho da Europa. Além dos membros deste, outros 4 países que não são membros assinaram a Convenção, quais sejam, Canadá, Japão, África do Sul e Estados Unidos, sendo que apenas os Estados Unidos já ratificaram o tratado. Cumpre relembrar que Canadá, Japão e Estados Unidos têm *status* de Membros Observadores. Keyser[346] lembra que até a adoção da Convenção pelo Comitê de Ministros em 8 de novembro de 2001, na sua 109° Sessão, foram 4 anos de trabalho e 27 minutas.

Finkelstein[347] salienta que a Convenção de Budapeste é o maior esforço no âmbito internacional para a repressão dos crimes cibernéticos. E. L. L. Ferreira[348] contextualiza a

---

(11 de maio de 2007). Nesse sentido ver: <http://pt.wikipedia.org/wiki/Conselho_da_Europa>. Acesso em: 22/01/2010. O único país da Europa que não é membro do Conselho é a Bielorrússia.

[340] Nesse sentido, ver <http://www.coe.int/about Coe/ index.asp?page=quisommesnous&l=en>. Acesso em: 21/ 01/2010.

[341] Nesse sentido, ver <http://www.coe.int/aboutcoe/index.asp?page=nepasconfondre&l=en>. Acesso em: 02/02/ 2010.

[342] Nesse sentido, ver < http://www.coe.int/aboutcoe/index.asp?page=leSaviezVous#peine>. Acesso em: 21/01/ 2010.

[343] Texto oficial da Convenção pode ser consultado em: <http://conventions.coe.int/Treaty/en/Treaties/Html/185 .htm>.

[344] África do Sul, Albânia, Alemanha, Armênia, Áustria, Azerbaijão, Bélgica, Bósnia Herzegovina, Bulgária, Canadá, Croácia, Chipre, Dinamarca, Eslováquia, Eslovênia, Espanha, Estados Unidos, Estônia, Finlândia, França, Geórgia, Grã-Bretanha, Grécia, Groelândia, Holanda, Hungria, Irlanda, Itália, Japão, Letônia, Liechtenstein, Lituânia, Luxemburgo, Macedônia, Malta, Moldávia, Montenegro, Noruega, Polônia, Portugal, República Checa, Romênia, Sérvia, Suécia, Suíça, Turquia e Ucrânia.

[345] Informações sobre adesão ao tratado e seu status disponíveis em: <http://conventions.coe.int/Treaty/ Commun/ChercheSig.asp?NT=185&CM=1&DF=13/03/2012&CL=ENG>. Acesso em: 13/03/2012.

[346] KEYSER, Op. Cit., p. 296.

[347] FINKELSTEIN, Op. Cit., p. 429.

[348] FERREIRA, Érica, *Internet*, p. 118.

Convenção, lembrando que foi editada logo após os incidentes terroristas de 11 de setembro de 2001. Na mesma linha, Gercke[349] defende que além da Resolução n° 63, aprovada na 55° Sessão da Assembléia Geral das Nações Unidas em 4 de dezembro de 2000[350], a Convenção do COE é o único arcabouço legislativo internacional complexo e que foi desenhado desde o início para ser uma convenção internacional. Para o autor, sua importância não pode ser limitada ao número de assinaturas ou ratificações, na medida em que muitos países, como Argentina, Paquistão, Egito, Filipinas e Nigéria, ainda que não tenham aderido à Convenção, utilizaram suas disposições para atualizar suas legislações nacionais[351].

A Convenção é baseada em diversas premissas que são mencionadas expressamente no preâmbulo, dentre as quais se destacam necessidade de uma política criminal comum a fim de proteger a sociedade da criminalidade no ciberespaço; conscientização das profundas mudanças provocadas pela digitalização, pela convergência e pela globalização permanente das redes informáticas; preocupação com o risco de que as redes informáticas sejam utilizadas para a prática de infrações criminais, assim como de que as provas dessas infrações sejam por elas disseminadas; reconhecimento da necessidade de cooperação entre estados e o setor privado para o combate desse tipo de criminalidade, especialmente, destacando a imprescindibilidade de se preservar os interesses legítimos ligados ao uso e desenvolvimento das TICs; rápida e eficaz cooperação internacional em matéria penal como um imperativo para uma luta efetiva contra a criminalidade cibernética; necessidade da convenção para impedir atos contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de rede e dados informáticos, bem como sua utilização fraudulenta; necessidade de garantir um equilíbrio adequado entre os interesses de aplicação da lei e o respeito aos direitos fundamentais; esforços internacionais, notadamente da Organização das Nações Unidas (ONU)[352], da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) e do G8[353].

E. L. L. Ferreira[354] identifica na Convenção de Budapeste, no seu preâmbulo, o bem jurídico tutelado pelos crimes cibernéticos. Explica a autora[355]:

---

[349] GERCKE, Op. Cit. p. 11-12.
[350] Resolução n.° 55/63, "Combatendo o Uso Criminoso das Tecnologias de Informação". Texto disponível em: <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N00/563/17/PDF/N0056317.pdf?_OpenElement>. Acesso em: 25/03/2011.
[351] GERCKE, Op. Cit. p. 12.
[352] Resoluções da Assembléia Geral n.° 53/70, 54/49, 55/28, 55/63, 56/19, 56/121, 57/53, 57/239 e 58/199.
[353] Grupos dos 7 países mais desenvolvidos do mundo mais Rússia.
[354] FERREIRA, Érica, *Internet*, p. 175.
[355] Id., *Internet*, p. 175.

> Pela Convenção de Cibercrime a Segurança Informática é o bem jurídico penal a ser protegido, considerando a reunião de três elementos: a integridade, a disponibilidade, e a confidencialidade. Com a característica de ser permanente. Nessa esteira, ainda que não haja consenso, existe um denominador comum no sentido de que a informação, inicialmente, seria o bem jurídico a ser protegido pelo Direito Penal e sua natureza jurídica é difusa, eis que atinge indeterminado número de pessoas e pode gerar conflito entre elas, grupo e/ou empresas, de forma recíproca e variada, sendo que todos possuem legítimos interesses de uso e fruição das tecnologias disponibilizadas pela Internet.

Assim como E. L. L. Ferreira, Rossini[356] também indica que a segurança informática é o bem jurídico tutelado pela Convenção, ressaltando que será permanente e autônomo, existindo sempre quando a conduta criminosa for cometida do ambiente de rede, "independentemente do bem jurídico 'original' que o tipo penal tradicional busca proteger".

Este Tratado Internacional contempla uma parte terminológica em que apresenta definições; outra parte, de direito penal material, na qual cabe a cada Estado Parte tomar as medidas cabíveis para adequar sua legislação interna quando pertinente, ou seja, a parte da convenção que dispõe sobre a tipificação dos crimes cibernéticos propriamente ditos; uma outra parte relacionada ao direito processual penal e, finalmente, a parte que diz respeito à cooperação internacional, além das disposições sobre adesão, assinatura, reservas etc.

Finkelstein[357] descreve que o documento teceu diretrizes no intuito de que as evidências dos crimes cibernéticos sejam aceitas perante a Justiça, com objetivo de reprimir esta criminalidade. Segundo a autora[358], "é disposição desta convenção que arquivos eletrônicos, registros de visitas a sites ou mesmos documentos eletrônicos devem passar a ser aceitos como prova de ocorrência de crime eletrônico".

Inicialmente, a Convenção apresenta alguns conceitos no seu art. 1°, a fim de viabilizar a correta interpretação do documento. Para tanto, define sistema informático[359], dados informáticos[360], fornecedor de serviço e dados de tráfego.

No aspecto de direito penal material, são previstas para criminalização pelos ordenamentos nacionais as seguintes infrações: acesso ilegítimo (art. 2°), interceptação ilegítima (art. 3°), interferência em dados (art. 4°), interferência em sistemas (art. 5°), uso

---

[356] ROSSINI, Op. Cit., p. 35.
[357] FINKELSTEIN, Op. Cit., p. 430.
[358] Id., Op. Cit., p. 430.
[359] Art. 1°, a) "Sistema informático' significa qualquer dispositivo isolado ou grupo de dispositivos relacionados ou interligados, em que um ou mais de entre eles, desenvolve, em execução de um programa, o tratamento automatizado dos dados".
[360] Art. 1°, b) "Dados informáticos' significa qualquer representação de fatos, informações ou de conceitos sob uma forma suscetível de processamento num sistema de computadores, incluindo um programa, apto a fazer um sistema informático executar uma função".

abusivo de dispositivos (art. 6°), falsidade informática (art. 7°), estelionato informático (art. 8°), pornografia infantil envolvendo o uso de sistema informático (art. 9°) e violação de direito do autor e direitos conexos (art. 10). A Convenção também prevê a criminalização da tentativa e da cumplicidade (art. 11). Ao longo do texto existe a expressa menção à possibilidade de adoção de reservas por parte dos países signatários, quando da assinatura do tratado.

Referindo-se a esta parte de direito penal substantivo, Rossini[361] destaca que a Convenção sugere a criação do tipo incriminador, mas não recomenda propriamente a sua redação, fato que permite o respeito às características de cada país signatário.

Cabe menção ao fato da Convenção instituir a responsabilização de pessoa jurídica no artigo 12, ressalvando no subitem 3, que cada Estado-Membro escolherá se a responsabilidade se dará no âmbito civil, penal ou administrativo. Neste ponto, Rossini[362]defende a necessidade da quebra do paradigma de que a empresa não tem capacidade de delinquir, ainda que seja necessária a edição de Emenda Constitucional, a fim de permitir que empresas possam ser responsabilizadas, criminalmente, no Sistema Penal Brasileiro[363;364].

Já em relação ao direito processual, estipula diversos institutos: conservação rápida de dados informáticos armazenados; conservação rápida e divulgação parcial de tráfego; busca e apreensão de dados informáticos armazenados; fornecimento de dados; recolhimento em tempo real de dados relativos ao tráfego; interceptação de dados relativos ao conteúdo e jurisdição. Faz-se uma ressalva quanto ao disposto no art. 16, que trata da conservação de dados informáticos e que no seu item 2, determina o prazo máximo de 90 dias, prorrogável, para a conservação e preservação da integridade destes dados, contados da expedição de ordem judicial que obrigue a sua conservação (art. 18). Este prazo não pode ser confundido com o prazo que os provedores de acesso devem conservar os *logs*, ainda não regulamentado no Brasil mas, que na União Européia, por força da Diretiva 2006/24/CE, fica entre 6 meses e 2 anos, consoante Finkelstein[365]. Recorda-se, neste ponto, que o celeumático PL n.° 84/1999 prevê o prazo de três anos, o que é irrazoável na opinião dos provedores em face dos vultosos

[361] ROSSINI, Op. Cit., p. 43.
[362] Id., Op. Cit., p. 83.
[363] Id., Op. Cit., p. 96.
[364] Sobre as razões pelas quais o autor defende a responsabilidade penal das pessoas jurídicas, ver ROSSONI, Op. Cit., p. 83-99.
[365] FINKELSTEIN, Op. Cit., p. 431.

custos gerados[366]; e que o texto do Marco Civil da Internet, PL n.° 2.126/2011, estabelece o prazo de 1 ano[367].

O Tratado também estabelece as bases para a Cooperação Internacional nessa matéria, dispondo sobre os princípios gerais relativos à cooperação internacional, à extradição e ao auxílio mútuo; a informação espontânea, os procedimentos relativos aos pedidos de auxílio mútuo na ausência de acordos internacionais aplicáveis; as disposições específicas sobre o auxílio mútuo em matéria de medidas cautelares e em matéria de poderes de investigação; e participação na Rede 24/7[368].

A parte final do texto apresenta normas referentes à assinatura, à vigência, à adesão, à aplicação territorial, às reservas e à denúncia da Convenção, dentre outras.

E. L. L. Ferreira[369] cita o exame da Convenção efetuada por Rossini[370], nos seguintes termos:

> Augusto Eduardo de Souza Rossini, ao analisar os termos da Convenção, pontuou alguns tópicos, dentre eles, o fato da conduta dolosa ser a regra, não existindo qualquer referência às modalidades culposas (negligência, imprudência ou imperícia) e a sugestão da responsabilização dos atos preparatórios, circunstâncias já presentes no ordenamento nacional, a exemplo do crime de formação de quadrilha. Destaca, ainda, a importância que se dá à proteção de dados verdadeiros, bem como, à pornografia infantil, cujo art. 9° incluiu os verbos "oferecer" ou "disponibilizar" eleito como um dos grandes avanços da Convenção, pois *abarcam condutas realizadas dentro e fora da rede, em páginas abertas ou através de* ***e-mails***.

Conforme já observado no item B da Parte I, o Brasil, desde o final do ano de 2008, já possui tipificadas diversas condutas relacionadas às práticas de pedofilia e pornografia infantil, cometidas através das TICs, essencialmente da Internet.

Voltando ao exame do tratado, E. L. L. Ferreira[371], ao analisar o art. 22 da Convenção, que prescreve as normas relativas à jurisdição, entende que "o sistema brasileiro harmoniza-se plenamente com a Convenção, restando agora apenas aguardar que seja subscrita pelo país". Ainda debruçada sobre o tema, a autora[372] defende que a maioria das condutas previstas para criminalização já se encontra tipificada no Direito Brasileiro, sendo necessárias algumas

---

[366] SAFERNET BRASIL. Observatório do Congresso Nacional: o PL do Sen. Eduardo Azeredo e a Convenção contra o Cibercrime. Disponível em: <http://www.safernet.org.br/twiki/bin/view/Colaborar/PLSAzeredoXConvencao_Cibercrime>. Acesso em: 25/07/2009.
[367] Art. 11 do PL 2.126/2011.
[368] Rede criada no âmbito do G8 que exige dos países aderentes a indicação de um ponto de contato disponível 24 horas, 7 dias por semana, para o recebimento de informações e/ou pedido de cooperação, relativos a casos que envolvam evidências eletrônicas, da qual o Brasil faz parte, sendo a Polícia Federal o contato.
[369] FERREIRA, Érica, *Internet*, p. 166.
[370] Apud FERREIRA, Érica, *Internet*, p. 166.
[371] FERREIRA, Érica, *Internet*, p. 167.
[372] Id., *Internet*, p. 177.

adequações, *v.g*., a equiparação legal do conceito de coisa ao conceito de documento digital. Na mesma esteira, Rossini[373] afirma:

> A maioria das sugestões constantes da seção de direito material da Convenção de Budapeste já está tipificada no Brasil, restando poucas adaptações a permitir que o país possa assiná-la. Estas adequações podem ser feitas por equiparações legais, conforme já acontece com alguns institutos de Direito Penal, merecendo especial atenção aos conceitos de coisa e documento digitais, atualmente lacunas no ordenamento, a permitir que, respectivamente, alguns delitos patrimoniais e de falsificação tradicionais possam abarcar condutas praticadas em ambiente informático.

Uma das críticas mais contundentes ao tratado é que não assegura a preservação do direito fundamental à privacidade, cabendo a ressalva de que cada país aderente deve implementar as disposições de acordo com as regras e os princípios vigentes para o seu ordenamento, determinando, por exemplo, a necessidade de autorização judicial para conservação de dados, busca e apreensão de dados, interceptação de dados, enfim, para todos os institutos que provoquem quebra de sigilo.

Nessa linha, Rustad[374] reforça que os críticos reclamam que à Convenção falta equilíbrio, concedendo muito poder aos órgãos de segurança pública em detrimento das liberdades civis, ressaltando que o equilíbrio entre a privacidade e a aplicação da lei é ainda mais difícil, considerando-se que os países signatários divergem radicalmente no tocante aos direitos e liberdades fundamentais. O autor ainda explica que poucos questionam a necessidade de algum tipo de tratado, sendo que a oposição à Convenção é essencialmente formada pelo setor privado (larga variedade de interesses das indústrias e dos provedores de serviço da Internet), que busca um regime global mínimo[375].

Questiona-se a possibilidade de adesão pelo Brasil à Convenção, cuja análise ficou sob a responsabilidade da Coordenação-Geral de Combates aos Ilícitos Transnacionais do Ministério das Relações Exteriores. Sobre o assunto, Lucero[376] afirma com propriedade:

> Examinada à luz do direito pátrio, em grupo de trabalho sob coordenação do Itamaraty, ao longo de 2008 e 2009, a Convenção de Budapeste não logrou consenso entre os órgãos consultados por conta de dificuldades na internalização de alguns dispositivos do documento, notadamente sobre compromissos internacionais na área de propriedade intelectual dos quais o Brasil não é parte, e aos quais a Convenção não oferece a possibilidade de

---

[373] ROSSINI, Op. Cit., p. 248.
[374] Id., Op. Cit., p. 96.
[375] Id., Op. Cit., p. 96.
[376] LUCERO, Everton. Governança de Internet: aspectos da formação de um regime global e oportunidades para a ação diplomática. Brasília: Fundação Alexandre Gusmão, 2011. 236 p. p. 142. Disponível em: <http://www.funag.gov.br/biblioteca/index.php?option=com_docman&task=_doc_details&gid=89&Itemid=41>. Acesso em: 25/08/2011.

> fazer reserva. Na avaliação do Governo brasileiro, não parecem promissoras as perspectivas de sucesso das tentativas do Conselho da Europa e Partes Contratantes da Convenção de afirmá-la como diploma universal sobre o assunto.

Vislumbra-se que além dos obstáculos supracitados, existe uma dificuldade diplomática que reside no fato do Brasil, ao contrário de outros países como os Estados Unidos, Japão, Canadá e África do Sul, não ter sido chamado para participar das negociações iniciais para a celebração do tratado.

Cabe a ressalva da grande pressão exercida pelos países que assinaram e/ou ratificaram a convenção e pelo próprio Conselho da Europa para que outros países também adiram à Convenção. No entanto, o fato é que nenhum país em desenvolvimento da América Latina e da Ásia foi convidado a negociar seus termos e agora esses países se vêem compelidos a assinarem tal tratado. Ademais, referente ao Continente Africano, somente a África do Sul participou. Neste sentido, as discussões realizadas nos Fóruns de Governança da Internet, Fórum das Nações Unidas criado para a discussão aberta, democrática e plural de tópicos essenciais à regulação da Internet, como recursos críticos de Internet (infraestrutura), abertura, acesso e segurança, em atendimento ao mandato contido no artigo 72 da Agenda de Túnis para a Sociedade da Informação[377], convergiram para a idéia de que a adesão à Convenção de Budapeste seria a única alternativa viável no combate a esta criminalidade, visto ser o único documento juridicamente vinculante[378]. Além disso, ao ser levantada a possibilidade de negociação de um tratado com todos os países interessados, a idéia foi rechaçada pelo fato de que seria um processo extremamente longo, de que países que já

---

[377] Artigo 72 da Agenda de Túnis para a Sociedade da Informação: "*We ask the UN Secretary-General, in an open and inclusive process, to convene, by the second quarter of 2006, a meeting of the new forum for multi-stakeholder policy dialogue—called the Internet Governance Forum (IGF). The mandate of the Forum includes inter alia to: a. Discuss public policy issues related to key elements of Internet governance in order to foster the sustainability, robustness, security, stability and development of the Internet…*". Texto completo disponível em: < http://www.itu.int/wsis/docs2/tunis/off/6rev1.html>.

[378] Nesse sentido, ver a transcrição do Workshop 23 - *Cybercrime Common Standards and the Joint Action,* organizado pelo Conselho da Europa no V IGF realizado em Vilnius, na Lituânia em setembro de 2010, no qual um representante do COE manifestou-se da seguinte forma: *"Our main arguments are that the key tools and instruments to cope with [c]ybercrime are already available, doesn't mean that some more won't be developed but the body is available and the core problem is that these instruments are not necessarily implemented all over the world, and therefore, we need to see how can we overcome this core problem*". Outra intervenção de outro representate destacou: "*The only exception is Europe, and Europe in June [sic] legislation is binding and the problem is [that] [c]ybercrime, is global and it's not limited only with[in] all those 27 member states. That's why I would like to stress that right now[:] there is one existing instrument and the number of parties to the convention is quite low, implementation level is quite poor but the states can improve that situation and they can join the convention*". A transcrição complete do workshop está disponível em: <http://www.intgovforum.org/cms/component/content/article/102-transcripts2010/735-23>. Acesso em: 18/12/2010.

possuem legislação precisariam adequá-las ao novo texto e de que países em processo de aprovar suas legislações poderiam paralisar o seu trâmite em face da notícia[379].

Na edição do Fórum de Governança da Internet (IGF) em 2010, a delegação brasileira defendeu que a Convenção sobre Crimes Cibernéticos seria uma iniciativa regional e como tal, deveria alimentar um processo internacional de negociação em que todos os interessados pudessem participar[380].

Traz-se à colação as conclusões sobre a Convenção contidas na recente publicação de 2010, "Livro Verde: segurança cibernética no Brasil", do Departamento de Segurança da Informação e Comunicações (DSIC) do Gabinete de Segurança Institucional da Presidência da República[381]:

> Finalmente, **destaca-se a importância para o país de construir as bases para o entendimento internacional sobre a segurança cibernética, especialmente sobre crime cibernético, o quanto antes, e contando com a maior participação de órgãos possível. Já é entendido por vários países que, atualmente, a Convenção de Budapeste não atende as exigências atuais de crimes cibernéticos, dado os avanços tecnológicos ocorridos e tampouco é suficiente em termos da cooperação internacional**. Assim, como resultado da Convenção do Crime Cibernético, ocorrida no ano de 2010, em Salvador/Brasil, foi emitida Declaração, consensada pelos 158 países sobre tal aspecto, o que abriu a oportunidade de criação de grupo para tratar globalmente a matéria - crime cibernético. Existe, portanto, proposta em andamento de uma nova Convenção, de caráter global, a qual teria como ponto de partida, a cooperação no âmbito dos BRICS (Brasil, Rússia, Índia, China e África do Sul)[382].

Deve-se ainda ressalvar uma peculiaridade quanto à possibilidade de adesão de outros Estados que não são membros, pois ainda que seja a iniciativa regional de maior abrangência, a adesão destes países fica sujeita ao convite do Comitê de Ministros do Conselho da Europa, após a consulta e obtenção de consenso unânime dos países contratantes da convenção,

---

[379] VELASCO, Cristos; CRAVO, Vanessa. The Status of Cybercrime in Mexico, Brazil and the Outcome on Cybercrime and Security of the Fifth Meeting of the Internet Governance Forum, *Revista de Contratación Electrónica*, n. 113, maio 2011, p. 25-38. Disponível em: <http://libros-revistas-derecho.vlex.es/vid/cybercrime-mexico-governance-322030959>. Acesso em: 18/10/2011.

[380] Manifestação de integrante da delegação brasileira no V IGF realizado em Vilnius, na Lituânia, em setembro de 2010, na sessão principal sobre segurança, abertura e privacidade, nos seguintes termos: "*In the last 10 or 15 years, we have seen many regional or specific initiatives towards the question of security and the Internet, mainly of them the [sic] initiatives from [the] industry [sector], from the Convention of Europe, Budapest Convention, law enforcement initiatives and is [sic] so on. We understand these are all valuable contributions but they must feed international consultation process where all stakeholders, all [g]overnments, private sector, [c]ivil [s]ociety, can participate and write the principles and mechanisms within their own capacity towards a secure Internet. This approach of international participation is very important […]*." Texto complete da transcrição da sessão disponível em: <http://www.intgovforum.org/cms/component/ content/article/102-transcripts2010/658-sop>. Acesso em: 18/12/2010.

[381] BRASIL. Presidência da República, *Livro*, p. 23-24.

[382] Grifo nosso.

consoante art. 37, parágrafo 1°[383]. Dessa maneira, existe uma limitação à ampla participação de Estados Não Membros do COE, os quais devem submeter-se a um processo de consulta e aprovação, antes de serem convidados a aderir[384].

Stein e Ghernaouti-Helie[385] sustentam que a Convenção é um marco no combate aos crimes cibernéticos, porém é baseada em condutas do final dos anos '90, sendo que novos métodos devem ser cobertos pelas leis criminais, tais como *phishing, spam*, roubo de identidade, terrorismo cibernético, ataque às ICI, dentre outras e que mesmo a terminologia não era necessariamente adequada para 2010. Ademais os autores relembram que a Convenção não atingiu um nível de aceitação nas outras regiões e países, salientando que, para as outras regiões globais, a Convenção de Budapeste continua sendo e sempre será uma convenção européia[386].

Cabe ressaltar ainda que os autores defendem um tratado ou um conjunto de tratados no âmbito das Nações Unidas dedicado ao espaço cibernético como proposta global para esta década, abordando segurança cibernética, crimes cibernéticos e outras ameaças cibernéticas como um arcabouço para a paz, segurança e justiça neste ambiente, o qual representa um quinto domínio comum, ao lado da terra, mar, ar e espaço sideral[387].

Ainda que nenhum país na América Latina tenha participado das negociações e tenha aderido à Convenção até a presente data, quatro países latino-americanos já foram

---

[383] *Article 37 – Accession to the Convention. 1After 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*. Texto completo da Convenção disponível em: <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>. Acesso em: 11/03/2011.

[384] Nesse sentido ver as observações do Documento de trabalho elaborado pela Secretaria do Escritório das Nações Unidas sobre Drogas e Crime em preparação para o Décimo-Segundo Congresso das Nações Unidas sobre Prevenção ao Crime e Justiça Criminal, realizado em Salvador, no Brasil, de 12 a 19 de abril de 2010 , disponível em: <http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_9/V1050382e.pdf>. Acesso em: 23/02/2011. p. 11-12. O Documento também alerta que por força do art. 44 da Convenção, a possibilidade dos Estados Não Membros de proporem amendas é restrita.

[385] STEIN, Schojolberg; GHERNAOUTI-HELIE, Solange. *Global Treaty on Cybersecurity and Cybercrime*. 2 ed. 2011. 97 p. p. *i-ii.* Disponível em: <http://www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf>. Acesso em: 10/05/2011. O trabalho propõe uma minuta de tratado global sobre segurança cibernética, crimes cibernéticos e outras ameaças cibernéticas, abarcando medidas de direto penal material, descrevendo as condutas que devem ser tipificadas; medidas de direito processual para investigação e persecução penal; e medidas de jurisdição global. Por fim ainda apresenta na sua segunda parte medidas de segurança cibernética.

[386] STEIN, Schojolberg; GHERNAOUTI-HELIE, Solange. Op. Cit., p. *ii.*

[387] Id., Op. Cit., p. *ii.*

convidados: Costa Rica, Chile, México e República Dominicana. Além deles, a Argentina, formalmente, já solicitou a sua adesão[388].

Nota-se que a Convenção sobre Crimes Cibernéticos do Conselho da Europa possui uma Convenção derivada, chamada de Protocolo Adicional à Convenção sobre Crimes Cibernéticos Relativo à Criminalização de Atos de Natureza Racista e Xenófoba Cometidos através de Sistemas Informáticos.

Nesse contexto, a Europa, berço do nazismo, sempre demonstrou grande preocupação em relação a essa forma de discriminação exacerbada pela crescente xenofobia contra os imigrantes, experimentada nas últimas décadas.

Com a evolução das TICs, em especial a Internet, observa-se um novo campo em que a discriminação, incluindo a racial, tem sido propagada, até mesmo, em decorrência das características próprias dos crimes cibernéticos (dificuldade de comprovação e de rastreamento), exigindo, assim, novos mecanismos de proteção contra a discriminação e de repressão a estas práticas.

Dessa maneira foi concebido o Protocolo Adicional, Convenção do Conselho da Europa n.° 189[389]; assinada em Estrasburgo, na França, em 28 de janeiro de 2003. Conta com 35 países signatários[390], dos quais 20 já ratificaram a Convenção[391]. O início da vigência data de 1° de março de 2006, com a ratificação por 5 países. Além de membros do Conselho da Europa, Canadá e África do Sul assinaram, mas ainda não a ratificaram. Os Estados Unidos já declararam que não assinarão o Protocolo Aditivo em face da 1° Emenda, que garante liberdade de expressão.

É permitida a adesão de qualquer Estado que tenha aderido à Convenção sobre Crimes Cibernéticos, sendo que a vigência para Estados que expressem consentimento ulterior dar-se-á no primeiro dia do mês seguinte ao termo de um período de 3 meses, a contar do depósito do instrumento.

As premissas do Protocolo são liberdade e igualdade em dignidade e direitos de todas as pessoas; necessidade de garantir integral e eficaz implementação dos direitos humanos sem discriminação; caracterização dos atos de natureza racista e xenófoba como uma violação aos

---

[388] Nesse sentido ver a nota de rodapé n.° 47 de VELASCO, Cristos; CRAVO, Vanessa, Op. Cit., p. 16.
[389] Texto oficial da Convenção pode ser consultado em: < http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm>.
[390] Africa do Sul, Albânia, Alemanha, Armênia, Áustria, Bélgica, Bósnia Herzegovina, Canadá, Croácia, Chipre, Dinamarca, Eslovênia, Estônia, Finlândia, França, Grécia, Groelândia, Holanda, Itália, Letônia, Liechtenstein, Lituânia, Luxemburgo, Macedônia, Malta, Moldávia, Montenegro, Noruega, Polônia, Portugal, Romênia, Sérvia, Suécia, Suíça, Ucrânia.
[391] Informações sobre adesão ao tratado e seu status disponíveis em: <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=189&CM=1&DF=13/03/2012&CL=ENG>. Acesso em 13/03/2012.

direitos humanos e uma ameaça ao Estado de Direito e à estabilidade democrática; a necessidade dos ordenamentos jurídicos nacionais e internacionais disporem de respostas jurídicas adequadas à propaganda racista e xenófoba praticada através de sistemas informáticos; previsão de meios modernos e flexíveis de cooperação internacional na Convenção sobre Crimes Cibernéticos; necessidade de harmonizar as disposições de direito material relativas à luta contra a propaganda racista e xenófoba; risco do uso indevido dos sistemas informáticos para efeitos de difusão de propaganda racista e xenófoba; necessidade de garantir equilíbrio adequado entre liberdade de expressão e luta eficaz contra atos de natureza racista e xenófoba; observância aos instrumentos jurídicos internacionais, em especial a Convenção Internacional das Nações Unidas sobre a Eliminação de Todas as Formas de Discriminação Racial e complementaridade em relação à Convenção sobre Crimes Cibernéticos.

Partindo-se para a análise do Protocolo, no art. 2° está definido o conceito de material racista e xenófobo, essencial para a compreensão das condutas previstas para criminalização, que se transcreve abaixo:

> qualquer material escrito, imagem ou outra representação de idéias e teorias que preconize ou encoraje o ódio, a discriminação ou a violência contra qualquer pessoa ou grupo de pessoas, em função da sua raça, cor, ascendência ou origem nacional ou étnica, ou ainda da sua religião, na medida em que sirva de pretexto a qualquer um dos outros elementos ou incite à prática de tais atos.

O Protocolo estipula os seguintes comportamentos para criminalização pelos ordenamentos nacionais: difusão de material racista e xenófobo através de sistemas informáticos; ameaça com motivação racista e xenófoba; insulto com motivação racista e xenófoba; negação, minimização grosseira, aprovação ou justificação do genocídio ou de crimes contra a humanidade; auxílio e cumplicidade; e também relata as possibilidades de reservas.

O crime de difusão de material racista e xenófobo através de sistemas informáticos reprime a difusão ou outras formas de colocação à disposição do público, de forma intencional, através de sistema informático, de material racista e xenófobo (art. 3°, 1).

O crime de ameaça com motivação racista e xenófoba é caracterizado pela ameaça, intencional e ilegítima, através de sistema informático, de cometimento de crime grave, conforme definido pelo ordenamento interno, contra uma pessoa ou grupo de pessoas por pertencerem a um grupo que se caracterize por sua raça, cor, ascendência ou origem nacional

ou étnica, ou ainda, por sua religião, na medida em que sirva de pretexto a qualquer um dos outros elementos (art. 4°).

Configura o delito de insulto com motivação racista e xenófoba, o insulto, intencional e ilegítimo, através de sistema informático, dirigido a uma pessoa ou a um grupo de pessoas por pertencerem a um grupo que se caracterize por sua raça, cor, ascendência ou origem nacional ou étnica, ou ainda, por sua religião, na medida em que sirva de pretexto a qualquer um dos outros elementos (art. 5°, 1).

Já a negação, minimização grosseira, aprovação ou justificação do genocídio ou dos crimes contra a humanidade concretiza-se pela difusão ou outras formas de colocação à disposição do público, de forma intencional e ilegítima, através de sistema informático, de material que negue, minimize de forma grosseira, aprove ou justifique atos de genocídio ou de crimes contra a humanidade, conforme definidos pelo direito internacional e reconhecidos como tal por uma decisão definitiva emanada do Tribunal Militar Internacional, estabelecido pelo Acordo de Londres, de 8 de agosto de 1945, ou qualquer outro tribunal internacional estabelecido por instrumentos internacionais pertinentes e cuja competência tenha sido reconhecida pela Parte interessada (art. 6°, 2).

O Protocolo também prescreve a criminalização do auxílio e da cumplicidade, considerados como o auxílio para a prática ou a ação, como cúmplice, visando à prática efetiva, de forma intencional e ilegítima, de crime definido no protocolo (art. 7°). Além disso, fixa a possibilidade de reservas, no sentido de limitar alguns tipos à promoção ou incitação à discriminação associada ao ódio ou violência (para as condutas previstas no art. 3°, 1; art .6°, 1, quais sejam, a difusão de material racista e xenófobo através de sistemas informáticos e a negação, minimização grosseira, aprovação ou justificação do genocídio ou dos crimes contra a humanidade) e à exposição ao ódio, ao desprezo e ao ridículo (art. 5°, 1- insulto com motivação racista e xenófoba).

A utilização da rede mundial de computadores como veículo da prática de atos racistas e xenófobos não é uma realidade vivenciada somente na Europa. A SaferNet Brasil[392] recebeu no período de 1° de janeiro de 2006 a 1° de abril de 2011, 37.244 denúncias classificadas como racismo ou xenofobia; 21.247 denúncias classificadas como neonazismo e 16.784

[392] A SaferNet Brasil é uma associação civil de direito privado, com atuação nacional, sem fins lucrativos, fundada em 20 de dezembro de 2005, referência no combate aos crimes e violações aos Direitos Humanos na Internet. Possui convênios com o Ministério Público Federal e com o Núcleo de Informação e Coordenação do Ponto BR - NIC.br, entidade civil sem fins lucrativos que implementa as decisões do Comitê Gestor da Internet no Brasil – CGI.br. Uma das mais importantes atividades da SaferNet é o recebimento de denúncias.

denúncias classificadas como intolerância religiosa[393]. Os conceitos de racismo, xenofobia e intolerância religiosa apresentados pelo site no momento da classificação da denúncia são idênticos, sendo descritos como:

> material escrito, imagens ou qualquer outro tipo de representação de idéias ou teorias que promovam e/ou incitem o ódio, a discriminação ou violência contra qualquer indivíduo ou grupo de indivíduos, baseado na raça, cor, religião, descendência ou origem étnica ou nacional[394].

Nota-se que o conceito apresentado de racismo, xenofobia e intolerância religiosa é bastante semelhante ao conceito de material racista ou xenófobo presente no Protocolo Adicional, permitindo o enquadramento de todas as denúncias sob a figura do racismo ou xenofobia, o que significa que no Brasil foram denunciados quase 54 mil incidentes envolvendo este tipo de discriminação na Rede Mundial de Computadores, em um período de 5 anos e 3 meses, conforme relatado anteriormente.

O Protocolo Adicional aprimora a Convenção de Budapeste, ofertando uma resposta adequada para essas graves violações dos direitos humanos que têm sido frequente e crescentemente, verificadas no ambiente virtual.

Após a explanação desses dois principais documentos internacionais de combate à criminalidade cibernética, gestados pelo Conselho da Europa, passa-se ao exame da outra organização regional que não integra o Sistema das Nações Unidas e tem se destacado nesta área: a Organização para a Cooperação e Desenvolvimento Econômico (OCDE).

B.2 Organização para a Cooperação e Desenvolvimento Econômico (OCDE)

O nascimento da Organização para Cooperação e Desenvolvimento Econômico (OCDE) remonta ao período posterior à segunda guerra mundial, quando os líderes da Europa chegaram à conclusão de que a melhor maneira para assegurar a paz duradora seria encorajar a cooperação e a reconstrução ao invés de punir os derrotados, evitando assim cometer os mesmos erros dos seus predecessores no final da primeira guerra mundial. Dessa maneira, foi estabelecida em 1947, a OCDE com a responsabilidade de executar o Plano Marshall para a

---

[393] SAFERNET BRASIL. *Indicadores*. Disponível em: <http://www.safernet.org.br/site/indicadores>. Acesso em: 19/05/2011.
[394] SAFERNET BRASIL. *Denunciar*. Disponível em: <http://www.safernet.org.br/site/denunciar>. Acesso em: 19/05/2011.

reconstrução da Europa, nascendo oficialmente em 30 de setembro de 1960, com a vigência da Convenção da OCDE[395].

Atualmente, a OECD conta com 34 países membros, sendo que o Brasil, apesar de não ser membro, faz parte do Programa de Engajamento Aumentado[396], sendo que a soma dos membros, dos integrantes do Programa de Engajamento Aumentado e dos candidatos à adesão, totaliza 40 países e responde por 80% do comércio e investimento mundial[397].

A missão da entidade, essencialmente, é trabalhar para uma economia mundial mais forte, mais limpa e mais justa, ajudando os governos e a sociedade a colher os benefícios da globalização, ao mesmo tempo que enfrentando os desafios do acompanhamento econômico, social e de governança. A OCDE coloca alta prioridade em decifrar assuntos emergentes e identificar políticas a fim de ajudar os fazedores de políticas (*policy makers*)[398].

De acordo com o artigo 1° da Convenção da OCDE[399] os objetivos da entidade são promover políticas para: a) atingir o mais alto e sustentável nível de crescimento econômico, de emprego e de padrão de vida nos países membros, enquanto que mantendo a estabilidade financeira e, assim, contribuindo para o desenvolvimento da economia mundial; b) contribuir para uma sólida expansão econômica nos países membros e não membros no processo de desenvolvimento econômico; e c) contribuir para a expansão multilateral e não discriminatória do comércio mundial, de acordo com as obrigações internacionais.

Já o artigo 2° esclarece que na busca destes objetivos, os membros da OCDE deverão, de forma individual e conjunta: a) promover o uso eficiente dos recursos econômicos; b) promover o desenvolvimento dos recursos nos campos científico e tecnológico, encorajando a

---

[395] Nesse sentido, ver o histórico oficial da entidade constante no seu site oficial, disponível em: <http://www.oecd.org/document/25/0,3746,en_36734052_36761863_36952473_1_1_1_1,00.html> . Acesso em: 27/02/2011; e o Relatório Anual da entidade, ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. *Secretary-General's Report to Ministers 2010*. 80 p. p. 4-5, 76-77. Disponível em: <http://www.oecd.org/dataoecd/ 62/12/45342482.pdf>. Acesso em: 27/02/2011.

[396] Países membros e ano de adesão: Alemanha (1961); Austrália (1971); Áustria (1961); Bélgica (1961); Canadá (1961); Chile (2010); Coréia do Sul (1996); Dinamarca (1961); Eslováquia (2000); Eslovênia (2010); Espanha (1961); Estados Unidos (1961); Estônia (2010); Finlândia (1969); França (1961); Grécia (1961); Hungria (1996); Irlanda (1961); Islândia (1961); Israel (2010); Itália (1962); Japão (1964); Holanda (1961); Luxemburgo (1961); México (1994); Noruega (1961); Nova Zelândia (1973); Polônia (1996); Portugal (1961); Reino Unido (1961); República Tcheca (1995); Suécia (1961); Suiça (1961); e Turquia (1961). País candidato à adesão: Rússia. Países integrantes do Programa de Engajamento aumentado: África do Sul, Brasil, China e Indonésia, conforme ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, *Op. Cit*., p. 5, e informações oficiais sobre países membros e data de ratificação da convenção disponível em: <http://www.oecd.org/document/58/0,3746,en_2649_201185_1889402_1_1_1_1,00.html>. Acesso em: 27/02/2011.

[397] Informações constantes do histórico oficial da entidade, disponível em: <http://www.oecd.org/document/25/0,3746,en_36734052_36761863_36952473_1_1_1_1,00.html> . Acesso em: 27/02/2011.

[398] ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, *Op. Cit*., p. 4.

[399] Texto da Convenção disponível em: <http://www.oecd.org/document/7/0,3746,en_2649_201185_1915847_1_1_1_1,00.html> . Acesso em: 27/02/2011.

pesquisa e promovendo treinamento vocacional; c) buscar políticas desenhadas para atingir o crescimento econômico e a estabilidade financeira interna e externa e evitar desenvolvimentos que possam colocar em risco suas economias ou as de outros países; d) buscar seus esforços para reduzir ou abolir obstáculos à troca de bens e serviços e atuais pagamentos e manter e estender a liberalização do movimento de capitais; e e) contribuir para o desenvolvimento econômico dos países membros e não membros, no processo de desenvolvimento econômico pelos meios apropriados, e, em particular, pelo fluxo de capital desses países, levando em consideração a importância para suas economias de receber assistência técnica e de assegurar a expansão de mercados de exportação.

A estrutura da Organização é composta de um conselho, integrado pelos representantes de cada um dos Estados-Membros, uma secretaria e mais de 250 comitês, grupos de trabalho e grupo de *experts*[400], dentro dos quais se destaca o Comitê sobre Políticas de Informação, Computadores e Comunicação (*Committee on Information, Communications and Computer Policy* - ICCP)[401], que compõe a Diretoria para Ciência, Tecnologia e Indústria. Considerando que as TICs transformaram as economias e as sociedades, sendo fundamentais para o desenvolvimento social, cultural e econômico, o ICCP foi criado para tratar das questões políticas que são chave para a Economia da Internet, relacionadas à conectividade, à criatividade e à confiança, sendo que esta última questão refere-se justamente a como dar proteção e fortalecer a autonomia dos consumidores e usuários. O Comitê possui 4 grupos de trabalho: Grupo de Trabalho sobre Políticas de Serviço e Infraestrutura de Comunicações; Grupo de Trabalho sobre Economia da Informação; Grupo de Trabalho sobre Segurança da Informação e Privacidade; e Grupo de Trabalho sobre Indicadores da SI. O trabalho do ICCP e dos seus grupos de trabalho envolvem a análise e o desenvolvimento de políticas, produzindo recomendações e orientações de políticas, servindo de fórum para a troca de experiências entre os Estados-Membros e desenvolvendo indicadores[402].

O Grupo de Trabalho sobre Segurança da Informação e Privacidade (*Working Party on Information Security and Privacy - WPISP*) é um fórum intergovernamental que desenvolve opções de políticas por consenso para manter a confiança na sociedade global interconectada, assistindo governos, setor privado e sociedade civil no desenvolvimento de uma cultura de segurança cibernética e na construção de confiança *online*. Envolve a pesquisa

---

[400] Informações obtidas no site da OCDE, disponível em: <http://www.oecd.org/pages/0,3417,en_36734052_36761791_1_1_1_1_1,00.html>. Acesso em: 27/02/2011.

[401] ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. *Committee on Information, Communications and Computer Policy (ICCP).* Disponível em: <http://www.oecd.org/dataoecd/18/39/37328586.pdf>. Acesso em: 27/02/2011.

[402] Id., Op. Cit., p. 1.

sobre políticas nacionais de segurança da informação, a organização de *workshops* para troca de experiências, inclusive com países não membros e a manutenção do *site* denominado "*Site* de Cultura de Segurança", para alcançar a todas as partes interessadas. Cabe ressaltar que o Grupo funciona como uma rede de *experts* dos setores público e privado e da sociedade civil, servindo também como plataforma única para monitorar tendências; compartilhar e testar experiências; analisar o impacto da tecnologia sobre a segurança da informação e privacidade; e fornecer orientação sobre políticas[403].

De acordo com a OCDE, o trabalho do WPISP serve de base para o desenvolvimento de políticas nacionais coordenadas; é balanceado, pragmático e respeita as diferenças legais, culturais e sociais; beneficia a mais ampla comunidade internacional, através da cooperação da OCDE com economias que não são membros e é reconhecido por outras organizações regionais e internacionais[404].

No cumprimento de seu mandato o Grupo é responsável pela elaboração de diversas publicações que servem de norte para países membros e não membros elaborarem suas próprias políticas, destacando-se: Diretrizes da OCDE para a Segurança das Redes e Sistemas de Informação: em Direção à Cultura de Segurança; Relatório sobre a Promoção da Cultura de Segurança nos Países da OCDE; Privacidade Online: Orientação da OCDE sobre Política e Prática; Diretrizes da OCDE para a Proteção dos Consumidores de Práticas Comerciais Transnacionais Fraudulentas e Enganosas; Diretrizes da OCDE sobre a Proteção da Privacidade e Fluxo Transfronteiriço de Dados Pessoais; e Política de Criptografia: As Orientações e as Questões[405].

Cabe menção, o fato de que o Brasil participou como membro observador *ad hoc* das reuniões do WPISP, ocorridas em 2009 e 2010, apresentando inclusive um estudo comparativo sobre estratégias nacionais de segurança cibernética, o que motivou a criação de um grupo de trabalho com a presença de países voluntários, cuja presidência é de responsabilidade do delegado de Portugal na OCDE[406].

---

[403] ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. *Working Party on Information Security and Privacy.* Disponível em: <http://www.oecd.org/dataoecd/20/2/36871394.pdf>. Acesso em: 28/02/2011.

[404] ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. *Working,* p. 2.

[405] Tradução livre dos títulos das publicações: *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (2002); Promotion of a Culture of Security in OECD Countries (2005 report); Privacy Online: OECD Guidance on Policy and Practice (2003); OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders (2003); OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980); and Cryptography Policy: The Guidelines and the Issues (1998).* Publicações disponíveis em: <www.oecd.org/sti/security-privacy>.

[406] Nesse sentido ver: BRASIL. Presidência da República, *Livro*, p. 21.

É justamente no âmbito do esforço da OCDE sobre segurança das TICs e proteção à privacidade, que foi iniciado o estudo sobre a criminalidade cibernética. Segundo Rosa[407], o trabalho da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) nestes temas iniciou em 1983, quando a entidade começou a estudar a possibilidade de aplicar e harmonizar no âmbito internacional as leis penais, no intuito de combater a utilização indevida de programas de computadores. O autor ainda revela que, em 1986 a OCDE publicou um informe intitulado "Delitos Informáticos", propondo uma conceituação ampla para esses crimes[408], com a seguinte definição: "qualquer conduta ilegal não-ética, ou não-autorizada que envolva o processamento automático de dados e/ou transmissão de dados". Trata-se da publicação intitulada de "*Computer-Related Crime: Analysis of Legal Policy*"[409], abordando assim, os crimes relacionados ao uso do computador.

A Publicação da UIT[410], "Entendendo os Crimes Cibernéticos: um Guia para Países em Desenvolvimento", esclarece que o relatório analisou a legislação existente e fez propostas para o combate dessa criminalidade. Além disso, o documento recomendou uma lista mínima de ofensas que os países deveriam tipificar, por exemplo: fraude relacionada a computadores, falsidade relacionada a computadores, alteração de programas de computadores e de dados e a interceptação de comunicações. O Guia elaborado pela UIT[411]ainda indica que, em 1990, o ICCP criou um grupo de *experts* para desenvolver uma lista de diretrizes para a segurança da informação, trabalho que foi finalizado em 1992, com a aprovação pelo Conselho da OCDE, das "Diretrizes da OCDE para a Segurança dos Sistemas de Informação" [412], as quais foram substituídas pelas "Diretrizes da OCDE para a Segurança das Redes e Sistemas de Informação: em Direção à Cultura de Segurança" [413], documento aprovado em 2002.

As diretrizes aprovadas em 1992 já dispunham sobre a necessidade de sancionamento da má utilização dos sistemas de informação, no seu memorando explanatório, como importante meio na proteção dos interesses daqueles que dependem dos sistemas de informação contra danos resultantes de ataques à disponibilidade, confidencialidade e integridade dos sistemas de informação e seus componentes. Como exemplo dessas condutas

---

[407] ROSA, Op. Cit., p. 55.
[408] Id., Op. Cit., p. 55.
[409] Publicação não disponível no site da OCDE.
[410] INTERNATIONAL TELECOMUNICATION UNION, *Understanding,* p. 102.
[411] Id., Op. Cit*.*, p. 102.
[412] *OECD Guidelines for the Security of Information Systems*, disponível em: <http://www.oecd.org/document/19/0,3746,en_2649_34255_1815059_1_1_1_1,00.html>. Acesso em: 03/03/2011.
[413] ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security.* França: OCDE, 2002. 30 p. Disponível em: http://www.oecd.org /dataoecd/16/22/15582260.pdf>. Acesso em: 03/03/2011.

que deveriam ser sancionadas, o documento exemplifica: danos e interrupção de sistemas de informação pela inserção de *vírus and worms*; alteração de dados; acesso ilegal a dados; fraude de computador; falsificação de computador e reprodução não autorizada de programas de computador. Além disso, a publicação ainda revela que, à época, já existia um crescente acordo internacional sobre o âmago das ofensas relacionadas a computador que deveriam ser tipificadas pelas legislações penais nacionais, fato refletido no desenvolvimento de legislação sobre crimes de computador e proteção de dados nos países membros da OCDE nas últimas duas décadas e no trabalho da OCDE e de outros órgãos internacionais sobre o combate de crimes relacionados ao computador. Ainda cabe ressaltar que a OCDE em 1992 já alertava que, para a cooperação internacional em matéria penal avançar, o processo de harmonização das legislações deveria ser apoiado e considerado pelos países quando da revisão das suas leis[414].

Desde 1992, as diretrizes sofreram um processo de revisão em 1997 e a atual versão, aprovada como Recomendação pelo Conselho da OCDE, em 25 de julho de 2002, foi revisada pelo WPISP, de acordo com o mandato do ICCP, tendo sido iniciado o trabalho de revisão em 2001 e acelerado pela tragédia de 11 de Setembro de 2001[415].

A última versão das Diretrizes da OCDE para a Segurança das Redes e Sistemas de Informação: em Direção à Cultura de Segurança, de 2002, observa, no seu prefácio, que a situação desde 1992 mudou radicalmente, com a utilização de computadores pessoais cada vez mais poderosos, convergência tecnológica e universalização do acesso à Internet, fazendo com que todos os participantes da cadeia (governo, setor privado, sociedade civil organizada, academia e usuários) estejam cada vez mais interconectados transnacionalmente. Além disso,

---

[414] Nesse sentido, ver texto completo das diretrizes no tocante às sanções: "*Sanctions for misuse of information systems are an important means in the protection of the interests of those relying on information systems from harm resulting from attacks to the availability, confidentiality and integrity of information systems and their components. Examples of such attacks include damaging or disrupting information systems by inserting viruses and worms, alteration of data, illegal access to data, computer fraud or forgery, and unauthorised reproduction of computer programs. In combating such dangers, countries have chosen to describe and respond to the offending acts in a variety of ways. There is growing international agreement on the core of computer-related offences that should be covered by national penal laws. This is reflected in the development of computer crime and data protection legislation in OECD Member countries during the last two decades and in the work of the OECD and other international bodies on legislation to combat computer-related crime […]. National legislation should be reviewed periodically to ensure that it adequately meets the dangers arising from the misuse of information systems […].The development of legislation in OECD Member countries has already led, particularly under the influence of international organisations, including the OECD, to a certain degree of harmonization. In order to further international co-operation in penal matters (including in the areas of mutual assistance, extradition and other international co-operation described below), this harmonization process should be supported and taken into account by countries when reviewing their legislation*", disponível em: <http://www.oecd.org/document/19/0,3746,en_2649_34255_1815059_1_1_1_1,00.html>. Acesso em: 03/03/2011.

[415] ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, *OECD Guidelines for the Security of Information Systems and Networks*, p. 16.

o documento ressalta que a Internet é suporte das infraestruturas críticas de serviços essenciais para a sociedade como energia, transporte e finanças e que o contínuo aumento da interconectividade, resultou em um número crescente e ampla variedade de ameaças e vulnerabilidade das redes e dos sistemas de informação[416].

No que diz respeito às condutas que podem ser identificadas como crime, o texto da Recomendação do Conselho da OCDE que aprovou a atualização das Diretrizes de Segurança na sua 1.037° Sessão, em 25 de julho de 2002, reconhece que os dados e as informações armazenados e transmitidos pelas redes e sistemas de informação estão sujeitos a ameaças de diversos meios de acesso não autorizado, uso, desfalque, alteração, transmissão de códigos maliciosos, denegação de serviço ou destruição e exigem as apropriadas salvaguardas[417].

As diretrizes contemplam nove princípios complementares que devem ser interpretados conjuntamente. São eles: conscientização, responsabilidade, resposta, ética, democracia, avaliação do risco, implementação e desenho de segurança, gestão de segurança e reavaliação[418].

---

[416] ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, *OECD Guidelines for the Security of Information Systems and Networks*, p. 7.
[417] *Id*., *Op. Cit*., p. 14.
[418] ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, *OECD Guidelines for the Security of Information Systems and Networks*, p. 10-12. Conteúdo dos princípios constantes das diretrizes: "*1) Awareness. Participants should be aware of the need for security of information systems and networks and what they can do to enhance security. Awareness of the risks and available safeguards is the first line of defense for the security of information systems and networks. Information systems and networks can be affected by both internal and external risks. Participants should understand that security failures may significantly harm systems and networks under their control. They should also be aware of the potential harm to others arising from interconnectivity and interdependency. Participants should be aware of the configuration of, and available updates for, their system, its place within networks, good practices that they can implement to enhance security, and the needs of other participants; 2) Responsibility. All participants are responsible for the security of information systems and networks. Participants depend upon interconnected local and global information systems and networks and should understand their responsibility for the security of those information systems and networks. They should be accountable in a manner appropriate to their individual roles. Participants should review their own policies, practices, measures, and procedures regularly and assess whether these are appropriate to their environment. Those who develop, design and supply products and services should address system and network security and distribute appropriate information including updates in a timely manner so that users are better able to understand the security functionality of products and services and their responsibilities related to security; 3) Response. Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents. Recognising the interconnectivity of information systems and networks and the potential for rapid and widespread damage, participants should act in a timely and co-operative manner to address security incidents. They should share information about threats and vulnerabilities, as appropriate, and implement procedures for rapid and effective co-operation to prevent, detect and respond to security incidents. Where permissible, this may involve cross-border information sharing and co-operation; 4) Ethics. Participants should respect the legitimate interests of others. Given the pervasiveness of information systems and networks in our societies, participants need to recognise that their action or inaction may harm others. Ethical conduct is therefore crucial and participants should strive to develop and adopt best practices and to promote conduct that recognises security needs and respects the legitimate interests of others; 5) Democracy. The security of information systems and networks should be compatible with essential values of a democratic society. Security should be implemented in a manner consistent with the values recognised by democratic societies including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency; 6) Risk*

O Princípio da Conscientização aborda a necessidade de que todos os participantes da cadeia estejam conscientes dos riscos, da necessidade de segurança e das medidas que eles podem adotar para aumentar a segurança, enquanto que o Princípio da Responsabilidade atesta que todos os participantes da cadeia (governos, setor privado e usuários) são responsáveis pela segurança, dentro dos seus respectivos papéis, devendo compreender sua responsabilidade. O Princípio da Resposta determina que os participantes devem agir de forma cooperativa e oportuna para prever, detectar, responder e tratar os incidentes de segurança, compartilhando informações sobre ameaças e vulnerabilidade, quando apropriado, prevendo inclusive a partilha dessas informações transfronteiriçamente e a cooperação internacional. Já o Princípio Ético defende que os participantes devem respeitar os interesses legítimos dos outros, reconhecendo que suas ações ou omissões podem prejudicar outrem. O Princípio Democrático estabelece que a segurança das redes e sistemas de informação deve ser compatível com os valores essenciais de uma sociedade democrática, respeitando assim a liberdade do intercâmbio de idéias e pensamentos, o livre fluxo da informação, a confidencialidade da informação e comunicação, a proteção dos dados pessoais, a abertura e a transparência.

O Princípio da Avaliação do Risco esclarece que os participantes devem conduzir avaliações de risco, a fim de identificar ameaças e vulnerabilidades, devendo abranger fatores

---

assessment. Participants should conduct risk assessments. Risk assessment identifies threats and vulnerabilities and should be sufficiently broad-based to encompass key internal and external factors, such as technology, physical and human factors, policies and third-party services with security implications. Risk assessment will allow determination of the acceptable level of risk and assist the selection of appropriate controls to manage the risk of potential harm to information systems and networks in light of the nature and importance of the information to be protected. Because of the growing interconnectivity of information systems, risk assessment should include consideration of the potential harm that may originate from others or be caused to others; 7) Security design and implementation. Participants should incorporate security as an essential element of information systems and networks. Systems, networks and policies need to be properly designed, implemented and co-ordinated to optimise security. A major, but not exclusive, focus of this effort is the design and adoption of appropriate safeguards and solutions to avoid or limit potential harm from identified threats and vulnerabilities. Both technical and non-technical safeguards and solutions are required and should be proportionate to the value of the information on the organisation's systems and networks. Security should be a fundamental element of all products, services, systems and networks, and an integral part of system design and architecture. For end users, security design and implementation consists largely of selecting and configuring products and services for their system; 8) Security management. Participants should adopt a comprehensive approach to security management. Security management should be based on risk assessment and should be dynamic, encompassing all levels of participants' activities and all aspects of their operations. It should include forward-looking responses to emerging threats and address prevention, detection and response to incidents, systems recovery, ongoing maintenance, review and audit. Information system and network security policies, practices, measures and procedures should be co-ordinated and integrated to create a coherent system of security. The requirements of security management depend upon the level of involvement, the role of the participant, the risk involved and system requirements; and 9) Reassessment. Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures. New and changing threats and vulnerabilities are continuously discovered. Participants should continually review, reassess and modify all aspects of security to deal with these evolving risks".

internos e externos, permitindo assim a determinação do nível de risco aceitável e assistindo a seleção do controle apropriado para gerenciar os riscos de danos potenciais. O Princípio de Implementação e Desenho de Segurança alerta que os participantes devem incorporar a segurança como elemento essencial das redes e sistemas de informação, os quais devem ser desenhados, implementados e coordenados para otimizar a segurança, a fim de evitar ou limitar os potenciais danos das ameaças e vulnerabilidades identificadas sendo que, para o usuário final, o princípio consiste na seleção e configuração de produtos e serviços para seus sistemas. Já o Princípio de Gerenciamento de Segurança prevê que os participantes devem adotar uma abordagem compreensiva e dinâmica de gerenciamento de segurança, baseando-se na avaliação de risco, e abarcando todas as atividades da cadeia de participantes, sendo que as práticas, medidas, procedimentos e políticas de segurança da rede e dos sistemas de informação devem ser coordenados e integrados no intuito de criar um sistema coerente de segurança. Por fim, o último, Princípio da Reavaliação enuncia que os participantes devem revisar e reavaliar as redes e sistemas de informação e realizar as modificações apropriadas das políticas de segurança, práticas, medidas e procedimentos, a fim de enfrentar a evolução dos riscos, visto que novas e cambiantes ameaças são descobertas continuamente[419].

Após a atualização das diretrizes em 2002, a OCDE continuou a trabalhar na temática da segurança cibernética, destacando-se as publicações anteriormente citadas: "Diretrizes da OCDE para a Proteção dos Consumidores de Práticas Comerciais Transnacionais Fraudulentas e Enganosas", "Privacidade *Online*: Orientação da OCDE sobre Política e Prática", ambas de 2003, e "Relatório sobre a Promoção da Cultura de Segurança nos Países da OCDE", de 2005.

Assim como a UIT, a OCDE também possui um portal sobre no tema na Internet[420], o qual concentra *links* para os trabalhos desenvolvidos pela OCDE relacionados à segurança, assim como iniciativas dos países na promoção da cultura de segurança cibernética, ressaltando-se que, além de projetos dos Estados-Membros da organização, o *site* traz referência de iniciativa do Brasil, indicando o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República. Além disso, o *site* traz referências de ferramentas disponíveis *online* e informações sobre cooperação internacional.

---

[419] Idem nota n.° 247.

[420] Acesso ao site sobre segurança da OCDE pelo endereço< http://www.oecd.org/sti/cultureofsecurity>. Acesso em 06/02/2011. O portal encontra-se desatualizado.

Atualmente, da análise dos últimos trabalhos e publicações da OCDE[421] percebe-se que a organização tem concentrado seus esforços na área de segurança da informação e privacidade nos seguintes tópicos: *spam*, furto de identidade *online*, infraestrutura crítica de informação, gerenciamento de identidade digital, proteção das crianças *online*, vírus de computador, aplicação da lei e cooperação, além de temas emergentes como a identificação por radiofrequência (RFID) [422], sendo que todos os tópicos acabam por ter relação direta ou indireta com a temática da criminalidade cibernética, visto que abordam assuntos que podem ser considerados delitos, por exemplo: *spam*, vírus e furto de identidade *online*, assim como trata também de aplicação da lei e cooperação, e, por fim, abarca questões que impactam no direito à privacidade, refletindo também na segurança das informações.

Dessa maneira, resta evidenciado que a OCDE é um dos principais atores na esfera regional/internacional, trabalhando para o enfrentamento dos crimes de computador desde a Década de 80, acompanhando da evolução tecnológica, através da análise e formulação de políticas para o combate dessas ameaças.

[421] Nesse sentido ver as informações constantes do site do *WPISP*, disponível em: <www.oecd.org/sti/security-privacy>. Acesso em: 07/03/2011.

[422] A RFID consiste na transmissão sem fio de dados por rótulos eletrônicos, anexados ou embarcados a objetos para fins de identificação, tecnologia que gera questionamentos sobre respeito à privacidade. Nesse sentido, ver ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. *RFID Radio Frequency Identification: a focus on information security and privacy applications, impacts and countries initiatives*. 118 p. p. 3. Disponível em: <http://www.oecd.org/dataoecd/19/42/40892347.pdf>. Acesso em 07/03/2011.

CONSIDERAÇÕES FINAIS

A pesquisa realizada partiu da premissa que era importante e necessário, primeiramente, entender o quê são os crimes cibernéticos, a fim de que, com base nessas lições, fosse possível apresentar os trabalhos desenvolvidos em âmbito regional e internacional em busca da prevenção e repressão desses crimes. A compreensão do fenômeno foi possível com o estudo que abarca terminologia utilizada, conceituação, bem jurídico tutelado, histórico e contextualização, características, sujeitos ativo e passivo e técnicas empregadas. Além disso, examina-se como estes delitos são tratados pelo Sistema Penal Brasileiro, mencionando-se o ordenamento vigente, os projetos de lei em trâmite no Congresso Nacional e a jurisprudência.

Ainda que não exista consenso, assenta-se a definição destas infrações penais como condutas típicas (ação ou omissão), antijurídicas e culpáveis praticadas por meio das Tecnologias de Informação e Comunicação (TICs) ou contra elas, ressaltado que a sua utilização como ferramenta pressupõe processamento automático e/ou a transmissão de dados.

Esses delitos podem lesionar os diversos bens jurídicos tradicionalmente protegidos pelo direito penal (crime cibernético impuro ou impróprio), nos casos em que as TICs são utilizadas como meio, ou a própria segurança da informação (crime cibernético puro ou próprio), caso em que as TICs são o alvo da conduta delitiva.

Como características principais, menciona-se a transnacionalidade, talvez a sua mais marcante nota, em face da facilidade e da velocidade com que tais delitos ultrapassam as fronteiras nacionais; a difícil comprovação da materialidade e da autoria; a efemeridade dos vestígios; e grande lesividade das ações, visto que um ato praticado no nosso país pode, sem grandes dificuldades e sem necessitar de envolvimento de um elevado número de pessoas e de uma elevada soma de dinheiro, atingir indivíduos de todos os continentes e em todos os países do mundo, causando danos de difícil mensuração, visto o enorme prejuízo econômico e as externalidades negativas que gera.

Ainda que não exista uma legislação específica no Brasil para a persecução dessas infrações, não se pode olvidar que o sistema fornece uma resposta, ainda que precise ser aprimorada e que a Lei n.° 11.829/2008, que alterou o art. 241 do Estatuto da Criança e do Adolescente, agregou de maneira positiva e consideravelmente com o objetivo de criminalizar a posse de material classificado como pornografia infantil e de coibir o desenvolvimento desta recriminável prática por meio da Internet.

O Brasil precisa consolidar questões prévias não penais e essenciais à repressão destas condutas, como por exemplo a guarda de *logs* pelos provedores de acesso, para posteriormente discutir ampla e interdisciplinarmete quais as são as condutas praticadas contras as TICs, crimes cibernéticos puros ou próprios, que efetivamente exigem a intervenção do Direito Penal. Ressalta-se que a criminalização dos crimes cibernéticos próprios que ainda não estão tipificados é necessária e urgente.

Também se faz necessário discutir se a pena dos crimes tradicionalmente tutelados (crimes cibernéticos impuros ou impróprios), como por exemplo crimes contra a honra e crimes contra o patrimônio, é adequada. Neste aspecto, sustenta-se que é necessário atualizá-las em face da lesividade das condutas, no intuito de torná-las proporcionais aos danos causados.

Tendo em vista as peculiaridades do fenômeno, justamente, a comunidade internacional foi compelida a coordenar esforços para enfrentar essa criminalidade, sendo o Conselho da Europa, a Organização para a Cooperação e Desenvolvimento Econômico, e órgãos e agências do Sistema das Nações Unidas (Assembléia Geral das Nações Unidas, Escritório das Nações Unidas sobre Drogas e Crime e União Internacional de Telecomunicações) os maiores expoentes nesta problemática, motivo pelo qual a segunda parte deste estudo foca nas atividades e iniciativas por eles desenvolvidas.

Especificamente quanto ao Sistema das Nações Unidas existem diversos órgãos e agências que têm liderado as iniciativas e estudos internacionais na matéria, notadamente a Assembléia Geral das Nações Unidas, órgão máximo deliberativo das Nações Unidas, Escritório das Nações Unidas sobre Drogas e Crime e órgãos a ele relacionados e a União Internacional de Telecomunicações, agência especializada das Nações Unidas para as Tecnologias de Informação e Comunicação.

A Assembléia Geral tem exercido um forte papel, mantendo desde 1998 em sua pauta, o assunto do avanço destas tecnologias e o seu impacto para a segurança internacional, bem como da necessidade de criação de uma cultura global de segurança cibernética, protegendo-se também as Infraestruturas Críticas de Informação.

A atuação do Escritório das Nações Unidas sobre Drogas e Crime nesta temática tem especial destaque na assistência aos países no desenvolvimento da apropriada legislação nacional, além de também trabalhar para a harmonização destas legislações internas, tendo recebido a atribuição de conduzir o extenso e profundo estudo sobre crimes cibernéticos que já está sendo realizado no âmbito da Comissão sobre Prevenção ao Crime e Justiça Criminal, com previsão de conclusão para 2013, podendo subsidiar um tratado internacional na matéria.

O papel da União Internacional de Telecomunicações, com seu mandato decorrente da Agenda de Túnis da Cúpula Mundial sobre a Sociedade da Informação, também não pode ser esquecido nem minimizado, fornecendo importante subsídio técnico sobre o assunto e demonstrando que a evolução tecnológica traz novos paradigmas na luta contra a criminalidade, a qual não pode ser enfrentada sem uma política interdisciplinar.

A menção ao Conselho da Europa justifica-se pela sua Convenção de Budapeste e seu Protocolo Adicional. Embora seja o único documento transnacional e vinculante sobre o assunto, cabe a ressalva de que sua adesão é limitada aos Estados-Membros do Conselho da Europa e aos seus Membros-Observadores e de que não tem condições de oferecer uma resposta internacional adequada ao problema, seja pela desatualização do texto seja pelas dificuldades ocasionadas pela restrita fase de negociação, que contemplou um limitado e específico número de países, não membros do Conselho da Europa, dificultando sua desvinculação do continente Europeu. Conforme relatado no texto, a posição do atual Governo Brasileiro não vislumbra a adesão brasileira ao tratado, considerando-o uma iniciativa regional que deve alimentar um processo mais amplo de negociação, defendendo a celebração de um tratado internacional.

Subscreve-se a posição brasileira de não aderir ao tratado e conclamar esforços dos países para a negociação internacional, visto que o texto já tem mais de 10 anos e neste período foi vivenciada grande evolução tecnológica; que se pode aplicar as lições aprendidas no combate desta criminalidade para construir um texto mais eficaz; e que todos os países interessados podem participar e contribuir para um novo texto, aumentando a chance de que os países assinem e ratifiquem ou adiram à nova convenção. Confrontando-se com a Convenção do Conselho da Europa sobre Crimes Cibernéticos, acredita-se que a celebração de um novo tratado sobre a matéria ampliaria as perspectivas de sua implementação e da sua eficácia.

Não é menos importante o empenho da Organização para a Cooperação e Desenvolvimento Econômico, precursora de iniciativas e estudos na matéria, sendo que os reflexos do seu trabalho não se limita aos seus Estados-Membros, consistindo importante fonte de práticas que subsidiam a formulação de políticas sobre o tópico, as quais são amplamente reconhecidas e utilizadas pelas demais organizações regionais e internacionais e por diversos países, independente de serem membros ou não.

Dessa forma, percebe-se que pela extensão, consistência e constância do enfrentamento do tema na agenda diplomática internacional e regional a partir da Década de 90 e acentuada com o início do novo século, não há alternativa para o combate efetivo desta criminalidade sem cooperação internacional e adequação das legislações nacionais.

O estudo atribuído ao Grupo de *Experts* sobre Crimes Cibernéticos no seio da Comissão sobre Prevenção ao Crime e Justiça Criminal, e sob a responsabilidade do Escritório das Nações Unidas sobre Drogas e Crime, com conclusão prevista para 2013 e que conta com representação regional, acena para a concreta possibilidade de negociação de um tratado internacional, gestado no âmbito do Sistema das Nações Unidas em curto prazo, uma vez que pode construir importantes consensos no assunto, visto que dentre os tópicos do estudo, estão incluidos a criminalização de condutas, as abordagens comuns para legislação, a cooperação internacional, e as salvaguardas e a proteção aos direitos fundamentais, pontos fundamentais para acordo entre os Países, a fim de permitir a negociação de texto.

O últimos anos foram marcados, nacional e internacionalmente, pelo lançamento de inúmeras iniciativas e acontecimentos referentes a crimes cibernéticos e para os próximos anos não se imagina cenário diverso, visto que o tópico continuará na agenda diplomática internacional até que se alcance o nível desejado de cooperação e de repressão por parte dos países, avistando-se, repisa-se, a possibilidade de negociação de um novo tratado em curto prazo. Internamente, assistir-se-á aos desdobramentos da discussão do Marco Civil da Internet, os quais subsidiarão a posterior criminalização de condutas que caracterizariam crimes cibernéticos puros ou próprios e que não encontram abrigo nas tipificações hoje existentes no nosso ordenamento.

REFERÊNCIAS

ALBUQUERQUE, Roberto Chacon de. *A Criminalidade Informática*. São Paulo: Editora Juarez de Oliveira, 2006. 264 p.

AMBOS, Kai. *A Parte Geral do Direito Penal Internacional: bases para uma elaboração dogmática*. Ed. brasileira reform. e atual. São Paulo: Editora Revista dos Tribunais, 2008. 703 p.

BARROS, Marco Antonio de. Tutela Punitiva Tecnológica. *In*: PAESANI, Liliana Minardi (Coord.). *O Direito na Sociedade da Informação*. São Paulo: Editora Atlas, 2007. 333 p. p. 275-300.

BECK, Ulrich. *Sociedade de Risco: rumo a uma outra modernidade.*Tradução de Sebstião Nascimento. São Paulo: Ed. 34, 2010. 383 p.

BRASIL. Ministério da Ciência e Tecnologia. *Sociedade da Informação no Brasil:* livro verde. Brasília, 2000. 231 p. Disponível em: < http://www.socinfo.org.br/livro_verde/download.htm>. Acesso em: 15/08/2008.

_____. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. *Livro verde: segurança cibernética no Brasil*. Brasília: GSIPR/SE/DSIC, 2010. 63 p. Disponível em: <http://dsic.planalto.gov.br /documentos/publicacoes/1_Livro_Verde_SEG_CIBER.pdf>. Acesso em: 06/03/2011.

_____. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. *Guia de Referência para a Segurança das Infraestruturas Críticas da Informação*. Versão 1. Brasília: GSIPR/SE/DSIC, 2010. 151 p. Disponível em: <http://dsic.planalto.gov.br/documentos/publicacoes/2_Guia_SICI.pdf>. Acesso em: 06/03/2011.

CANÇADO TRINDADE, Antônio Augusto; DIREITO, Carlos Alberto, Menezes; PEREIRA, Antonio Celso Alves (coord.). *Novas Perspectivas do Direito Internacional Contemporâneo: Estudos em Homenagem ao Professor Celso D. de Albuquerque Mello*. Rio de Janeiro: Renovar, 2008.

CAPELLER, Wanda de Lemos. A Transnacionalidade no Âmbito Penal: reflexões sobre as mutações do Crime e do controle. *In*: MELLO, Celso de Albuquerque (Coord.). *Anuário Direito e Globalização*. V. 1. Rio de Janeiro: Renovar, 1999. p. 113-134.

CASTLE, Allan. *Transnational Organized Crime and International Security*. Working Paper n. 19. Institute of International Relations, University of British Columbia, Vancouver, nov., 1997. 14 p.

CENTRO DE TECNOLOGIA E SOCIEDADE, ESCOLA DE DIREITO DO RIO DE JANEIRO DA FUNDAÇÃO GETULIO VARGAS. *Comentários Comentários e Sugestões sobre o substitutivo do Projeto de Lei de Crimes Eletrônicos (PL n. 84/99) apresentado pela Comissão de Constituição e Justiça e de Cidadania, November 2009*. Disponível em: <http://virtualbib.fgv.br/dspace/bitstream/handle/10438/7719/coment%c3%a1rios%20ao%20substitutivo%20PL%2088-99.pdf?sequence=1>. Acesso em: 16/11/2010. 38 p.

CHERLOFF, Michael. *The cybersecurity challenge*. Disponível em: <http://www3. interscience.wiley.com/cgi-bin/fulltext/121564463/HTMLSTAR>. Acesso em: 07/07/2009.

CONCERINO, Arthur José. Internet e Segurança são Compatíveis? *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.). *Direito & internet: aspectos jurídicos relevantes*. 2 ed. São Paulo: Quartier Latin, 2005. 543 p. p. 153-178.

CORRÊA, Gustavo Testa. *Aspectos Jurídicos da Internet*. 4 ed. rev. e atual. São Paulo: Saraiva, 2008. 151 p.

CRUZ, Danielle da Rocha. *Criminalidade Informática – Tipificação Penal das Condutas Ilícitas Realizadas com Cartões de Crédito***.** Rio de Janeiro: Forense, 2006. 224 p.

DAOUN, Alexandre Jean. Crimes Informáticos e o Papel do Direito Penal na Tecnologia da Informação. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.). *Direito & internet: aspectos jurídicos relevantes*. Vol. II. São Paulo: Quartier Latin, 2008. 718 p. p. 173-183.

_____; BLUM, Renato M. S. Ópice. Cybercrimes. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.). *Direito & internet: aspectos jurídicos relevantes*. 2 ed. São Paulo: Quartier Latin, 2005. 543 p. p. 141-152.

DE LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.). *Direito & internet: aspectos jurídicos relevantes*. 2 ed. São Paulo: Quartier Latin, 2005. 543 p.

_____. Newton; SIMÃO FILHO, Adalberto (Coord.). *Direito & internet: aspectos jurídicos relevantes*. Vol. II. São Paulo: Quartier Latin, 2008. 718 p.

DENNING, Dorothy E. *Cyberterrorism*. Disponível em: <http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html>. Acesso em 06/07/2009.

DONEDA, Danilo. Perspectivas para Combate ao Spam. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.). *Direito & internet: aspectos jurídicos relevantes*. Vol. II. São Paulo: Quartier Latin, 2008. 718 p. p. 255-276.

DRAETTA, Ugo. Internet et commerce électronique en droit international des affaires. *Recueil des cours de l'Académie de droit international de La Haye*, vol. 314, 2005. p. 9-232.

FARIA, José Eduardo C. O. *O direito na economia globalizada*. São Paulo: Malheiros, 1999. 359 p.

FERREIRA, Érica Lourenço de Lima. *Criminalidade Econômica Empresarial e Cibernética: o empresário como delinqüente econômico e os crimes cometidos através da Internet*. Florianópolis: Momento Atual, 2004. 122 p.

_____. *Internet: Macrocriminalidade e Jurisdição Internacional.* Curitiba: Juruá, 2008. 204 p.

FERREIRA, Ivette Senise. A Criminalidade Informática. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.). *Direito & internet: aspectos jurídicos relevantes*. 2 ed. São Paulo: Quartier Latin, 2005. 543 p. p. 237-267.

FINKELSTEIN, Maria Eugênia. Fraude Eletrônica. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.). *Direito & internet: aspectos jurídicos relevantes*. Vol. II. São Paulo: Quartier Latin, 2008. 718 p. p. 403-440.

GERCKE, Marco. *An Introduction to Cybercrime*. UNAFEI 140th International Training Course, Resource Material Series n.° 79, 2008, 29 p. Disponível em: <http://www.unafei.or.jp/ english/pdf/RS_No79/No79_05VE_Gerke.pdf> Acesso em: 20/03/2011.

GINSBURG, Jane C. The Private International Law of Copyright in an Era of Technological Change. *Recueil des cours de l'Académie de droit international de La Haye*, vol. 273, 1998. p. 239-405.

GORDON, Sarah. *Cyberterrorism?* Disponível em: <http://www.symantec.com/avcenter/reference/cyberterrorism.pdf>. Acesso em: 06/07/2009.

GOUVÊA, Sandra. *O Direito na Era Digital: crimes praticados por meio da informática*. Rio de Janeiro: Mauad, 1997. 164 p.

GRABOSKY, Peter. *Electronic Crime*. Master Series in Criminology. New Jersey: Pearson Prentice Hall, 2007. 123 p.

HENTEA, Mariana; DHILLON, Harpal S.; DHILLOM, Manpreet. Towards Changes in Information Security Education. J*ournal of Information Technology Education*, V. 5, 2006. Disponível em: <http://jite.informingscience.org/documents/Vol5/v5p221-233Hentea148.pdf>. Acesso em: 07/07/2009.

INTERNATIONAL TELECOMMUNICATION UNION. *Cybersecurity for All : ITU's work for a safer world.* Genebra: UIT, 2008. 32 p. Disponível em: <http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-CYBER-2008-PDF-E.pdf>. Acesso em: 25/10/2009.

_____. *Cybersecurity Gateway*. Disponível em: <http://www.itu.int/cybersecurity/gateway/>. Acesso em: 12/10/2009.

_____. *ITU Building the Information Society.* Genebra: UIT, 2007. 44 p. Disponível em: <http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-BIS-2007-PDF-E.pdf>. Acesso em: 07/10/2009.

_____. *ITU Toolkit for Cybercrime Legislation*. Disponível em: <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf>. Acesso em: 07/10/2009.

_____. *ITU Toolkit for Promoting a Culture of Cybersecurity.* Disponível em: <http://www.itu.int/cybersecurity/gateway/promoting_culture.html>. Acesso em: 07/10/2009.

_____. *Question 22-1: Securing information and communication networks: best practices for developing a culture of cybersecurity*. Final Report. 72 p. Disponível em: <http://www.itu.int/dms_pub/itu-d/opb/stg/D-STG-SG01.22-2010-PDF-E.pdf>. Acesso em: 05/03/2011.

_____. *Understanding Cybercrime: a guide for developing countries*. 225 p. Disponível em: <http://www.itu.int /ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf>. Acesso em: 07/10/2009.

INTERNET CRIME COMPLAINT CENTER – IC3. *2009 Internet Crime Report*. 25 p. Disponível em: <http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf>. Acesso em: 10/03/2011.

JAYME, Erik (vários textos). *Cadernos do Programa de Pós-Graduação em Direito da Universidade Federal do Rio Grande do Sul - PPGDir/UFRGS*, vol. 1, n. 1, mar. 2003.

KEYSER, Mike. The Council of Europe Convention on Cybercrime, *J. Transnational Law & Policy*, vol. 12:2, spring 2003, p. 287-326. Disponível em: <http://www.law.fsu.edu/Journals/transnational/vol12_2/keyser.pdf>. Acesso em 20/03/2011.

KERR, Kathryn. Putting cyberterrorism into context. *AusCERT Member Newsletter,* vol. 7, n. 2, jul. 2003. Disponível em: <http://www.auscert.org.au/render.html?it=3552>. Acesso em: 09/07/2009.

KURBALIJA, Jovan. *An Introduction to Internet Governance*. 164 p. DiploFoundation and National Internet Exchange of India (NIXI): 2008. Disponível em: <http://www.diplomacy.edu/poolbin.asp?IDPool=806>. Acesso em junho de 2009.

_____.; GELBSTEIN, Eduardo. *Governança de Internet: questões, atores e cisões*. DiploFoundation, 2005. 164 p.

LAFER, CELSO. A *Internacionalização dos Direitos Humanos: Constituição, Racismo e Relações Internacionais.* São Paulo: Manole, 2005. 135 p.

LEMOS, Ronaldo. *Direito, Tecnologia e Cultura*. Rio de Janeiro: Editora FGV, 2005. 211 p.

LIMA, Paulo Marco Ferreira. *Crimes de Computador e Segurança Computacional***.** Campinas: Millenium, 2007. 234 p.

LUCERO, Everton. Governança de Internet: aspectos da formação de um regime global e oportunidades para a ação diplomática. Brasília: Fundação Alexandre Gusmão, 2011. 236 p. Disponível em: <http://www.funag.gov.br/biblioteca/index.php?option=com_docman&task=doc_details&gid=89&Itemid=41>. Acesso em: 25/08/2011.

MARQUES, Cláudia Lima. *Confiança no Comércio Eletrônico e a Proteção do Consumidor: (um estudo dos negocios jurídicos no comercio eletrônico)*. São Paulo: Editora Revista dos Tribunais, 2004. 544 p.

MEDEIROS, Antônio Paulo Cachapuz. (org.*) Desafios do Direito Internacional Contemporâneo*. Brasília: Fundação Alexandre de Gusmão, 2007.

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. *Secretary-General's Report to Ministers 2010*. 80 p. Disponível em: <http://www.oecd.org/dataoecd/62/12/45342482.pdf>. Acesso em: 27/02/2011.

_____. *Committee on Information, Communications and Computer Policy (ICCP).* Disponível em: <http://www.oecd.org/dataoecd/18/39/37328586.pdf>. Acesso em: 27/02/2011.

_____. *OECD Guidelines for the Security of Information Systems. D*isponível em: <http://www.oecd.org/document/19/0,3746,en_2649_34255_1815059_1_1_1_1,00.html>. Acesso em: 03/03/2011.

_____. *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security.* França: OCDE, 2002. 30 p. Disponível em: http://www.oecd.org/dataoecd/16/22/15582260.pdf>. Acesso em: 03/03/2011.

_____. *RFID Radio Frequency Identification: a focus on information security and privacy applications, impacts and countries initiatives*. 118 p. Disponível em: <http://www.oecd.org/dataoecd/19/42/40892347.pdf>. Acesso em 07/03/2011.

_____. *Working Party on Information Security and Privacy.* Disponível em: <http://www.oecd.org/dataoecd/20/2/36871394.pdf>. Acesso em: 28/02/2011.

PAESANI, Liliana Minardi (Coord.). *O Direito na Sociedade da Informação*. São Paulo: Editora Atlas, 2007. 333 p.

PAYNE, Shirley. *Developing Security Education and Awareness Programs*. Disponível em: <http://net.educause.edu/ir/library/pdf/eqm0347.pdf>. Acesso em 07/07/2009.

PINHEIRO, Patricia Peck. *Direito digital*. 2 ed. 2 tir. rev., atual. e ampl. São Paulo: Saraiva, 2008. 407 p.

PIOVESAN, Flávia. *Direitos Humanos e o Direito Constitucional Internacional*. 9 ed. rev., ampl. e atual. São Paulo: Saraiva, 2008. 552 p.

RAMOS, André de Carvalho. *Processo Internacional de Direitos Humanos: análise dos sistemas de apuração de violações de direitos humanos e implementação das decisões no Brasil*. Rio de Janeiro: Renovar, 2002. 424 p.

ROSA, Fabrízio. *Crimes de Informática*. 3 ed. São Paulo: Bookseller, 2007. 141 p.

ROSENNE, Shabtai. The perplexities of modern international law: general course on public international law. *Recueil des cours de l'Académie de droit international de La Haye*, vol. 291, 2001. p. 10-463.

ROSSINI, Augusto. *Informática, Telemática e Direito Penal*. São Paulo: Memória Jurídica, 2004. 352 p.

RUSTAD, Michael L. Private Enforcement of Cybercrime on the Electronic Frontier, *Southern California Interdisciplinary Law Journal*, v. 11:63, 2001, p. 63-116. Disponível em: <http://www-bcf.usc.edu/~idjlaw/PDF/11-1/11-1%20Rustad.pdf >. Acesso: 21/03/2011.

SAFERNET BRASIL. *Indicadores*. Disponível em: <http://www.safernet.org.br/site/indicadores >. Acesso em: 05/05/2009.

_____. Observatório do Congresso Nacional: o PL do Sen. Eduardo Azeredo e a Convenção contra o Cibercrime. Disponível em: <http://www.safernet.org.br/twiki/bin/view/Colaborar/PLSAzeredoXConvencaoCibercrime>. Acesso em: 25/07/2009.

SCANLAN, Emma. The Fight to Save America's Inbox: State Legislation and Litigation in the Wake of CAN-SPAM, *2 Shidler J. L. Com. & Tech*, dez. 2005. 7 p. Disponível em: <http://www.lctjournal.washington.edu/Vol2/a012Scanlan.html>. Acesso em: 20/08/2011.

SILVA, Rita de Cássia Lopes da. *Direito Penal e Sistema Informático*. São Paulo: Editora Revista dos Tribunais, 2003. 141 p.

SILVA JÚNIOR, Délio Lins e. Crimes informáticos: sua vitimização e a questão do tipo objetivo. In: D'ÁVILA, Fábio Roberto; SOUZA, Paulo Vinicius Sporleder de (Coords.) *Direito Penal secundário*. São Paulo: RT e Coibra Editora, 2006. 506 p. p. 311-337.

SMITH, Bradford L. The Third Industrial Revolution: Law and Policy for the Internet. *Recueil des cours de l'Académie de droit international de La Haye*, vol. 282, 2000. p. 229-464.

SOFAER, Abraham D.; GOODMAN, Seymour E. Cyber Crime and Security: the transnational dimension. In: *The Transnational Dimension of Cyber Crime and Terrorism.* Hoover Press, 2001. Disponível em: <http://media.hoover.org/documents/0817999825_1.pdf>. Acesso em: 21/03/2011.

STEIN, Schojolberg; GHERNAOUTI-HELIE, Solange. *Global Treaty on Cybersecurity and Cybercrime*. 2 ed. 2011. 97 p. Disponível em: <http://www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf >. Acesso em: 10/05/2011.

TEIXEIRA, Tarcisio. *Direito Eletrônico***.** São Paulo: Juarez de Oliveira, 2007. 211 p.

TEMMINGH, ROELOF. Putting the Tea back into Cyber Terrorism. Disponível em: <http://www.blackhat.com/presentations/bh-usa-03/bh-us-03-sensepost/bh-us-03-sensepost-paper .pdf>. Acesso em 07/07/2009.

TOLEDO, Francisco de Assis. *Princípios Básicos de Direito Penal*. 5 ed. 8 tir. São Paulo: Saraiva, 2000. 362 p.

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES (UIT). *CMSI: Documentos Finales*. Genebra: UIT, 2006. 102p. Disponível em: <*http://www.itu.int/wsis/outcome/booklet-es.pdf*>. Acesso em: 10/10/2009.

_____. *Miembros*. Genebra: UIT, 2008. 36 p. Disponível em: <http://www.itu.int /dmspub/itu-s/opb/gen/S-GEN-MEMB-2008-PDF-S.pdf.>. Acesso em: 18/01/2010.

_____. Protección de la Infancia en Línea. Genebra: UIT, 2009. 16 p. Disponível em: <http://www.itu.int/osg/csd/cybersecurity/gca/cop/cop-brochure.pdf>. Acesso em: 21/01/2010.

_____. *UIT – La Visión: Ayudamos al Mundo a Comunicarse*. Genebra: UIT, 2007. 20 p. Disponível em: <http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-HLPW-2007-PDF-S.pdf>. Acesso em: 18/01/2010.

_____. *UIT, Informe Anual de la Unión, 2008.* Genebra: UIT, 2009. 88 p. Disponível em: < http://www.itu.int/publ/S-CONF-AREP-2008/en>. Acesso em: 18/01/2010.

UNITED NATIONS OFFICE ON DRUGS AND CRIME. *Making the World Safer from Crime, Drugs and Terrorism*. Eslováquia: UNODC, 2007. 4 p. Disponível em: <http://www.unodc.org/pdf/unodc_brochure_2007.pdf>. Acesso em: 23/02/2011.

_____. *2010 Report*. 74 p. Disponível em: http://www.unodc.org/documents/frontpage/ UNODC_Annual_Report_2010_LowRes.pdf>. Acesso em: 23/02/2011.

VELASCO, Cristos; CRAVO, Vanessa. The Status of Cybercrime in Mexico, Brazil and the Outcome on Cybercrime and Security of the Fifth Meeting of the Internet Governance Forum, *Revista de Contratación Electrónica*, n. 113, maio 2011, p. 25-38. Disponível em: <http://libros-revistas-derecho.vlex.es/vid/cybercrime-mexico-governance-322030959>. Acesso em: 18/10/2011.

VIANNA, Túlio Lima. Do Delito de Dano e de sua Aplicação ao Direito Penal Informático. *Revista dos Tribunais*, São Paulo, a. 92, n. 807, p. 486-492, jan. 2003. Disponível em: <http:// www.tuliovianna.org/index.php?option=com_docman&task=doc_download&gid=43&Itemid =67>. Acesso em: 05/07/2009.

_____. Dos Crimes pela Internet. *In:* REINALDO FILHO, Demócrito (coord.). *Direito da Informática: temas polêmicos.* Bauru: EDIPRO, 2002. 432 p. p. 211-224.

_____. *Fundamentos de Direito Penal Informático: do acesso não autorizado a sistemas computacionais.* Rio de Janeiro: Forense, 2003. 167 p.

WAISBERG, IVO. O Novo Direito e o Velho Princípio. *In*: LEMOS, RONALDO; WAISBERG, IVO (org.). *Conflitos Sobre Nomes de Domínio e Outras Questões Jurídicas da Internet.* São Paulo: Editora FGV; Editora Revista dos Tribunais, 2003. 435 p. p. 417-426.

WEBSTER, William H.; BORCHGRAVE, Arnaud de. *Cyberterrorism and cyberwarfare thus become a plausible alternative*. Disponível em: <http://www.crime-research.org/library /Judge.htm>. Acesso em 06/07/2009.

ZAFFARONI, Eugênio Raúl; PIERANGELI, José Henrique. *Manual de Direito Penal Brasileiro – Parte Geral*. São Paulo: Editora Revista dos Tribunais, 2004.

ZANIOLO, Pedro Augusto. *Crimes modernos: o impacto da tecnologia no direito.* Curitiba: Juruá, 2007. 487 p.

ANEXO A – SUBSTITUTIVO DO SENADO AO PROJETO DE LEI DA CÂMARA Nº 89, DE 2003 (PL Nº 84, DE 1999, NA CASA DE ORIGEM).

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 dedezembro de 1940 (Código Penal), o Decreto-Lei nº 1.001, de 21 de outubro de1969 (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 demaio 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 PenalMilitar), a Lei nº 7.716, de 5 de janeiro de 1989, a Lei nº 8.069, de 13 de julho de1990, 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, ouque 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 aumentadade 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 dedezembro 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 utilizaçãode identidade de terceiros para a prática do crime, a pena é aumentadade sexta parte."

Art. 4º O caput do art. 163 do Decreto-Lei nº 2.848, de 7 de dezembro de1940 (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 nº2.848, 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 de1940 (Código Penal) passam a vigorar com as seguintes redações:

"Atentado contra a segurança de serviço de utilidadePública

Art. 265. Atentar contra a segurança ou o funcionamento deserviço 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 decomunicação, de rede de computadores, de sistema informatizado oude 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 de1940 (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 de1940 (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 TítuloV 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 coisaalheia 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 oudado 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 SISTEMASINFORMATIZADOS

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 aumentadade 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 umterço.

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 consequência 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 deregulamento, 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, passaa vigorar com a seguinte redação:

"Art. 241. Apresentar, produzir, vender, receptar, fornecer, divulgar, publicar ou armazenar consigo, por qualquer meio decomunicação, 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

ANEXO B – RESOLUÇÃO N.° 63 DA ASSEMBLÉIA GERAL DAS NAÇÕES UNIDAS, APROVADA NA 55° SESSÃO.

Resolution adopted by the General Assembly [*on the report of the Third Committee (A/55/593)*]

55/63. Combating the criminal misuse of information technologies

The General Assembly,

Recalling the United Nations Millennium Declaration, in which Member States resolved to ensure that the benefits of new technologies, especially information and communication technologies, in conformity with recommendations contained in the Ministerial Declaration of the high-level segment of the substantive session of 2000 of the Economic and Social Council, are available to all,

Recalling also its resolution 45/121 of 14 December 1990, in which it endorsed the recommendations of the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, and noting in particular there solution on computer-related crimes, in which the Eighth Congress called upon States to intensify their efforts to combat computer-related abuses more effectively,

Emphasizing the contributions that the United Nations, in particular the Commission on Crime Prevention and Criminal Justice, can make in the promotion of more efficient and effective law enforcement and administration of justice and of the highest standards of fairness and human dignity,

Recognizing that the free flow of information can promote economic and social development, education and democratic governance,

Noting significant advancements in the development and application of information technologies and means of telecommunication,

Expressing concern that technological advancements have created new possibilities for criminal activity, in particular the criminal misuse of information technologies,

Noting that reliance on information technologies, while it may vary from State to State, has resulted in a substantial increase in global cooperation and coordination, with the result that the criminal misuse of information technologies may have a grave impact on all States,

Recognizing that gaps in the access to and use of information technologies by States can diminish the effectiveness of international cooperation in combating the criminal misuse of information technologies, and noting the need to facilitate the transfer of information technologies, in particular to developing countries,

Noting the necessity of preventing the criminal misuse of information technologies,

Recognizing the need for cooperation between States and private industry in combating the criminal misuse of information technologies,

Underlining the need for enhanced coordination and cooperation among States in combating the criminal misuse of information technologies, and, in this context, stressing the role that can be played by both the United Nations and regional organizations,

Welcoming the work of the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders,

Noting the work of the Committee of Experts on Crime in Cyberspace of the Council of Europe on a draft convention on cybercrime, the principles agreed to by the Ministers of Justice and the Interior of the Group of Eight in Washington, D.C., on 10 December 1997, which were endorsed by the heads of State of the Group of Eight in Birmingham, United Kingdom of Great Britain and Northern Ireland, on 17 May 1998, the work of the Conference of the Group of Eight on a dialogue between government and industry on safety and confidence in cyberspace, held in Paris from 15 to 17 May 2000, and the recommendations approved on 3 March 2000 by the Third Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas, convened in San José, Costa Rica, from 1 to 3 March 2000 within the framework of the Organization of American States,

1. *Notes with appreciation* the efforts of the above-mentioned bodies to prevent the criminal misuse of information technologies, and also notes the value of, inter alia, the following measures to combat such misuse:

(*a*) States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies;

(*b*) Law enforcement cooperation in the investigation and prosecution of international cases of criminal misuse of information technologies should be coordinated among all concerned States;

(*c*) Information should be exchanged between States regarding the problems that they face in combating the criminal misuse of information technologies;

(*d*) Law enforcement personnel should be trained and equipped to address the criminal misuse of information technologies;

(*e*) Legal systems should protect the confidentiality, integrity and availability of data and computer systems from unauthorized impairment and ensure that criminal abuse is penalized;

(*f*) Legal systems should permit the preservation of and quick access to electronic data pertaining to particular criminal investigations;

(*g*) Mutual assistance regimes should ensure the timely investigation of the criminal misuse of information technologies and the timely gathering and exchange of evidence in such cases;

(*h*) The general public should be made aware of the need to prevent and combat the criminal misuse of information technologies;

(*i*) To the extent practicable, information technologies should be designed to help to prevent and detect criminal misuse, trace criminals and collect evidence;

(*j*) The fight against the criminal misuse of information technologies requires the development of solutions taking into account both the protection of individual freedoms and privacy and the preservation of the capacity of Governments to fight such criminal misuse;

2. *Invites* States to take into account the above-mentioned measures in their efforts to combat the criminal misuse of information technologies;

3. *Decides* to maintain the question of the criminal misuse of information technologies on the agenda of its fifty-sixth session, as part of the item entitled “Crime prevention and criminal justice”.

81st plenary meeting

4 December 2000

ANEXO C - RESOLUÇÃO N.° 239 DA ASSEMBLÉIA GERAL DAS NAÇÕES UNIDAS, APROVADA NA 57° SESSÃO.

Resolution adopted by the General Assembly [*on the report of the Second Committee (A/57/529/Add.3)*]

57/239. Creation of a global culture of cybersecurity

The General Assembly,

Noting the growing dependence of Governments, businesses, other organizations and individual users on information technologies for the provision of essential goods and services, the conduct of business and the exchange of information,

Recognizing that the need for cybersecurity increases as countries increase their participation in the information society,

Recalling its resolutions 55/63 of 4 December 2000 and 56/121 of 19 December 2001 on establishing the legal basis for combating the criminal misuse of information technologies,

Recalling also its resolutions 53/70 of 4 December 1998, 54/49 of 1 December 1999, 55/28 of 20 November 2000, 56/19 of 29 November 2001 and 57/53 of 22 November 2002 on developments in the field of information and telecommunications in the context of international security,

Aware that effective cybersecurity is not merely a matter of government or law enforcement practices, but must be addressed through prevention and supported throughout society,

Aware also that technology alone cannot ensure cybersecurity and that priority must be given to cybersecurity planning and management throughout society,

Recognizing that, in a manner appropriate to their roles, government, business, other organizations, and individual owners and users of information technologies must be aware of relevant cybersecurity risks and preventive measures and must assume responsibility for and take steps to enhance the security of these information technologies,

Recognizing also that gaps in access to and the use of information technologies by States can diminish the effectiveness of international cooperation in combating the criminal misuse of information technology and in creating a global culture of cybersecurity, and noting the need to facilitate the transfer of information technologies, in particular to developing countries,

Recognizing further the importance of international cooperation for achieving cybersecurity through the support of national efforts aimed at the enhancement of human capacity, increased learning and employment opportunities, improved public services and better quality

of life by taking advantage of advanced, reliable and secure information and communication technologies and networks and by promoting universal access,

Noting that, as a result of increasing interconnectivity, information systems and networks are now exposed to a growing number and a wider variety of threat sand vulnerabilities which raise new security issues for all,

Noting also the work of relevant international and regional organizations on enhancing cybersecurity and the security of information technologies,

1. *Takes note* of the elements annexed to the present resolution, with a view to creating a global culture of cybersecurity;

2. *Invites* all relevant international organizations to consider, inter alia, these elements for the creation of such a culture in any future work on cybersecurity;

3. *Invites* Member States to take into account these elements, inter alia, in their efforts to develop throughout their societies a culture of cybersecurity in the application and use of information technologies;

4. *Invites* Member States and all relevant international organizations to take, inter alia, these elements and the need for a global culture of cybersecurity into account in their preparations for the World Summit on the Information Society, to be held at Geneva from 10 to 12 December 2003 and at Tunis in 2005;

5. *Stresses* the necessity to facilitate the transfer of information technology and capacity-building to developing countries, in order to help them to take measures in cybersecurity.

78th plenary meeting

20 December 2002

Annex

Elements for creating a global culture of cybersecurity

Rapid advances in information technology have changed the way Governments, businesses, other organizations and individual users who develop, own, provide, manage, service and use information systems and networks ("participants") must approach cybersecurity. A global culture of cybersecurity will require that all participants address the following nine complementary elements:

(*a*) *Awareness.* Participants should be aware of the need for security of information systems and networks and what they can do to enhance security;

(*b*) *Responsibility*. Participants are responsible for the security of information systems and networks in a manner appropriate to their individual roles. They should review their own

policies, practices, measures and procedures regularly, and should assess whether they are appropriate to their environment;

(*c*) *Response*. Participants should act in a timely and cooperative manner to prevent, detect and respond to security incidents. They should share information about threats and vulnerabilities, as appropriate, and implement procedures for rapid and effective cooperation to prevent, detect and respond to security incidents. This may involve cross-border information-sharing and cooperation;

(*d*) *Ethics*. Given the pervasiveness of information systems and networks in modern societies, participants need to respect the legitimate interests of others and recognize that their action or inaction may harm others;

(*e*) *Democracy*. Security should be implemented in a manner consistent with the values recognized by democratic societies, including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency;

(*f*) *Risk assessment*. All participants should conduct periodic risk assessments that identify threats and vulnerabilities; are sufficiently broad-based to encompass key internal and external factors, such as technology, physical and human factors, policies and third-party services with security implications; allow determination of the acceptable level of risk; and assist in the selection of appropriate controls to manage the risk of potential harm to information systems and networks in the light of the nature and importance of the information to be protected;

(*g*) *Security design and implementation*. Participants should incorporate security as an essential element in the planning and design, operation and use of information systems and networks;

(*h*) *Security management*. Participants should adopt a comprehensive approach to security management based on risk assessment that is dynamic, encompassing all levels of participants' activities and all aspects of their operations;

(*i*) *Reassessment*. Participants should review and reassess the security of information systems and networks and should make appropriate modifications to security policies, practices, measures and procedures that include addressing new and changing threats and vulnerabilities.

ANEXO D - RESOLUÇÃO N.° 211 DA ASSEMBLÉIA GERAL DAS NAÇÕES UNIDAS, APROVADA NA 64° SESSÃO.

Resolution adopted by the General Assembly [*on the report of the Second Committee (A/64/422/Add.3)*]

64/211. Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures

The General Assembly,

Recalling its resolutions 55/63 of 4 December 2000 and 56/121 of 19 December 2001 on combating the criminal misuse of information technologies, 57/239 of 20 December 2002 on the creation of a global culture of cybersecurity and 58/199 of 23 December 2003 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures,

Recalling also its resolutions 53/70 of 4 December 1998, 54/49 of 1 December 1999, 55/28 of 20 November 2000, 56/19 of 29 November 2001, 57/53 of 22 November 2002, 58/32 of 8 December 2003, 59/61 of 3 December 2004, 60/45of 8 December 2005, 61/54 of 6 December 2006, 62/17 of 5 December 2007 and 63/37 of 2 December 2008 on developments with respect to information technologies in the context of international security,

Recalling further the outcomes of the World Summit on the Information Society, held in Geneva from 10 to 12 December 2003 (first phase) and in Tunis from 16 to 18 November 2005 (second phase),

Recognizing that confidence and security in the use of information and communications technologies are among the main pillars of the information society and that a robust global culture of cybersecurity needs to be encouraged, promoted, developed and vigorously implemented,

Recognizing also the increasing contribution made by networked information technologies to many of the essential functions of daily life, commerce and the provision of goods and services, research, innovation and entrepreneurship, and to the free flow of information among individuals and organizations, Governments, business and civil society,

Recognizing further that, in a manner appropriate to their roles, Governments, business, organizations and individual owners and users of information technologies must assume responsibility for and take steps to enhance the security of these information technologies,

Recognizing the importance of the mandate of the Internet Governance Forum as a multi-stakeholder dialogue to discuss various matters, including public policy issues related to key

elements of Internet governance in order to foster sustainability, robustness, security, stability and development of the Internet, and reiterating that all Governments should have an equal role and responsibility for international Internet governance and for ensuring the stability, security and continuity of the Internet,

Reaffirming the continuing need to enhance cooperation, to enable Governments, on an equal footing, to carry out their roles and responsibilities in international public policy issues pertaining to the Internet, but not the day-to-day technical and operational matters that do not impact on international public policy issues,

Recognizing that each country will determine its own critical information infrastructures,

Reaffirming the need to harness the potential of information and communications technologies to promote the achievement of the internationally agreed development goals, including the Millennium Development Goals, recognizing that gaps in access to and use of information technologies by States can diminish their economic prosperity, and reaffirming also the effectiveness of cooperation in combating the criminal misuse of information technology and in creating a global culture of cybersecurity,

Stressing the need for enhanced efforts to close the digital divide in order to achieve universal access to information and communications technologies and to protect critical information infrastructures by facilitating the transfer of information technology and capacity-building to developing countries, especially the least developed countries, in the areas of cybersecurity best practices and training,

Expressing concern that threats to the reliable functioning of critical information infrastructures and to the integrity of the information carried over those networks are growing in both sophistication and gravity, affecting domestic, national and international welfare,

Affirming that the security of critical information infrastructures is a responsibility Governments must address systematically and an area in which they must lead nationally, in coordination with relevant stakeholders, who in turn must be aware of relevant risks, preventive measures and effective responses in a manner appropriate to their respective roles,

Recognizing that national efforts should be supported by international information-sharing and collaboration, so as to effectively confront the increasingly transnational nature of such threats,

Noting the work of relevant regional and international organizations on enhancing cybersecurity, and reiterating their role in encouraging national efforts and fostering international cooperation,

Noting also the 2009 report of the International Telecommunication Union on securing information and communication networks and best practices for developing a culture of cybersecurity, which focused on a comprehensive national approach to cybersecurity consistent with free speech, the free flow of information and due process of law,

Recognizing that national efforts to protect critical information infrastructures benefit from a periodic assessment of their progress,

1. *Invites* Member States to use, if and when they deem appropriate, the annexed voluntary self-assessment tool for national efforts to protect critical information infrastructures in order to assist in assessing their efforts in this regard to strengthen their cybersecurity, so as to highlight areas for further action, with the goal of increasing the global culture of cybersecurity;

2. *Encourages* Member States and relevant regional and international organizations that have developed strategies to deal with cybersecurity and the protection of critical information infrastructures to share their best practices and measures that could assist other Member States in their efforts to facilitate the achievement of cybersecurity by providing such information to the Secretary-General for compilation and dissemination to Member States.

66th plenary meeting

21 December 2009

Annex

Voluntary self-assessment tool for national efforts to protect critical information infrastructures

Taking stock of cybersecurity needs and strategies

1. Assess the role of information and communications technologies in your national economy, national security, critical infrastructures (such as transportation, water and food supplies, public health, energy, finance, emergency services) and civil society.

2. Determine the cybersecurity and critical information infrastructure protection risks to your economy, national security, critical infrastructures and civil society that must be managed.

3. Understand the vulnerabilities of the networks in use, the relative levels of threat faced by each sector at present and the current management plan; note how changes in the economic environment, national security priorities and civil society needs affect these calculations.

4. Determine the goals of the national cybersecurity and critical information infrastructure protection strategy; describe its goals, the current level of implementation, measures that exist

to gauge its progress, its relation to other national policy objectives and how such a strategy fits within regional and international initiatives.

Stakeholder roles and responsibilities

5. Determine key stakeholders with a role in cybersecurity and critical information infrastructure protection and describe the role of each in the development of relevant policies and operations, including:

• National Government ministries or agencies, noting primary points of contact and responsibilities of each;

• Other government (local and regional) participants;

• Non-governmental actors, including industry, civil society and academia;

• Individual citizens, noting whether average users of the Internet have access to basic training in avoiding threats online and whether there is a national awareness-raising campaign regarding cybersecurity.

Policy processes and participation

6. Identify formal and informal venues that currently exist for Government industry collaboration in the development of cybersecurity and critical information infrastructure protection policy and operations; determine participants, role(s) and objectives, methods for obtaining and addressing input, and adequacy in achieving relevant cybersecurity and critical information infrastructure protection goals.

7. Identify other forums or structures that may be needed to integrate the government and non-government perspectives and knowledge necessary to realize national cybersecurity and critical information infrastructure protection goals.

Public-private cooperation

8. Collect all actions taken and plans to develop collaboration between government and the private sector, including any arrangements for information sharing and incident management.

9. Collect all current and planned initiatives to promote shared interests and address common challenges among both critical infrastructure participants and private-sector actors mutually dependent on the same interconnected critical infrastructure.

Incident management and recovery

10. Identify the Government agency that serves as the coordinator for incident management, including capability for watch, warning, response and recovery functions; the cooperating Government agencies; non-governmental cooperating participants, including industry and other partners; and any arrangements in place for cooperation and trusted information-sharing.

11. Separately, identify national-level computer incident response capacity, including any computer incident response team with national responsibilities and its roles and responsibilities, including existing tools and procedures for the protection of Government computer networks, and existing tools and procedures for the dissemination of incident-management information.

12. Identify networks and processes of international cooperation that may enhance incident response and contingency planning, identifying partners and arrangements for bilateral and multilateral cooperation, where appropriate.

Legal frameworks

13. Review and update legal authorities (including those related to cybercrime, privacy, data protection, commercial law, digital signatures and encryption) that may be outdated or obsolete as a result of the rapid uptake of and dependence upon new information and communications technologies, and use regional and international conventions, arrangements and precedents in these reviews. Ascertain whether your country has developed necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks, for example, General Assembly resolutions 55/63 and 56/121 on combating the criminal misuse of information technologies, and regional initiatives, including the Council of Europe Convention on Cybercrime.

14. Determine the current status of national cybercrime authorities and procedures, including legal authorities and national cybercrime units, and the level of understanding among prosecutors, judges and legislators of cybercrime issues.

15. Assess the adequacy of current legal codes and authorities in addressing the current and future challenges of cybercrime, and of cyberspace more generally.

16. Examine national participation in international efforts to combat cybercrime, such as the round-the-clock Cybercrime Point of Contact Network.

17. Determine the requirements for national law enforcement agencies to cooperate with international counterparts to investigate transnational cybercrime in those instances in which infrastructure is situated or perpetrators reside in national territory, but victims reside elsewhere.

Developing a global culture of cybersecurity

18. Summarize actions taken and plans to develop a national culture of cybersecurity referred to in General Assembly resolutions 57/239 and 58/199, including implementation of a cybersecurity plan for Government-operated systems, national awareness-raising

programmes, outreach programmes to, among others, children and individual users, and national cybersecurity and critical information infrastructure protection training requirements.

ANEXO E - RESOLUÇÃO N.° 41 DA ASSEMBLÉIA GERAL DAS NAÇÕES UNIDAS, APROVADA NA 65° SESSÃO.

Resolution adopted by the General Assembly [*on the report of the First Committee (A/65/405)*]

65/41. Developments in the field of information and telecommunications in the context of international security

The General Assembly,

Recalling its resolutions 53/70 of 4 December 1998, 54/49 of 1 December 1999, 55/28 of 20 November 2000, 56/19 of 29 November 2001, 57/53 of 22 November 2002, 58/32 of 8 December 2003, 59/61 of 3 December 2004, 60/45 of 8 December 2005, 61/54 of 6 December 2006, 62/17 of 5 December 2007, 63/37 of 2 December 2008 and 64/25 of 2 December 2009,

Recalling also its resolutions on the role of science and technology in the context of international security, in which, inter alia, it recognized that scientific and technological developments could have both civilian and military applications and that progress in science and technology for civilian applications needed to be maintained and encouraged,

Noting that considerable progress has been achieved in developing and applying the latest information technologies and means of telecommunication,

Affirming that it sees in this process the broadest positive opportunities for the further development of civilization, the expansion of opportunities for cooperation for the common good of all States, the enhancement of the creative potential of humankind and additional improvements in the circulation of information in the global community,

Recalling, in this connection, the approaches and principles outlined at the Information Society and Development Conference, held in Midrand, South Africa, from 13 to 15 May 1996,

Bearing in mind the results of the Ministerial Conference on Terrorism, held in Paris on 30 July 1996, and the recommendations that it made,

Bearing in mind also the results of the World Summit on the Information Society, held in Geneva from 10 to 12 December 2003 (first phase) and in Tunis from 16 to 18 November 2005 (second phase),

Noting that the dissemination and use of information technologies and means affect the interests of the entire international community and that optimum effectiveness is enhanced by broad international cooperation,

Expressing concern that these technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure of States to the detriment of their security in both civil and military fields,

Considering that it is necessary to prevent the use of information resources or technologies for criminal or terrorist purposes,

Noting the contribution of those Member States that have submitted their assessments on issues of information security to the Secretary-General pursuant to paragraphs 1 to 3 of resolutions 53/70, 54/49, 55/28, 56/19, 57/53, 58/32, 59/61,60/45, 61/54, 62/17, 63/37 and 64/25,

Taking note of the reports of the Secretary-General containing those assessments,

Welcoming the initiative taken by the Secretariat and the United Nations Institute for Disarmament Research in convening international meetings of experts in Geneva in August 1999 and April 2008 on developments in the field of information and telecommunications in the context of international security, as well as the results of those meetings,

Considering that the assessments of the Member States contained in there ports of the Secretary-General and the international meetings of experts have contributed to a better understanding of the substance of issues of international information security and related notions,

Bearing in mind that the Secretary-General, in fulfilment of resolution 60/45, established in 2009, on the basis of equitable geographical distribution, a group of governmental experts, which, in accordance with its mandate, considered existing and potential threats in the sphere of information security and possible cooperative measures to address them and conducted a study on relevant international concepts aimed at strengthening the security of global information and telecommunications systems,

Welcoming the effective work of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security and the relevant outcome report transmitted by the Secretary-General,

Taking note of the assessments and recommendations contained in the report of the Group of Governmental Experts,

1. *Calls upon* Member States to promote further at multilateral levels the consideration of existing and potential threats in the field of information security, as well as possible strategies to address the threats emerging in this field, consistent with the need to preserve the free flow of information;

2. *Considers* that the purpose of such strategies could be served through further examination of relevant international concepts aimed at strengthening the security of global information and telecommunications systems;

3. *Invites* all Member States, taking into account the assessments and recommendations contained in the report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,4 to continue to inform the Secretary-General of their views and assessments on the following questions:

(*a*) General appreciation of the issues of information security;

(*b*) Efforts taken at the national level to strengthen information security and promote international cooperation in this field;

(*c*) The content of the concepts mentioned in paragraph 2 above;

(*d*) Possible measures that could be taken by the international community to strengthen information security at the global level;

4. *Requests* the Secretary-General, with the assistance of a group of governmental experts, to be established in 2012 on the basis of equitable geographical distribution, taking into account the assessments and recommendations contained in the above-mentioned report, to continue to study existing and potential threats in the sphere of information security and possible cooperative measures to address them, as well as the concepts referred to in paragraph 2 above, and to submit a report on the results of this study to the Assembly at its sixty-eighth session;

5. *Decides* to include in the provisional agenda of its sixty-sixth session the item entitled "Developments in the field of information and telecommunications in the context of international security".

60th plenary meeting

8 December 2010

ANEXO F - RESOLUÇÃO N.° 230 DA ASSEMBLÉIA GERAL DAS NAÇÕES UNIDAS, APROVADA NA 65° SESSÃO.

Resolution adopted by the General Assembly [*on the report of the Third Committee (A/65/457)*]

65/230. Twelfth United Nations Congress on Crime Prevention and Criminal Justice

The General Assembly,

Emphasizing the responsibility assumed by the United Nations in the field of crime prevention and criminal justice in pursuance of Economic and Social Council resolution 155 C (VII) of 13 August 1948 and General Assembly resolution 415 (V) of 1 December 1950,

Acknowledging that the United Nations congresses on crime prevention and criminal justice, as major intergovernmental forums, have influenced national policies and practices and promoted international cooperation in this field by facilitating the exchange of views and experience, mobilizing public opinion and recommending policy options at the national, regional and international levels,

Recalling its resolution 46/152 of 18 December 1991, in the annex to which Member States affirmed that the United Nations congresses on crime prevention and criminal justice should be held every five years and should provide a forum for, inter alia, the exchange of views between States, intergovernmental and non-governmental organizations and individual experts representing various professions and disciplines, the exchange of experiences in research, law and policy development, and the identification of emerging trends and issues in crime prevention and criminal justice,

Recalling also its resolution 57/270 B of 23 June 2003 on the integrated and coordinated implementation of and follow-up to the outcomes of major United Nations conferences and summits in the economic and social fields, in which it stressed that all countries should promote policies consistent and coherent with the commitments of the major United Nations conferences and summits, emphasized that the United Nations system had an important responsibility to assist Governments to stay fully engaged in the follow-up to and implementation of agreements and commitments reached at the major United Nations conferences and summits and invited its intergovernmental bodies to further promote the implementation of the outcomes of the major United Nations conferences and summits,

Recalling further its resolution 64/180 of 18 December 2009, in which it called upon the Twelfth United Nations Congress on Crime Prevention and Criminal Justice to formulate concrete proposals for further follow-up and action, paying particular attention to practical

arrangements relating to the effective implementation of the international legal instruments pertaining to transnational organized crime, terrorism and corruption and technical assistance activities relating thereto, and requested the Commission on Crime Prevention and Criminal Justice at its nineteenth session to give high priority to considering the conclusions and recommendations of the Twelfth Congress, with a view to recommending, through the Economic and Social Council, appropriate follow-up by the General Assembly at its sixty-fifth session,

Bearing in mind the United Nations Millennium Declaration, adopted by the Heads of State and Government at the Millennium Summit of the United Nations on 8 September 2000, in which Heads of State and Government resolved, inter alia, to strengthen respect for the rule of law in international as well as in national affairs, to take concerted action against international terrorism and accede as soon as possible to all the relevant international conventions, to redouble their efforts to implement their commitment to counter the world drug problem, and to intensify their efforts to fight transnational crime in all its dimensions, including trafficking as well as smuggling in human beings and money-laundering,

Having considered the report of the Twelfth Congress 2 and the related recommendations made by the Commission at its nineteenth session,

1. *Expresses its satisfaction* with the results achieved by the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Salvador, Brazil, from 12 to 19 April 2010, including the Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World, adopted at the high-level segment of the Twelfth Congress;

2. *Expresses its appreciation* to the United Nations Office on Drugs and Crime for the work done in the preparations for and follow-up to the Twelfth Congress, and thanks the institutes of the United Nations crime prevention and criminal justice programme network for their contribution to the Congress, in particular with regard to the workshops held within the framework of the Congress;

3. *Takes note with appreciation* of the report of the Twelfth Congress, which contains the results of the Congress, including the conclusions and recommendations made at the workshops and at the high-level segment held during the Congress;

4. *Endorses* the Salvador Declaration adopted by the Twelfth Congress, as approved by the Commission on Crime Prevention and Criminal Justice and annexed to the present resolution;

5. *Invites* Governments to take into consideration the Salvador Declaration and the recommendations adopted by the Twelfth Congress when formulating legislation and policy

directives and to make all efforts, where appropriate, to implement the principles contained therein, taking into account the economic, social, legal and cultural specificities of their respective States;

6. *Invites* Member States to identify areas covered in the Salvador Declaration where further tools and training manuals based on international standards and best practices are needed, and to submit that information to the Commission on Crime Prevention and Criminal Justice so that it may take that information into account when considering potential areas of future activity of the United Nations Office on Drugs and Crime;

7. *Welcomes* the decision of the Government of Brazil to contribute a percentage of the value of confiscated assets to the United Nations Office on Drugs and Crime, pursuant to article 30 of the United Nations Convention against Transnational Organized Crime and article 62 of the United Nations Convention against Corruption, as well as paragraph 9 of General Assembly resolution 55/25 of 15 November 2000 and paragraph 4 of Assembly resolution 58/4 of 31 October 2003, and looks forward to expeditious implementation of that decision;

8. *Also welcomes* the prompt consideration and action by the Commission on Crime Prevention and Criminal Justice on a number of issues addressed in the Salvador Declaration, including those addressed in separate resolutions approved by the Commission at its nineteenth session, such as violence against migrants, migrant workers and their families, emerging forms of crime that have a significant impact on the environment and international cooperation in criminal matters;

9. *Requests* the Commission on Crime Prevention and Criminal Justice to establish, in line with paragraph 42 of the Salvador Declaration, an open-ended intergovernmental expert group, to be convened prior to the twentieth session of the Commission, to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime;

10. *Also requests* the Commission on Crime Prevention and Criminal Justice to establish, in line with paragraph 49 of the Salvador Declaration, an open-ended intergovernmental expert group, to be convened between the twentieth and twenty-first sessions of the Commission, to exchange information on best practices, as well as national legislation and existing international law, and on the revision of existing United Nations standard minimum rules for

the treatment of prisoners so that they reflect recent advances in correctional science and best practices, with a view to making recommendations to the Commission on possible next steps;

11. *Requests* the open-ended intergovernmental expert groups established pursuant to paragraphs 9 and 10 above to report to the Commission on Crime Prevention and Criminal Justice on progress in their work;

12. *Requests* the United Nations Office on Drugs and Crime, in the development and implementation of its technical assistance programmes, to aim for sustainable and long-lasting results in the prevention, prosecution and punishment of crime, in particular by building, modernizing and strengthening criminal justice systems, as well as promoting the rule of law, and to design such programmes to achieve those aims for all components of the criminal justice system, in an integrated way and with a long-term perspective, increasing the capacity of requesting States to prevent and suppress the various types of crime affecting societies, including organized crime and cybercrime;

13. *Also requests* the United Nations Office on Drugs and Crime to continue to provide technical assistance to facilitate the ratification and implementation of the United Nations Convention against Corruption, the United Nations Convention against Transnational Organized Crime and the international instruments related to the prevention and suppression of terrorism;

14. *Requests* the Commission on Crime Prevention and Criminal Justice to consider at its twentieth session options to improve the efficiency of the process involved in the United Nations congresses on crime prevention and criminal justice, taking into account the recommendations made by the Intergovernmental Group of Experts on Lessons Learned from United Nations Congresses on Crime Prevention and Criminal Justice at its meeting, held in Bangkok from 15 to 18 August 2006;

15. *Requests* the Secretary-General to distribute the report of the Twelfth Congress, including the Salvador Declaration, to Member States, intergovernmental organizations and non-governmental organizations, so as to ensure that the recommendations of the Congress are disseminated as widely as possible, and to seek proposals by Member States for ways and means of ensuring appropriate follow-up to the Salvador Declaration for consideration and action by the Commission on Crime Prevention and Criminal Justice at its twentieth session;

16. *Welcomes with appreciation* the offer of the Government of Qatar to act as host to the Thirteenth United Nations Congress on Crime Prevention and Criminal Justice, in 2015;

17. *Expresses its profound gratitude* to the people and Government of Brazil for the warm and generous hospitality extended to the participants in the Twelfth Congress and for the excellent facilities provided for the Congress;

18. *Requests* the Secretary-General to submit to the General Assembly at its sixty-sixth session a report on the implementation of the present resolution.

71st plenary meeting

21 December 2010

Annex

Salvador Declaration on Comprehensive Strategies for Global Challenges:
Crime Prevention and Criminal Justice Systems and Their Development in a Changing World

We, the States Members of the United Nations,

Having assembled at the Twelfth United Nations Congress on Crime Prevention and Criminal Justice in Salvador, Brazil, from 12 to 19 April 2010, to take more effective concerted action, in a spirit of cooperation, to prevent, prosecute and punish crime and seek justice,

Recalling the work of the eleven previous United Nations congresses on crime prevention and criminal justice, the conclusions and recommendations of the regional preparatory meetings for the Twelfth Congress 8 and the documents prepared by the relevant working groups established by the Commission on Crime Prevention and Criminal Justice,

Reaffirming the necessity of respecting and protecting human rights and fundamental freedoms in the prevention of crime and the administration of, and access to, justice, including criminal justice,

Recognizing the centrality of crime prevention and the criminal justice system to the rule of law and that long-term sustainable economic and social development and the establishment of a functioning, efficient, effective and humane criminal justice system have a positive influence on each other,

Noting with concern the rise of new and emerging forms of transnational crime,

Greatly concerned by the negative impact of organized crime on human rights, the rule of law, security and development, as well as by the sophistication, diversity and transnational aspects of organized crime and its links with other criminal and, in some cases, terrorist activities,

Stressing the need to strengthen international, regional and subregional cooperation to effectively prevent, prosecute and punish crime, in particular by enhancing the national capacity of States through the provision of technical assistance,

Greatly concerned by criminal acts against migrants, migrant workers and their families and other groups in vulnerable situations, particularly those acts motivated by discrimination and other forms of intolerance,

Declare as follows:

1. We recognize that an effective, fair and humane criminal justice system is based on the commitment to uphold the protection of human rights in the administration of justice and the prevention and control of crime.

2. We also recognize that it is the responsibility of each Member State to update, where appropriate, and maintain an effective, fair, accountable and humane crime prevention and criminal justice system.

3. We acknowledge the value and impact of the United Nations standards and norms in crime prevention and criminal justice and endeavour to use those standards and norms as guiding principles in designing and implementing our national crime prevention and criminal justice policies, laws, procedures and programmes.

4. Bearing in mind the universal character of the United Nations standards and norms in crime prevention and criminal justice, we invite the Commission on Crime Prevention and Criminal Justice to consider reviewing and, if necessary, updating and supplementing them. In order to render them effective, we recommend that appropriate efforts be made to promote the widest application of those standards and norms and to raise awareness of them among authorities and entities responsible for their application at the national level.

5. We acknowledge the need for Member States to ensure effective gender equality in crime prevention, access to justice and the protection offered by the criminal justice system.

6. We express deep concern about the pervasiveness of violence against women in all its different forms and manifestations worldwide, and urge States to enhance efforts to prevent, prosecute and punish violence against women. In this regard, we note with appreciation the draft updated Model Strategies and Practical Measures on the Elimination of Violence against Women in the Field of Crime Prevention and Criminal Justice, as finalized by the intergovernmental expert group at its meeting held in Bangkok from 23 to 25 March 2009,10 and look forward to their consideration by the Commission on Crime Prevention and Criminal Justice.

7. We recognize the importance of adopting appropriate legislation and policies to prevent victimization, including revictimization, and to provide protection and assistance to victims.

8. We consider that international cooperation and technical assistance can play an important role in achieving sustainable and long-lasting results in the prevention, prosecution and

punishment of crime, in particular by building, modernizing and strengthening our criminal justice systems and promoting the rule of law. Specific technical assistance programmes should thus be designed to achieve these aims, for all the components of the criminal justice system, in an integrated way and with a long-term perspective, enabling the capacity of requesting States to prevent and suppress the various types of crime affecting their societies, including organized crime. In that regard, the experience and expertise accumulated over the years by the United Nations Office on Drugs and Crime constitute a valuable asset.

9. We strongly recommend the allocation of sufficient human and financial resources to develop and implement effective policies, programmes and training dealing with crime prevention, criminal justice and the prevention of terrorism. In this regard, we stress the serious need to provide the United Nations Office on Drugs and Crime with a level of resources commensurate with its mandate. We call upon Member States and other international donors to support, and coordinate with, the United Nations Office on Drugs and Crime, including its regional and country offices, the institutes of the United Nations crime prevention and criminal justice programme network and requesting States in the provision of technical assistance to strengthen their capacity to prevent crime.

10. We acknowledge the leading role of the United Nations Office on Drugs and Crime in providing technical assistance to facilitate the ratification and implementation of the international instruments related to the prevention and suppression of terrorism.

11. We invite the Commission on Crime Prevention and Criminal Justice to consider strengthening the capacity of the United Nations Office on Drugs and Crime to collect, analyse and disseminate accurate, reliable and comparable data on world crime and victimization trends and patterns, and we call upon Member States to support the gathering and analysis of information and to consider designating focal points and provide information when requested to do so by the Commission.

12. We welcome the decision of the Commission on Crime Prevention and Criminal Justice to engage in a thematic debate on protection against trafficking in cultural property and the recommendations made by the open-ended intergovernmental expert group on protection against trafficking in cultural property at its meeting, held in Vienna from 24 to 26 November 2009, 11 and invite the Commission to conduct appropriate follow-up, including exploring the need for guidelines for crime prevention with respect to trafficking in cultural property.

Furthermore, we urge States that have not yet done so to develop effective legislation to prevent, prosecute and punish this crime in any of its forms and to strengthen international cooperation and technical assistance in this area, including the recovery and return of cultural

property, bearing in mind the existing relevant international instruments, including the United Nations Convention against Transnational Organized Crime, where appropriate.

13. We recognize the increasing risk of the convergence of transnational organized crime and illicit networks, many of which are new or evolving. We call upon Member States to cooperate, including through information-sharing, in an effort to address these evolving transnational criminal threats.

14. We acknowledge the challenge posed by emerging forms of crime that have a significant impact on the environment. We encourage Member States to strengthen their national crime prevention and criminal justice legislation, policies and practices in this area. We invite Member States to enhance international cooperation, technical assistance and the sharing of best practices in this area. We invite the Commission on Crime Prevention and Criminal Justice, in coordination with the relevant United Nations bodies, to study the nature of the challenge and ways to deal with it effectively.

15. We express our serious concerns about the challenge posed by economic fraud and identity-related crime and their links to other criminal and, in some cases, terrorist activities. We therefore invite Member States to take appropriate legal measures to prevent, prosecute and punish economic fraud and identity-related crime and to continue to support the work of the United Nations Office on Drugs and Crime in this area. Furthermore, Member States are encouraged to enhance international cooperation in this area, including through the exchange of relevant information and best practices, as well as through technical and legal assistance.

16. We recognize that international cooperation in criminal matters in accordance with international obligations and national laws is a cornerstone of the efforts of States to prevent, prosecute and punish crime, in particular in its transnational forms, and we encourage the continuation and reinforcement of such activities at all levels.

17. We call upon those States that have not yet done so to consider ratifying or acceding to the United Nations Convention against Corruption, welcome the establishment of its mechanism for the review of implementation, look forward to its effective implementation and acknowledge the work of the intergovernmental working groups on asset recovery and technical assistance.

18. We also call upon those States that have not yet done so to consider ratifying or acceding to the United Nations Convention against Transnational Organized Crime and the Protocols thereto, 12 and note with appreciation the decision of the General Assembly, in its resolution 64/179 of 18 December 2009, to hold in 2010 high-level meetings and a special treaty event. We also take note of ongoing initiatives aimed at exploring options regarding an appropriate

and effective mechanism to assist the Conference of the Parties to the United Nations Convention against Transnational Organized Crime in the review of the implementation of the Convention.

19. We call upon Member States that have not yet done so to consider ratifying or acceding to the international instruments against terrorism, including its financing. We also call upon all States parties to use those instruments and the relevant United Nations resolutions to enhance international cooperation in countering terrorism in all its forms and manifestations and its financing, including evolving features of the latter.

20. We call upon Member States, consistent with their international obligations, to establish or strengthen, as appropriate, central authorities fully empowered and equipped to deal with requests for international cooperation in criminal matters. In this perspective, regional legal cooperation networks could be supported.

21. Aware that gaps may exist in relation to international cooperation in criminal matters, we invite the Commission on Crime Prevention and Criminal Justice to consider reviewing this issue and explore the need for various means of addressing gaps that are identified.

22. We emphasize the need for the adoption of effective measures to implement the provisions on preventing, prosecuting and punishing money-laundering contained in the United Nations Convention against Transnational Organized Crime and the United Nations Convention against Corruption. We encourage Member States to develop strategies to combat money-laundering based on the provisions of these two Conventions.

23. We encourage Member States to consider developing strategies or policies to combat illicit capital flows and to curb the harmful effects of jurisdictions and territories uncooperative in tax matters.

24. We recognize the need to deny criminals and criminal organizations the proceeds of their crimes. We call upon all Member States, within their national legal systems, to adopt effective mechanisms for the seizure, restraint and confiscation of proceeds of crime and to strengthen international cooperation to ensure effective and prompt asset recovery. We also call upon States to preserve the value of seized and confiscated assets, including through disposal, where appropriate and possible, where there is a risk of their value diminishing.

25. Bearing in mind the need to reinforce criminal justice systems of developing countries and countries with economies in transition, we urge States parties to the United Nations Convention against Transnational Organized Crime and the United Nations Convention against Corruption to fully implement the technical assistance provisions of each Convention, including by giving special consideration to contributing, in accordance with their national

law and the provisions of those Conventions, a percentage of the proceeds of crime confiscated under each Convention to fund technical assistance through the United Nations Office on Drugs and Crime.

26. We are convinced of the importance of preventing youth crime, supporting the rehabilitation of young offenders and their reintegration into society, protecting child victims and witnesses, including efforts to prevent their revictimization, and addressing the needs of children of prisoners. We stress that such responses should take into account the human rights and best interests of children and youth, as called for in the Convention on the Rights of the Child and the Optional Protocols thereto, where applicable, and in other relevant United Nations standards and norms in juvenile justice, where appropriate.

27. We support the principle that the deprivation of liberty of children should be used only as a measure of last resort and for the shortest appropriate period of time. We recommend the broader application, as appropriate, of alternatives to imprisonment, restorative justice and other relevant measures that foster the diversion of young offenders from the criminal justice system.

28. We call upon States to develop and strengthen, where appropriate, legislation, policies and practices to punish all forms of crime that target children and youth, as well as for the protection of child victims and witnesses.

29. We encourage States to provide tailored training in an interdisciplinary approach to those involved in the administration of juvenile justice.

30. We invite the Commission on Crime Prevention and Criminal Justice to consider requesting the United Nations Office on Drugs and Crime to design and provide to States specific technical assistance programmes to achieve these aims.

31. We call upon civil society, including the media, to support the efforts to protect children and youth from exposure to content that may exacerbate violence and crime, particularly content depicting and glorifying acts of violence against women and children.

32. We are convinced of the need to accelerate efforts to fully implement the United Nations guidelines on crime prevention and the prevention components of existing conventions and other relevant international standards and norms.

33. We recognize that the development and adoption of crime prevention policies and their monitoring and evaluation are the responsibility of States. We believe that such efforts should be based on a participatory, collaborative and integrated approach that includes all relevant stakeholders, including those from civil society.

34. We recognize the importance of strengthening public-private partnerships in preventing and countering crime in all its forms and manifestations. We are convinced that, through the mutual and effective sharing of information, knowledge and experience and through joint and coordinated actions, Governments and businesses can develop, improve and implement measures to prevent, prosecute and punish crime, including emerging and changing challenges.

35. We stress the need for all States to have national and local action plans for crime prevention that take into account, inter alia, factors that place certain populations and places at higher risk of victimization and/or offending in a comprehensive, integrated and participatory manner, and for such plans to be based on the best available evidence and good practices. We stress that crime prevention should be considered an integral element of strategies to foster social and economic development in all States.

36. We urge Member States to consider adopting legislation, strategies and policies for the prevention of trafficking in persons, the prosecution of offenders and the protection of victims of trafficking, consistent with the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime. We call upon Member States, where applicable, in cooperation with civil society and non-governmental organizations, to follow a victim-centred approach with full respect for the human rights of the victims of trafficking, and to make better use of the tools developed by the United Nations Office on Drugs and Crime.

37. We urge Member States to consider adopting and implementing effective measures to prevent, prosecute and punish the smuggling of migrants and to ensure the rights of smuggled migrants, consistent with the Protocol against the Smuggling of Migrants by Land, Sea and Air, supplementing the United Nations Convention against Transnational Organized Crime. In this context, we recommend that Member States, inter alia, undertake awareness-raising campaigns, in cooperation with civil society and non-governmental organizations.

38. We affirm our determination to eliminate violence against migrants, migrant workers and their families, and we call upon Member States to adopt measures for preventing and addressing effectively cases of such violence and to ensure that those individuals receive humane and respectful treatment from States, regardless of their status. We also invite Member States to take immediate steps to incorporate into international crime prevention strategies and norms measures to prevent, prosecute and punish crimes involving violence against migrants, as well as violence associated with racism, xenophobia and related forms of

intolerance. We invite the Commission on Crime Prevention and Criminal Justice to consider this issue further in a comprehensive manner.

39. We note that the development of information and communications technologies and the increasing use of the Internet create new opportunities for offenders and facilitate the growth of crime.

40. We realize the vulnerability of children, and we call upon the private sector to promote and support efforts to prevent child sexual abuse and exploitation through the Internet.

41. We recommend that the United Nations Office on Drugs and Crime, upon request, provide, in cooperation with Member States, relevant international organizations and the private sector, technical assistance and training to States to improve national legislation and build the capacity of national authorities in order to deal with cybercrime, including the prevention, detection, investigation and prosecution of such crime in all its forms, and to enhance the security of computer networks.

42. We invite the Commission on Crime Prevention and Criminal Justice to consider convening an open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime.

43. We endeavour to take measures to promote wider education and awareness of the United Nations standards and norms in crime prevention and criminal justice to ensure a culture of respect for the rule of law. In this regard, we recognize the role of civil society and the media in cooperating with States in these efforts. We invite the United Nations Office on Drugs and Crime to continue to play a key role in the development and implementation of measures to promote and develop such a culture, in close coordination with other relevant United Nations entities.

44. We undertake to promote appropriate training of officials entrusted with upholding the rule of law, including correctional facility officers, law enforcement officials and the judiciary, as well as prosecutors and defence lawyers, in the use and application of those standards and norms.

45. We are concerned by urban crime and its impact on specific populations and places. We therefore recommend stronger coordination between security and social policies, with a view to addressing some of the root causes of urban violence.

46. We recognize that specific groups are particularly vulnerable to situations of urban crime, and we therefore recommend the adoption and implementation of civic intercultural programmes, where appropriate, aimed at combating racism and xenophobia, reducing the exclusion of minorities and migrants and thus promoting community cohesion.

47. We acknowledge the increasing links between transnational organized crime and drug trafficking in the context of the world drug problem. In this regard, we stress the urgent need for all States to enhance bilateral, regional and international cooperation to effectively counter the challenges posed by these links.

48. We recognize that the penitentiary system is one of the key components of the criminal justice system. We endeavour to use the United Nations standards and norms for the treatment of prisoners as a source of guidance in the development or updating of our national codes of penitentiary administration.

49. We invite the Commission on Crime Prevention and Criminal Justice to consider convening an open-ended intergovernmental expert group to exchange information on best practices, as well as national legislation and existing international law, and on the revision of existing United Nations standard minimum rules for the treatment of prisoners so that they reflect recent advances in correctional science and best practices, with a view to making recommendations to the Commission on possible next steps.

50. We welcome the draft United Nations Rules for the Treatment of Women Prisoners and Non-custodial Measures for Women Offenders.17 Taking note of the outcome and the recommendations of the meeting of the expert group to develop supplementary rules specific to the treatment of women in detention and in custodial and non-custodial settings, 18 we recommend that the Commission on Crime Prevention and Criminal Justice consider them as a matter of priority for appropriate action.

51. We stress the need to reinforce alternatives to imprisonment, which may include community service, restorative justice and electronic monitoring, and support rehabilitation and reintegration programmes, including those to correct offending behaviour, and educational and vocational programmes for prisoners.

52. We recommend that Member States endeavour to reduce pretrial detention, where appropriate, and promote increased access to justice and legal defence mechanisms.

53. We support effective and efficient follow-up of the outcomes of the United Nations congresses on crime prevention and criminal justice. We welcome the inclusion of a standing item on the agenda of the Commission on Crime Prevention and Criminal Justice at its annual

sessions on this matter and on preparations for future congresses on crime prevention and criminal justice.

54. We welcome with appreciation the offer of the Government of Qatar to act as host to the Thirteenth United Nations Congress on Crime Prevention and Criminal Justice, in 2015.

55. We express our profound gratitude to the people and Government of Brazil for their warm and generous hospitality and for the excellent facilities provided for the Twelfth Congress.

ANEXO G - CONVENÇÃO SOBRE CRIMES CIBERNÉTICOS

CONVENTION ON CYBERCRIME

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 well-unctioning 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 co-operation 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, sub-paragraphs 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; and

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 art 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 co-operation 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 e-mail, 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 preservation 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, seven-day-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 applicablemultilateral 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 it 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 the 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 whichthe 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 informed 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 out 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 invited to accede to it.

ANEXO H – PROTOCOLO ADICIONAL

ADDITIONAL PROTOCOL TO THE CONVENTION ON CYBERCRIME, CONCERNING THE CRIMINALISATION OF ACTS OF A RACIST AND XENOPHOBIC NATURE COMMITTED THROUGH COMPUTER SYSTEMS

The member States of the Council of Europe and the other States Parties to the Convention on Cybercrime, opened for signature in Budapest on 23 November 2001, signatory hereto;

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recalling that all human beings are born free and equal in dignity and rights;

Stressing the need to secure a full and effective implementation of all human rights without any discrimination or distinction, as enshrined in European and other international instruments;

Convinced that acts of a racist and xenophobic nature constitute a violation of human rights and a threat to the rule of law and democratic stability;

Considering that national and international law need to provide adequate legal responses to propaganda of a racist and xenophobic nature committed through computer systems;

Aware of the fact that propaganda to such acts is often subject to criminalisation in national legislation;

Having regard to the Convention on Cybercrime, which provides for modern and flexible means of international co-operation and convinced of the need to harmonise substantive law provisions concerning the fight against racist and xenophobic propaganda;

Aware that computer systems offer an unprecedented means of facilitating freedom of expression and communication around the globe;

Recognising that freedom of expression constitutes one of the essential foundations of a democratic society, and is one of the basic conditions for its progress and for the development of every human being;

Concerned, however, by the risk of misuse or abuse of such computer systems to disseminate racist and xenophobic propaganda;

Mindful of the need to ensure a proper balance between freedom of expression and an effective fight against acts of a racist and xenophobic nature;

Recognising that this Protocol is not intended to affect established principles relating to freedom of expression in national legal systems;

Taking into account the relevant international legal instruments in this field, and in particular the Convention for the Protection of Human Rights and Fundamental Freedoms and its Protocol No. 12 concerning the general prohibition of discrimination, the existing Council of Europe conventions on co-operation in the penal field, in particular the Convention on Cybercrime, the United Nations International Convention on the Elimination of All Forms of Racial Discrimination of 21 December 1965, the European Union Joint Action of 15 July 1996 adopted by the Council on the basis of Article K.3 of the Treaty on European Union, concerning action to combat racism and xenophobia;

Welcoming the recent developments which further advance international understanding and co-operation in combating cybercrime and racism and xenophobia;

Having 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, 10-11 October 1997) to seek common responses to the developments of the new technologies based on the standards and values of the Council of Europe;

Have agreed as follows:

Chapter I – Common provisions

Article 1 – Purpose

The purpose of this Protocol is to supplement, as between the Parties to the Protocol, the provisions of the Convention on Cybercrime, opened for signature in Budapest on 23 November 2001 (hereinafter referred to as "the Convention"), as regards the criminalisation of acts of a racist and xenophobic nature committed through computer systems.

Article 2 – Definition

1 For the purposes of this Protocol:

"*racist and xenophobic material*" means any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors.

2 The terms and expressions used in this Protocol shall be interpreted in the same manner as they are interpreted under the Convention.

Chapter II – Measures to be taken at national level

Article 3 – Dissemination of racist and xenophobic material through computer systems

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:

distributing, or otherwise making available, racist and xenophobic material to the public through a computer system.

2 A Party may reserve the right not to attach criminal liability to conduct as defined by paragraph 1 of this article, where the material, as defined in Article 2, paragraph 1, advocates, promotes or incites discrimination that is not associated with hatred or violence, provided that other effective remedies are available.

3 Notwithstanding paragraph 2 of this article, a Party may reserve the right not to apply paragraph 1 to those cases of discrimination for which, due to established principles in its national legal system concerning freedom of expression, it cannot provide for effective remedies as referred to in the said paragraph 2.

Article 4 – Racist and xenophobic motivated threat

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:

threatening, through a computer system, with the commission of a serious criminal offence as defined under its domestic law, (i) persons for the reason that they belong to a group, distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors, or (ii) a group of persons which is distinguished by any of these characteristics.

Article 5 – Racist and xenophobic motivated insult

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:

insulting publicly, through a computer system, (i) persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors; or (ii) a group of persons which is distinguished by any of these characteristics.

2 A Party may either:

a require that the offence referred to in paragraph 1 of this article has the effect that the person or group of persons referred to in paragraph 1 is exposed to hatred, contempt or ridicule; or

b reserve the right not to apply, in whole or in part, paragraph 1 of this article.

Article 6 – Denial, gross minimisation, approval or justification of genocide or crimes against humanity

1 Each Party shall adopt such legislative measures as may be necessary to establish the following conduct as criminal offences under its domestic law, when committed intentionally and without right:

distributing or otherwise making available, through a computer system to the public, material which denies, grossly minimises, approves or justifies acts constituting genocide or crimes against humanity, as defined by international law and recognised as such by final and binding decisions of the International Military Tribunal, established by the London Agreement of 8 August 1945, or of any other international court established by relevant international instruments and whose jurisdiction is recognised by that Party.

2 A Party may either

a require that the denial or the gross minimisation referred to in paragraph 1 of this article is committed with the intent to incite hatred, discrimination or violence against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors, or otherwise

b reserve the right not to apply, in whole or in part, paragraph 1 of this article.

Article 7 – Aiding and abetting

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, aiding or abetting the commission of any of the offences established in accordance with this Protocol, with intent that such offence be committed.

Chapter III — Relations between the Convention and this Protocol

Article 8 – Relations between the Convention and this Protocol

1 Articles 1, 12, 13, 22, 41, 44, 45 and 46 of the Convention shall apply, *mutatis mutandis*, to this Protocol.

2 The Parties shall extend the scope of application of the measures defined in Articles 14 to 21 and Articles 23 to 35 of the Convention, to Articles 2 to 7 of this Protocol.

Chapter IV – Final provisions

Article 9 – Expression of consent to be bound

1 This Protocol shall be open for signature by the States which have signed the Convention, which may express their consent to be bound by either:

a signature without reservation as to ratification, acceptance or approval; or

b signature subject to ratification, acceptance or approval, followed by ratification, acceptance or approval.

2 A State may not sign this Protocol without reservation as to ratification, acceptance or approval, or deposit an instrument of ratification, acceptance or approval, unless it has already deposited or simultaneously deposits an instrument of ratification, acceptance or approval of the Convention.

3 The instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

Article 10 – Entry into force

1 This Protocol 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 have expressed their consent to be bound by the Protocol, in accordance with the provisions of Article 9.

2 In respect of any State which subsequently expresses its consent to be bound by it, the Protocol shall enter into force on the first day of the month following the expiration of a period of three months after the date of its signature without reservation as to ratification, acceptance or approval or deposit of its instrument of ratification, acceptance or approval.

Article 11 – Accession

1 After the entry into force of this Protocol, any State which has acceded to the Convention may also accede to the Protocol.

2 Accession shall be effected by the deposit with the Secretary General of the Council of Europe of an instrument of accession which shall take effect on the first day of the month following the expiration of a period of three months after the date of its deposit.

Article 12 – Reservations and declarations

1 Reservations and declarations made by a Party to a provision of the Convention shall be applicable also to this Protocol, unless that Party declares otherwise at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession.

2 By a written notification addressed to the Secretary General of the Council of Europe, any Party 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 Articles 3, 5 and 6 of this Protocol. At the same time, a Party may avail itself, with respect to the provisions of this Protocol, of the reservation(s) provided for in Article 22, paragraph 2, and Article 41, paragraph 1, of the Convention, irrespective of the implementation made by that Party under the Convention. No other reservations may be made.

3 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 in Article 5, paragraph 2.a, and Article 6, paragraph 2.a, of this Protocol.

Article 13 – Status and withdrawal of reservations

1 A Party that has made a reservation in accordance with Article 12 above shall withdraw such reservation, in whole or in part, as soon as circumstances so permit. Such withdrawal shall take effect on the date of receipt of a notification addressed to the Secretary General of the Council of Europe. 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 The Secretary General of the Council of Europe may periodically enquire with Parties that have made one or more reservations in accordance with Article 12 as to the prospects for withdrawing such reservation(s).

Article 14 – Territorial application

1 Any Party 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 Protocol shall apply.

2 Any Party may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Protocol to any other territory specified in the declaration. In respect of such territory, the Protocol 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 15 – Denunciation

1 Any Party may, at any time, denounce this Protocol 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 16 – 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 Protocol as well as any State which has acceded to, or has been invited to accede to, this Protocol 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 Protocol in accordance with its Articles 9, 10 and 11;

d any other act, notification or communication relating to this Protocol.

In witness whereof the undersigned, being duly authorised thereto, have signed this Protocol.

Done at Strasbourg, this 28 January 2003, 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 Protocol, and to any State invited to accede to it.

ANEXO I - AGENDA DE TÚNIS PARA A SOCIEDADE DA INFORMAÇÃO

TUNIS AGENDA FOR THE INFORMATION SOCIETY

INTRODUCTION

1. We recognize that it is now time to move from principles to action, considering the work already being done in implementing the Geneva Plan of Action and identifying those areas where progress has been made, is being made, or has not taken place.

2. We reaffirm the commitments made in Geneva and build on them in Tunis by focusing on financial mechanisms for bridging the digital divide, on Internet governance and related issues, as well as on implementation and follow-up of the Geneva and Tunis decisions.

FINANCIAL MECHANISMS FOR MEETING THE CHALLENGES OF ICT FOR DEVELOPMENT

3. We thank the UN Secretary-General for his efforts in creating the Task Force on Financial Mechanisms (TFFM) and we commend the members on their report.

4. We recall that the mandate of the TFFM was to undertake a thorough review of the adequacy of existing financial mechanisms in meeting the challenges of ICT for development.

5. The TFFM report sets out the complexity of existing mechanisms, both private and public, which provide financing for ICTs in developing countries. It identifies areas where these could be improved and where ICTs could be given higher priority by developing countries and their development partners.

6. Based on the conclusion of the review of the report, we have considered the improvements and innovations of financial mechanisms, including the creation of a voluntary Digital Solidarity Fund, as mentioned in the Geneva Declaration of Principles.

7. We recognize the existence of the digital divide and the challenges that this poses for many countries, which are forced to choose between many competing objectives in their development planning and in demands for development funds whilst having limited resources.

8. We recognize the scale of the problem in bridging the digital divide, which will require adequate and sustainable investments in ICT infrastructure and services, and capacity building, and transfer of technology over many years to come.

9. We call upon the international community to promote the transfer of technology on mutually agreed terms, including ICTs, to adopt policies and programmes with a view to assisting developing countries to take advantage of technology in their pursuit of development through, *inter alia*, technical cooperation and the building of scientific and technological capacity in our efforts to bridge the digital and development divides.

10. We recognize that the internationally agreed development goals and objectives, including the Millennium Development Goals, are fundamental. The Monterrey Consensus on Financing for Development is the basis for the pursuit of adequate and appropriate financial mechanisms to promote ICT for development, in accordance with the Digital Solidarity Agenda of the Geneva Plan of Action.

11. We recognize and acknowledge the special and specific funding needs of the developing world, as referred to in paragraph 16 of the Geneva Declaration of Principles, which faces numerous challenges in the ICT sector, and that there is strong need to focus on their special financing needs to achieve the internationally agreed development goals and objectives, including the Millennium Development Goals.

12. We agree that the financing of ICT for development needs to be placed in the context of the growing importance of the role of ICTs, not only as a medium of communication, but also as a development enabler, and as a tool for the achievement of the internationally agreed development goals and objectives, including the Millennium Development Goals.

13. In the past, financing of ICT infrastructure in most developing countries has been based on public investment. Lately, a significant influx of investment has taken place where private-sector participation has been encouraged, based on a sound regulatory framework, and where public policies aimed at bridging the digital divide have been implemented.

14. We are greatly encouraged by the fact that advances in communication technology, and high-speed data networks are continuously increasing the possibilities for developing countries, and countries with economies in transition, to participate in the global market for ICT-enabled services on the basis of their comparative advantage. These emerging opportunities provide a powerful commercial basis for ICT infrastructural investment in these countries. Therefore, governments should take action, in the framework of national development policies, in order to support an enabling and competitive environment for the necessary investment in ICT infrastructure and for the development of new services. At the same time, countries should pursue policies and measures that would not discourage, impede or prevent the continued participation of these countries in the global market for ICT-enabled services.

15. We take note that the challenges for expanding the scope of useful accessible information content in the developing world are numerous; in particular, the issue of financing for various forms of content and applications requires new attention, as this area has often been overlooked by the focus on ICT infrastructure.

16. We recognize that attracting investment in ICTs has depended crucially upon an enabling environment, including good governance at all levels, and a supportive, transparent and pro-competitive policy and regulatory framework, reflecting national realities.

17. We endeavour to engage in a proactive dialogue on matters related to corporate social responsibility and good corporate governance of transnational corporations and their contribution to the economic and social development of developing countries in our efforts to bridge the digital divide.

18. We underline that market forces alone cannot guarantee the full participation of developing countries in the global market for ICT-enabled services. Therefore, we encourage the strengthening of international cooperation and solidarity aimed at enabling all countries, especially those referred to in paragraph 16 of the Geneva Declaration of Principles, to develop ICT infrastructure and ICT-enabled services that are viable and competitive at national and international levels.

19. We recognize that, in addition to the public sector, financing of ICT infrastructure by the private sector has come to play an important role in many countries and that domestic financing is being augmented by North-South flows and South-South cooperation.

20. We recognize that, as a result of the growing impact of sustainable private-sector investment in infrastructure, multilateral and bilateral public donors are redirecting public resources to other development objectives, including Poverty Reduction Strategy Papers and related programmes, policy reforms and mainstreaming of ICTs and capacity development. We encourage all governments to give appropriate priority to ICTs, including traditional ICTs such as broadcast radio and television, in their national development strategies. We also encourage multilateral institutions as well as bilateral public donors to consider also providing more financial support for regional and large-scale national ICT infrastructure projects and related capacity development. They should consider aligning their aid and partnership strategies with the priorities set by developing countries and countries with economies in transition in their national development strategies including their poverty reduction strategies.

21. We recognize that public finance plays a crucial role in providing ICT access and services to rural areas and disadvantaged populations including those in Small Island Developing States and Landlocked Developing Countries.

22. We note that ICT-related capacity-building needs represent a high priority in all developing countries and the current financing levels have not been adequate to meet the needs, although there are many different funding mechanisms supporting ICTs for development.

23. We recognize that there are a number of areas in need of greater financial resources and where current approaches to ICT for development financing have devoted insufficient attention to date. These include:

a) ICT capacity-building programmes, materials, tools, educational funding and specialized training initiatives, especially for regulators and other public-sector employees and organizations.

b) Communications access and connectivity for ICT services and applications in remote rural areas, Small Island Developing States, Landlocked Developing Countries and other locations presenting unique technological and market challenges.

c) Regional backbone infrastructure, regional networks, Network Access Points and related regional projects, to link networks across borders and in economically disadvantaged regions which may require coordinated policies including legal, regulatory and financial frameworks, and seed financing, and would benefit from sharing experiences and best practices.

d) Broadband capacity to facilitate the delivery of a broader range of services and applications, promote investment and provide Internet access at affordable prices to both existing and new users.

e) Coordinated assistance, as appropriate, for countries referred to in paragraph 16 of the Geneva Declaration of Principles, particularly Least Developed Countries and Small Island Developing States, in order to improve effectiveness and to lower transaction costs associated with the delivery of international donor support.

f) ICT applications and content aimed at the integration of ICTs into the implementation of poverty eradication strategies and in sector programmes, particularly in health, education, agriculture and the environment.

In addition, there is a need to consider the following other issues, which are relevant to ICT for development and which have not received adequate attention:

g) Sustainability of Information Society related projects, for example the maintenance of ICT infrastructure.

h) Special needs of Small, Medium and Micro Enterprises (SMMEs), such as funding requirements.

i) Local development and manufacturing of ICT applications and technologies by developing countries.

j) Activities on ICT-related institutional reform and enhanced capacity on legal and regulatory framework.

k) Improving organizational structures and business-process change aimed at optimizing the impact and effectiveness of ICT projects and other projects with significant ICT components;

l) Local government and initiatives based in local communities that deliver ICT services to communities in areas such as education, health and livelihood support.

24. Recognizing that the central responsibility for coordination of public financing programmes and public ICT development initiatives rests with governments, we recommend that further cross-sectoral and cross-institutional coordination should be undertaken, both on the part of donors and recipients within the national framework.

25. Multilateral development banks and institutions should consider adapting their existing mechanisms, and where appropriate designing new ones, to provide for national and regional demands on ICT development.

26. We acknowledge the following prerequisites for equitable and universal accessibility to, and better utilization of, financial mechanisms:

a) Creating policy and regulatory incentives aimed at universal access and the attraction of private-sector investment.

b) Identification and acknowledgement of the key role of ICTs in national development strategies, and their elaboration, when appropriate, in conjunction with e-strategies.

c) Developing institutional and implementation capacity to support the use of national universal service/access funds, and further study of these mechanisms and those aiming to mobilize domestic resources.

d) Encouraging the development of locally relevant information, applications and services that will benefit developing countries and countries with economies in transition.

e) Supporting the "scaling-up" of successful ICT-based pilot programmes.

f) Supporting the use of ICTs in government as a priority and crucial target area for ICT-based development interventions.

g) Building human resource and institutional capacity (knowledge) at every level for achieving Information Society objectives, especially in the public sector.

h) Encouraging business-sector entities to help jump-start wider demand for ICT services by supporting creative industries, local producers of cultural content and applications as well as small businesses.

i) Strengthening capacities to enhance the potential of securitized funds and utilizing them effectively.

27. We recommend improvements and innovations in existing financing mechanisms, including:

a) Improving financial mechanisms to make financial resources become adequate, more predictable, preferably untied, and sustainable.

b) Enhancing regional cooperation and creating multi-stakeholder partnerships, especially by creating incentives for building regional backbone infrastructure.

c) Providing affordable access to ICTs, by the following measures:

i. reducing international Internet costs charged by backbone providers, supporting, *inter alia*, the creation and development of regional ICT backbones and Internet Exchange Points to reduce interconnection cost and broaden network access;

ii. encouraging ITU to continue the study of the question of International Internet Connectivity (IIC) as an urgent matter to develop appropriate Recommendations.

d) Coordinating programmes among governments and major financial players to mitigate investment risks and transaction costs for operators entering less attractive rural and low-income market segments.

e) Helping to accelerate the development of domestic financial instruments, including by supporting local microfinance instruments, ICT business incubators, public credit instruments, reverse auction mechanisms, networking initiatives based on local communities, digital solidarity and other innovations.

f) Improving the ability to access financing facilities with a view to accelerating the pace of financing of ICT infrastructure and services, including the promotion of North-South flows as well as North-South and South-South cooperation.

g) Multilateral, regional and bilateral development organizations should consider the utility of creating a virtual forum for the sharing of information by all stakeholders on potential projects, on sources of financing and on institutional financial mechanisms.

h) Enabling developing countries to be increasingly able to generate funds for ICTs and to develop financial instruments, including trust funds and seed capital adapted to their economies.

i) Urging all countries to make concrete efforts to fulfil their commitments under the Monterrey Consensus.

j) Multilateral, regional and bilateral development organizations should consider cooperating to enhance their capacity to provide rapid response with a view to supporting developing countries that request assistance with respect to ICT policies;

k) Encouraging increased voluntary contributions.

l) Making, as appropriate, effective use of debt relief mechanisms as outlined in the Geneva Plan of Action, including *inter alia* debt cancellation and debt swapping, that may be used for financing ICT for development projects, including those within the framework of Poverty Reduction Strategies.

28. We welcome the Digital Solidarity Fund (DSF) established in Geneva as an innovativefinancial mechanism of a voluntary nature open to interested stakeholders with the objective of transforming the digital divide into digital opportunities for the developing world by focusing mainly on specific and urgent needs at the local level and seeking new voluntary sources of "solidarity" finance. The DSF will complement existing mechanisms for funding the Information Society, which should continue to be fully utilized to fund the growth of new ICT infrastructure and services.

INTERNET GOVERNANCE

29. We reaffirm the principles enunciated in the Geneva phase of the WSIS, in December 2003, that the Internet has evolved into a global facility available to the public and its governance should constitute a core issue of the Information Society agenda. The international management of the Internet should be multilateral, transparent and democratic, with the full involvement of governments, the private sector, civil society and international organizations. It should ensure an equitable distribution of resources, facilitate access for all and ensure a stable and secure functioning of the Internet, taking into account multilingualism.

30. We acknowledge that the Internet, a central element of the infrastructure of the Information Society, has evolved from a research and academic facility into a global facility available to the public.

31. We recognize that Internet governance, carried out according to the Geneva principles, is an essential element for a people-centred, inclusive, development-oriented and non-discriminatory Information Society. Furthermore, we commit ourselves to the stability and security of the Internet as a global facility and to ensuring the requisite legitimacy of its governance, based on the full participation of all stakeholders, from both developed and developing countries, within their respective roles and responsibilities.

32. We thank the UN Secretary-General for establishing the Working Group on Internet Governance (WGIG). We commend the chairman, members and secretariat for their work and for their report.

33. We take note of the WGIG's report that has endeavoured to develop a working definition of Internet governance. It has helped identify a number of public policy issues that

are relevant to Internet governance. The report has also enhanced our understanding of the respective roles and responsibilities of governments, intergovernmental and international organizations and other forums as well as the private sector and civil society from both developing and developed countries.

34. A working definition of Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.

35. We reaffirm that the management of the Internet encompasses both technical and public policy issues and should involve all stakeholders and relevant intergovernmental and international organizations. In this respect it is recognized that:

a) Policy authority for Internet-related public policy issues is the sovereign right of States. They have rights and responsibilities for international Internet-related public policy issues.

b) The private sector has had, and should continue to have, an important role in the development of the Internet, both in the technical and economic fields.

c) Civil society has also played an important role on Internet matters, especially at community level, and should continue to play such a role.

d) Intergovernmental organizations have had, and should continue to have, a facilitating role in the coordination of Internet-related public policy issues.

e) International organizations have also had and should continue to have an important role in the development of Internet-related technical standards and relevant policies.

36. We recognize the valuable contribution by the academic and technical communities within those stakeholder groups mentioned in paragraph 35 to the evolution, functioning and development of the Internet.

37. We seek to improve the coordination of the activities of international and intergovernmental organizations and other institutions concerned with Internet governance and the exchange of information among themselves. A multi-stakeholder approach should be adopted, as far as possible, at all levels.

38. We call for the reinforcement of specialized regional Internet resource management institutions to guarantee the national interest and rights of countries in that particular region to manage their own Internet resources, while maintaining global coordination in this area.

39. We seek to build confidence and security in the use of ICTs by strengthening the trust framework. We reaffirm the necessity to further promote, develop and implement in

cooperation with all stakeholders a global culture of cybersecurity, as outlined in UNGA Resolution 57/239 and other relevant regional frameworks. This culture requires national action and increased international cooperation to strengthen security while enhancing the protection of personal information, privacy and data. Continued development of the culture of cybersecurity should enhance access and trade and must take into account the level of social and economic development of each country and respect the development-oriented aspects of the Information Society.

40. We underline the importance of the prosecution of cybercrime, including cybercrime committed in one jurisdiction, but having effects in another. We further underline the necessity of effective and efficient tools and actions, at national and international levels, to promote international cooperation among, *inter alia*, law-enforcement agencies on cybercrime. We call upon governments in cooperation with other stakeholders to develop necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks, for example, UNGA Resolutions 55/63 and 56/121 on "*Combating the criminal misuse of information technologies*" and regional initiatives including, but not limited to, the Council of Europe's *Convention on Cybercrime*.

41. We resolve to deal effectively with the significant and growing problem posed by spam. We take note of current multilateral, multi-stakeholder frameworks for regional and international cooperation on spam, for example, the APEC Anti-Spam Strategy, the London Action Plan, the Seoul-Melbourne Anti–Spam Memorandum of Understanding and the relevant activities of OECD and ITU. We call upon all stakeholders to adopt a multi-pronged approach to counter spam that includes, *inter alia*, consumer and business education; appropriate legislation, law-enforcement authorities and tools; the continued development of technical and self-regulatory measures; best practices; and international cooperation.

42. We reaffirm our commitment to the freedom to seek, receive, impart and use information, in particular, for the creation, accumulation and dissemination of knowledge. We affirm that measures undertaken to ensure Internet stability and security, to fight cybercrime and to counter spam, must protect and respect the provisions for privacy and freedom of expression as contained in the relevant parts of the Universal Declaration of Human Rights and the Geneva Declaration of Principles.

43. We reiterate our commitments to the positive uses of the Internet and other ICTs and to take appropriate actions and preventive measures, as determined by law, against abusive uses of ICTs as mentioned under the *Ethical Dimensions of the Information Society* of the Geneva Declaration of Principles and Plan of Action.

44. We also underline the importance of countering terrorism in all its forms and manifestations on the Internet, while respecting human rights and in compliance with other obligations under international law, as outlined in UNGA A/60/L.1 with reference to Article 85 of the *2005 World Summit Outcome*.

45. We underline the importance of the security, continuity and stability of the Internet, and the need to protect the Internet and other ICT networks from threats and vulnerabilities. We affirm the need for a common understanding of the issues of Internet security, and for further cooperation to facilitate outreach, the collection and dissemination of security-related information and exchange of good practice among all stakeholders on measures to combat security threats, at national and international levels.

46. We call upon all stakeholders to ensure respect for privacy and the protection of personal information and data, whether via adoption of legislation, the implementation of collaborative frameworks, best practices and self-regulatory and technological measures by business and users. We encourage all stakeholders, in particular governments, to reaffirm the right of individuals to access information according to the Geneva Declaration of Principles and other mutually agreed relevant international instruments, and to coordinate internationally as appropriate.

47. We recognize the increasing volume and value of all e-business, both within and across national boundaries. We call for the development of national consumer-protection laws and practices, and enforcement mechanisms where necessary, to protect the right of consumers who purchase goods and services online, and for enhanced international cooperation to facilitate a further expansion, in a non-discriminatory way, under applicable national laws, of e-business as well as consumer confidence in it.

48. We note with satisfaction the increasing use of ICT by governments to serve citizens and encourage countries that have not yet done so to develop national programmes and strategies for e-government.

49. We reaffirm our commitment to turning the digital divide into digital opportunity, and we commit to ensuring harmonious and equitable development for all. We commit to foster and provide guidance on development areas in the broader Internet governance arrangements, and to include, amongst other issues, international interconnection costs, capacity building and technology/know-how transfer. We encourage the realization of multilingualism in the Internet development environment, and we support the development of software that renders itself easily to localization, and enables users to choose appropriate solutions from different software models including open-source, free and proprietary software.

50. We acknowledge that there are concerns, particularly amongst developing countries, that the charges for international Internet connectivity should be better balanced to enhance access. We therefore call for the development of strategies for increasing affordable global connectivity, thereby facilitating improved and equitable access for all, by:

a) Promoting Internet transit and interconnection costs that are commercially negotiated in a competitive environment and that should be oriented towards objective, transparent and non-discriminatory parameters, taking into account ongoing work on this subject.

b) Setting up regional high-speed Internet backbone networks and the creation of national, sub-regional and regional Internet Exchange Points (IXPs).

c) Recommending donor programmes and developmental financing mechanisms to consider the need to provide funding for initiatives that advance connectivity, IXPs and local content for developing countries.

d) Encouraging ITU to continue the study of the question of International Internet Connectivity (IIC) as a matter of urgency, and to periodically provide output for consideration and possible implementation. We also encourage other relevant institutions to address this issue.

e) Promoting the development and growth of low-cost terminal equipment, such as individual and collective user devices, especially for use in developing countries.

f) Encouraging Internet Service Providers (ISPs) and other parties in the commercial negotiations to adopt practices towards attainment of fair and balanced interconnectivity costs.

g) Encouraging relevant parties to commercially negotiate reduced interconnection costs for Least Developed Countries (LDCs), taking into account the special constraints of LDCs.

51. We encourage governments and other stakeholders, through partnerships where appropriate, to promote ICT education and training in developing countries, by establishing national strategies for ICT integration in education and workforce development and dedicating appropriate resources. Furthermore, international cooperation would be extended, on a voluntary basis, for capacity building in areas relevant to Internet governance. This may include, in particular, building centres of expertise and other institutions to facilitate know-how transfer and exchange of best practices, in order to enhance the participation of developing countries and all stakeholders in Internet governance mechanisms.

52. In order to ensure effective participation in global Internet governance, we urge international organizations, including intergovernmental organizations, where relevant, to ensure that all stakeholders, particularly from developing countries, have the opportunity to

participate in policy decision-making relating to Internet governance, and to promote and facilitate such participation.

53. We commit to working earnestly towards multilingualization of the Internet, as part of a multilateral, transparent and democratic process, involving governments and all stakeholders, in their respective roles. In this context, we also support local content development, translation and adaptation, digital archives, and diverse forms of digital and traditional media, and recognize that these activities can also strengthen local and indigenous communities. We would therefore underline the need to:

a) Advance the process for the introduction of multilingualism in a number of areas including domain names, e-mail addresses and keyword look-up.

b) Implement programmes that allow for the presence of multilingual domain names and content on the Internet and the use of various software models in order to fight against the linguistic digital divide and to ensure the participation of all in the emerging new society.

c) Strengthen cooperation between relevant bodies for the further development of technical standards and to foster their global deployment.

54. We recognize that an enabling environment, at national and international levels, supportive of foreign direct investment, transfer of technology, and international cooperation, particularly in the areas of finance, debt and trade, is essential for the development of the Information Society, including for the development and diffusion of the Internet and its optimal use. In particular, the roles of the private sector and civil society as the drivers of innovation and private investment in the development of the Internet are critical. Value is added at the edges of the network in both developed and developing countries when the international and domestic policy environment encourages investment and innovation.

55. We recognize that the existing arrangements for Internet governance have worked effectively to make the Internet the highly robust, dynamic and geographically diverse medium that it is today, with the private sector taking the lead in day-to-day operations, and with innovation and value creation at the edges.

56. The Internet remains a highly dynamic medium and therefore any framework and mechanisms designed to deal with Internet governance should be inclusive and responsive to the exponential growth and fast evolution of the Internet as a common platform for the development of multiple applications.

57. The security and stability of the Internet must be maintained.

58. We recognize that Internet governance includes more than Internet naming and addressing. It also includes other significant public policy issues such as, *inter alia*, critical

Internet resources, the security and safety of the Internet, and developmental aspects and issues pertaining to the use of the Internet.

59. We recognize that Internet governance includes social, economic and technical issues including affordability, reliability and quality of service.

60. We further recognize that there are many cross-cutting international public policy issues that require attention and are not adequately addressed by the current mechanisms.

61. We are convinced that there is a need to initiate, and reinforce, as appropriate, a transparent, democratic, and multilateral process, with the participation of governments, private sector, civil society and international organizations, in their respective roles. This process could envisage creation of a suitable framework or mechanisms, where justified, thus spurring the ongoing and active evolution of the current arrangements in order to synergize the efforts in this regard.

62. We emphasize that any Internet governance approach should be inclusive and responsive and should continue to promote an enabling environment for innovation, competition and investment.

63. Countries should not be involved in decisions regarding another country's country-code Top-Level Domain (ccTLD). Their legitimate interests, as expressed and defined by each country, in diverse ways, regarding decisions affecting their ccTLDs, need to be respected, upheld and addressed via a flexible and improved framework and mechanisms.

64. We recognize the need for further development of, and strengthened cooperation among, stakeholders for public policies for generic Top-Level Domain names (gTLDs).

65. We underline the need to maximize the participation of developing countries in decisions regarding Internet governance, which should reflect their interests, as well as in development and capacity building.

66. In view of the continuing internationalization of the Internet and the principle of universality, we agree to implement the Geneva Principles regarding Internet governance.

67. We agree, *inter alia*, to invite the UN Secretary-General to convene a new forum for multi-stakeholder policy dialogue.

68. We recognize that all governments should have an equal role and responsibility for international Internet governance and for ensuring the stability, security and continuity of the Internet. We also recognize the need for development of public policy by governments in consultation with all stakeholders.

69. We further recognize the need for enhanced cooperation in the future, to enable governments, on an equal footing, to carry out their roles and responsibilities, in international

public policy issues pertaining to the Internet, but not in the day-to-day technical and operational matters, that do not impact on international public policy issues.

70. Using relevant international organizations, such cooperation should include the development of globally-applicable principles on public policy issues associated with the coordination and management of critical Internet resources. In this regard, we call upon the organizations responsible for essential tasks associated with the Internet to contribute to creating an environment that facilitates this development of public policy principles.

71. The process towards enhanced cooperation, to be started by the UN Secretary-General, involving all relevant organizations by the end of the first quarter of 2006, will involve all stakeholders in their respective roles, will proceed as quickly as possible consistent with legal process, and will be responsive to innovation. Relevant organizations should commence a process towards enhanced cooperation involving all stakeholders, proceeding as quickly as possible and responsive to innovation. The same relevant organizations shall be requested to provide annual performance reports.

72. We ask the UN Secretary-General, in an open and inclusive process,to convene, by the second quarter of 2006, a meeting of the new forum for multi-stakeholder policy dialogue—called the *Internet Governance Forum* (IGF). The mandate of the Forum is to:

a) Discuss public policy issues related to key elements of Internet governance in order to foster the sustainability, robustness, security, stability and development of the Internet.

b) Facilitate discourse between bodies dealing with different cross-cutting international public policies regarding the Internet and discuss issues that do not fall within the scope of any existing body.

c) Interface with appropriate intergovernmental organizations and other institutions on matters under their purview.

d) Facilitate the exchange of information and best practices, and in this regard make full use of the expertise of the academic, scientific and technical communities.

e) Advise all stakeholders in proposing ways and means to accelerate the availability and affordability of the Internet in the developing world.

f) Strengthen and enhance the engagement of stakeholders in existing and/or future Internet governance mechanisms, particularly those from developing countries.

g) Identify emerging issues, bring them to the attention of the relevant bodies and the general public, and, where appropriate, make recommendations.

h) Contribute to capacity building for Internet governance in developing countries, drawing fully on local sources of knowledge and expertise.

i) Promote and assess, on an ongoing basis, the embodiment of WSIS principles in Internet governance processes.

j) Discuss, *inter alia*, issues relating to critical Internet resources.

k) Help to find solutions to the issues arising from the use and misuse of the Internet, of particular concern to everyday users.

l) Publish its proceedings.

73. The Internet Governance Forum, in its working and function, will be multilateral, multi-stakeholder, democratic and transparent. To that end, the proposed IGF could:

a) Build on the existing structures of Internet governance, with special emphasis on the complementarity between all stakeholders involved in this process – governments, business entities, civil society and intergovernmental organizations.

b) Have a lightweight and decentralized structure that would be subject to periodic review.

c) Meet periodically, as required. IGF meetings, in principle, may be held in parallel with major relevant UN conferences, *inter alia*, to use logistical support.

74. We encourage the UN Secretary-General to examine a range of options for the convening of the Forum, taking into consideration the proven competencies of all stakeholders in Internet governance and the need to ensure their full involvement.

75. The UN Secretary-General would report to UN Member States periodically on the operation of the Forum.

76. We ask the UN Secretary-General to examine the desirability of the continuation of the Forum, in formal consultation with Forum participants, within five years of its creation, and to make recommendations to the UN Membership in this regard.

77. The IGF would have no oversight function and would not replace existing arrangements, mechanisms, institutions or organizations, but would involve them and take advantage of their expertise. It would be constituted as a neutral, non-duplicative and non-binding process. It would have no involvement in day-to-day or technical operations of the Internet.

78. The UN Secretary-General should extend invitations to all stakeholders and relevant parties to participate at the inaugural meeting of the IGF, taking into consideration balanced geographical representation. The UN Secretary-General should also:

a) draw upon any appropriate resources from all interested stakeholders, including the proven expertise of ITU, as demonstrated during the WSIS process; and

b) establish an effective and cost-efficient bureau to support the IGF, ensuring multi-stakeholder participation.

79. Diverse matters relating to Internet governance would continue to be addressed in other relevant fora.

80. We encourage the development of multi-stakeholder processes at the national, regional and international levels to discuss and collaborate on the expansion and diffusion of the Internet as a means to support development efforts to achieve internationally agreed development goals and objectives, including the Millennium Development Goals.

81. We reaffirm our commitment to the full implementation of the Geneva Principles.

82. We welcome the generous offer of the Government of Greece to host the first meeting of the IGF in Athens no later than 2006 and we call upon the UN Secretary-General to extend invitations to all stakeholders and relevant parties to participate at the inaugural meeting of the IGF.

IMPLEMENTATION AND FOLLOW-UP

83. Building an inclusive development-oriented Information Society will require unremitting multi-stakeholder effort. We thus commit ourselves to remain fully engaged—nationally, regionally and internationally—to ensure sustainable implementation and follow-up of the outcomes and commitments reached during the WSIS process and its Geneva and Tunis phases of the Summit. Taking into account the multifaceted nature of building the Information Society, effective cooperation among governments, private sector, civil society and the United Nations and other international organizations, according to their different roles and responsibilities and leveraging on their expertise, is essential.

84. Governments and other stakeholders should identify those areas where further effort and resources are required, and jointly identify, and where appropriate develop, implementation strategies, mechanisms and processes for WSIS outcomes at international, regional, national and local levels, paying particular attention to people and groups that are still marginalized in their access to, and utilization of, ICTs.

85. Taking into consideration the leading role of governments in partnership with other stakeholders in implementing the WSIS outcomes, including the Geneva Plan of Action, at the national level, we encourage those governments that have not yet done so to elaborate, as appropriate, comprehensive, forward-looking and sustainable national e-strategies, including ICT strategies and sectoral e-strategies as appropriate, as an integral part of national development plans and poverty reduction strategies, as soon as possible and before 2010.

86. We support regional and international integration efforts aimed at building a people-centred, inclusive and development-oriented Information Society, and we reiterate that strong cooperation within and among regions is indispensable to support knowledge-sharing. Regional cooperation should contribute to national capacity building and to the development of regional implementation strategies.

87. We affirm that the exchange of views and sharing of effective practices and resources is essential to implementing the outcomes of WSIS at the regional and international levels. To this end, efforts should be made to provide and share, among all stakeholders, knowledge and know-how, related to the design, implementation, monitoring and evaluation of e-strategies and policies, as appropriate. We recognize as fundamental elements to bridge the digital divide in developing countries, in a sustainable way, poverty reduction, enhanced national capacity building and the promotion of national technological development.

88. We reaffirm that through the international cooperation of governments and the partnership of all stakeholders, it will be possible to succeed in our challenge of harnessing the potential of ICTs as a tool, at the service of development, to promote the use of information and knowledge to achieve the internationally agreed development goals and objectives, including the Millennium Development Goals, as well as to address the national and local development priorities, thereby further improving the socio- economic development of all human beings.

89. We are determined to improve international, regional and national connectivity and affordable access to ICTs and information through an enhanced international cooperation of all stakeholders that promotes technology exchange and technology transfer, human resource development and training, thus increasing the capacity of developing countries to innovate and to participate fully in, and contribute to, the Information Society.

90. We reaffirm our commitment to providing equitable access to information and knowledge for all, recognizing the role of ICTs for economic growth and development. We are committed to working towards achieving the indicative targets, set out in the Geneva Plan of Action, that serve as global references for improving connectivity and universal, ubiquitous, equitable, non-discriminatory and affordable access to, and use of, ICTs, considering different national circumstances, to be achieved by 2015, and to using ICTs, as a tool to achieve the internationally agreed development goals and objectives, including the Millennium Development Goals, by:

a) *mainstreaming and aligning national e-strategies*, across local, national, and regional action plans, as appropriate and in accordance with local and national development priorities, with in-built time-bound measures.

b) *developing and implementing enabling policies* that reflect national realities and that promote a supportive international environment, foreign direct investment as well as the mobilization of domestic resources, in order to promote and foster entrepreneurship, particularly Small, Medium and Micro Enterprises (SMMEs), taking into account the relevant market and cultural contexts. These policies should be reflected in a transparent, equitable regulatory framework to create a competitive environment to support these goals and strengthen economic growth.

c) *building ICT capacity* for all and confidence in the use of ICTs by all - including youth, older persons, women, indigenous peoples, people with disabilities, and remote and rural communities - through the improvement and delivery of relevant education and training programmes and systems including lifelong and distance learning.

d) *implementing effective training and education,* particularly in ICT science and technology, that motivates and promotes participation and active involvement of girls and women in the decision-making process of building the Information Society.

e) *paying special attention to the formulation of universal design conceptsand the use of assistive technologies* that promote access for all persons, including those with disabilities.

f) *promoting public policies aimed at providing affordable access* at all levels, including community-level,to hardware as well as software and connectivity through an increasingly converging technological environment, capacity building and local content.

g) *improving access to the world's health knowledgeand telemedicine services*, in particular in areas such as global cooperation in emergency response, access to and networking among health professionals to help improve quality of life and environmental conditions.

h) *building ICT capacities* to improve access and use of postal networks and services.

i) *using ICTs to improve access to agricultural knowledge*, combat poverty, and support production of and access to locally relevant agriculture-related content.

j) *developing and implementing e-government applications* based on open standards in order to enhance the growth and interoperability of e-government systems, at all levels, thereby furthering access to government information and services, and contributing to building ICT networks and developing services that are available anywhere and anytime, to anyone and on any device.

k) *supporting educational, scientific, and cultural institutions*, including libraries, archives and museums, in their role of developing, providing equitable, open and affordable access to, and preserving diverse and varied content, including in digital form, to support informal and formal education, research and innovation; and in particular supporting libraries in their public-service role of providing free and equitable access to information and of improving ICT literacy and community connectivity, particularly in underserved communities.

l) *enhancing the capacity of communities* in all regions to develop content in local and/or indigenous languages.

m) *strengthening the creation of quality e-content*, on national, regional and international levels.

n) *promoting the use of traditional and new media* in order to foster universal access to information, culture and knowledge for all people, especially vulnerable populations and populations in developing countries and using, *inter alia*, radio and television as educational and learning tools.

o) *reaffirming the independence, pluralism and diversity of media, and freedom of information* including through, as appropriate, the development of domestic legislation, we reiterate our call for the responsible use and treatment of information by the media in accordance with the highest ethical and professional standards. We reaffirm the necessity of reducing international imbalances affecting the media, particularly as regards infrastructure, technical resources and the development of human skills. These reaffirmations are made with reference to Geneva Declaration of Principles paragraphs 55 to 59.

p) *strongly encouraging ICT enterprises and entrepreneurs to develop and use environment-friendly production processes* in order to minimize the negative impacts of the use and manufacture of ICTs and disposal of ICT waste on people and the environment. In this context, it is important to give particular attention to the specific needs of the developing countries.

q) *incorporating regulatory, self-regulatory, and other effective policies and frameworks to protect children and young people* from abuse and exploitation through ICTs into national plans of action and e-strategies.

r) *promoting the development of advanced research networks,* at national, regional and international levels, in order to improve collaboration in science, technology and higher education.

s) *promoting voluntary service,* at the community level, to help maximize the developmental impact of ICTs.

t) *promoting the use of ICTs to enhance flexible ways of working*, including teleworking, leading to greater productivity and job creation.

91. We recognize the intrinsic relationship between disaster reduction, sustainable development and the eradication of poverty and that disasters seriously undermine investment in a very short time and remain a major impediment to sustainable development and poverty eradication. We are clear as to the important enabling role of ICTs at the national, regional and international levels including:

a) Promoting technical cooperation and enhancing the capacity of countries, particularly developing countries, in utilizing ICT tools for disaster early-warning, management and emergency communications, including dissemination of understandable warnings to those at risk.

b) Promoting regional and international cooperation for easy access to and sharing of information for disaster management, and exploring modalities for the easier participation of developing countries.

c) Working expeditiously towards the establishment of standards-based monitoring and worldwide early-warning systems linked to national and regional networks and facilitating emergency disaster response all over the world, particularly in high-risk regions.

92. We encourage countries, and all other interested parties, to make available child helplines, taking into account the need for mobilization of appropriate resources. For this purpose, easy-to-remember numbers, accessible from all phones and free of charge, should be made available.

93. We seek to digitize our historical data and cultural heritage for the benefit of future generations. We encourage effective information management policies in the public and private sectors, including the use of standards-based digital archiving and innovative solutions to overcome technological obsolescence, as a means to ensure the long-term preservation of, and continued access to, information.

94. We acknowledge that everyone should benefit from the potential that the Information Society offers. Therefore, we invite governments to assist, on a voluntary basis, those countries affected by any unilateral measure not in accordance with international law and the Charter of the United Nations that impedes the full achievement of economic and social development by the population of the affected countries, and that hinders the well-being of their population.

95. We call upon international and intergovernmental organizations to develop, within approved resources, their policy analysis and capacity-building programmes, based on

practical and replicable experiences of ICT matters, policies and actions that have led to economic growth and poverty alleviation, including through the improved competitiveness of enterprises.

96. We recall the importance of creating a trustworthy, transparent and non-discriminatory legal, regulatory and policy environment. To that end, we reiterate that ITU and other regional organizations should take steps to ensure rational, efficient and economic use of, and equitable access to, the radio-frequency spectrum by all countries, based on relevant international agreements.

97. We acknowledge that multi-stakeholder participation is essential to the successful building of a people-centred, inclusive and development-oriented Information Society and that governments could play an important role in this process. We underline that the participation of all stakeholders in implementing WSIS outcomes, and following them up on national, regional and international levels with the overarching goal of helping countries to achieve internationally agreed development goals and objectives, including the Millennium Development Goals, is key to that success.

98. We encourage strengthened and continuing cooperation between and among stakeholders to ensure effective implementation of the Geneva and Tunis outcomes, for instance through the promotion of national, regional and international multi-stakeholder partnerships including Public Private Partnerships (PPPs), and the promotion of national and regional multi-stakeholder thematic platforms, in a joint effort and dialogue with developing and less developed countries, development partners and actors in the ICT sector. In that respect, we welcome partnerships such as the ITU-led "Connect the World" initiative.

99. We agree to ensure the sustainability of progress towards the goals of WSIS after the completion of its Tunis phase and we decide, therefore, to establish a mechanism for implementation and follow-up at national, regional and international levels.

100. At the national level, based on the WSIS outcomes, we encourage governments, with the participation of all stakeholders and bearing in mind the importance of an enabling environment, to set up a national *implementation* mechanism, in which:

a) National e-strategies, where appropriate, should be an integral part of national development plans, including Poverty Reduction Strategies, aiming to contribute to the achievement of internationally agreed development goals and objectives, including the Millennium Development Goals.

b) ICTs should be fully mainstreamed into strategies for Official Development Assistance (ODA) through more effective information-sharing and coordination among

development partners, and through analysis and sharing of best practices and lessons learned from experience with ICT for development programmes.

c) Existing bilateral and multilateral technical assistance programmes, including those under the UN Development Assistance Framework, should be used whenever appropriate to assist governments in their implementation efforts at the national level.

d) Common Country Assessment reports should contain a component on ICT for development.

101. At the regional level:

a) Upon request from governments, regional intergovernmental organizations in collaboration with other stakeholders should carry out WSIS implementation activities, exchanging information and best practices at the regional level, as well as facilitating policy debate on the use of ICT for development, with a focus on attaining the internationally agreed development goals and objectives, including the Millennium Development Goals.

b) UN Regional Commissions, based on request of Member States and within approved budgetary resources, may organize regional WSIS follow-up activities in collaboration with regional and sub-regional organizations, with appropriate frequency, as well as assisting Member States with technical and relevant information for the development of regional strategies and the implementation of the outcomes of regional conferences.

c) We consider a multi-stakeholder approach and the participation in regional WSIS implementation activities by the private sector, civil society, and the United Nations and other international organizations to be essential.

102. At the international level, bearing in mind the importance of the enabling environment:

a) *Implementation and follow-up* of the outcomes of the Geneva and Tunis phases of the Summit should take into account the main themes and action lines in the Summit documents.

b) Each UN agency should act according to its mandate and competencies, and pursuant to decisions of their respective governing bodies, and within existing approved resources.

c) Implementation and follow-up should include intergovernmental and multi-stakeholder components.

103. We invite UN agencies and other intergovernmental organizations, in line with UNGA Resolution 57/270B, to facilitate activities among different stakeholders, including civil society and the business sector, to help national governments in their implementation efforts. We request the UN Secretary-General, in consultation with members of the UN system Chief Executives Board for coordination (CEB), to establish, within the CEB, a UN Group on the

Information Society consisting of the relevant UN bodies and organizations, with the mandate to facilitate the implementation of WSIS outcomes, and to suggest to CEB that, in considering lead agency(ies) of this Group, it takes into consideration the experience of, and activities in the WSIS process undertaken by, ITU, UNESCO and UNDP.

104. We further request the UN Secretary-General to report to the UNGA through ECOSOC by June 2006, on the modalities of the inter-agency coordination of the implementation of WSIS outcomes including recommendations on the follow-up process.

105. Werequest that ECOSOC oversees the system-wide follow-up of the Geneva and Tunis outcomes of WSIS. To this end, we request that ECOSOC, at its substantive session of 2006, reviews the mandate, agenda and composition of the Commission on Science and Technology for Development (CSTD), including considering the strengthening of the Commission, taking into account the multi-stakeholder approach.

106. WSIS implementation and follow-up should be an integral part of the UN integrated follow-up to major UN conferences and should contribute to the achievement of internationally agreed development goals and objectives, including the Millennium Development Goals. It should not require the creation of any new operational bodies.

107. International and regional organizations should assess and report regularly on universal accessibility of nations to ICTs, with the aim of creating equitable opportunities for the growth of ICT sectors of developing countries.

108. We attach great importance to multi-stakeholder implementation at the international level, which should be organized taking into account the themes and action lines in the Geneva Plan of Action, and moderated or facilitated by UN agencies when appropriate. An Annex to this document offers an indicative and non-exhaustive list of facilitators/moderators for the action lines of the Geneva Plan of Action.

109. The experience of, and the activities undertaken by, UN agencies in the WSIS process—notably ITU, UNESCO and UNDP—should continue to be used to their fullest extent. These three agencies should play leading facilitating roles in the implementation of the Geneva Plan of Action and organize a meeting of moderators/facilitators of action lines, as mentioned in the Annex.

110. The coordination of multi-stakeholder implementation activities would help to avoid duplication of activities. This should include, *inter alia*, information exchange, creation of knowledge, sharing of best practices, and assistance in developing multi-stakeholder and public-private partnerships.

111. We request the United Nations General Assembly (UNGA) to make an overall review of the implementation of WSIS outcomes in 2015.

112. We call for periodic evaluation, using an agreed methodology, such as described in paragraphs 113-120.

113. Appropriate indicators and benchmarking, including community connectivity indicators, should clarify the magnitude of the digital divide, in both its domestic and international dimensions, and keep it under regular assessment, and track global progress in the use of ICTs to achieve internationally agreed development goals and objectives, including the Millennium Development Goals.

114. The development of ICT indicators is important for measuring the digital divide. We note the launch, in June 2004, of the *Partnership on Measuring ICT for Development*, and its efforts:

a) to develop a common set of core ICT indicators; to increase the availability of internationally comparable ICT statistics as well as to establish a mutually agreed framework for their elaboration, for further consideration and decision by the UN Statistical Commission.

b) to promote capacity building in developing countries for monitoring the Information Society.

c) to assess the current and potential impact of ICTs on development and poverty reduction.

d) to develop specific gender-disaggregated indicators to measure the digital divide in its various dimensions.

115. We also note the launch of the *ICT Opportunity Index* and the *Digital Opportunity Index*, which will build upon the common set of core ICT indicators as they were defined within the *Partnership on Measuring ICT for Development*.

116. We stress that all indices and indicators must take into account different levels of development and national circumstances.

117. The further development of these indicators should be undertaken in a collaborative, cost-effective and non-duplicative fashion.

118. We invite the international community to strengthen the statistical capacity of developing countries by giving appropriate support at national and regional levels.

119. We commit ourselves to review and follow up progress in bridging the digital divide, taking into account the different levels of development among nations, so as to achieve the internationally agreed development goals and objectives, including the Millennium Development Goals, assessing the effectiveness of investment and international cooperation

efforts in building the Information Society, identifying gaps as well as deficits in investment and devising strategies to address them.

120. The sharing of information related to the implementation of WSIS outcomes is an important element of evaluation. We note with appreciation the *Report on the Stocktaking of WSIS-related activities*, which will serve as one of the valuable tools for assisting with the follow-up, beyond the conclusion of the Tunis phase of the Summit, as well as the "*Golden Book*" of initiatives launched during the Tunis phase. We encourage all WSIS stakeholders to continue to contribute information on their activities to the public WSIS stocktaking database maintained by ITU. In this regard, we invite all countries to gather information at the national level with the involvement of all stakeholders, to contribute to the stocktaking.

121. There is a need to build more awareness of the Internet in order to make it a global facility which is truly available to the public. We call upon the UNGA to declare 17 May as World Information Society Day to help to raise awareness, on an annual basis, of the importance of this global facility, on the issues dealt with in the Summit, especially the possibilities that the use of ICT can bring for societies and economies, as well as of ways to bridge the digital divide.

122. We request the Secretary-General of the Summit to report to the General Assembly of the United Nations on its outcome, as requested in UNGA Resolution 59/220.

Annex

Action Line	Possible moderators/facilitators
C1. The role of public governance authorities and all stakeholders in the promotion of ICTs for development	ECOSOC/UN Regional Commissions/ITU
C2. Information and communication infrastructure	ITU
C3. Access to information and knowledge	ITU/UNESCO
C4. Capacity building	UNDP/UNESCO/ITU/ UNCTAD
C5. Building confidence and security in the use of ICTs	ITU
C6. Enabling environment	ITU/UNDP/UN Regional CommissionsS/UNCTAD
C7. ICT Applications	
E-government	UNDP/ITU

E-business	WTO/UNCTAD/ITU/UPU
E-learning	UNESCO/ITU/UNIDO
E-health	WHO/ITU
E-employment	ILO/ITU
E-environment	WHO/WMO/UNEP/UN-Habitat/ITU/ICAO
E-agriculture	FAO/ITU
E-science	UNESCO/ITU/UNCTAD
C8. Cultural diversity and identity, linguistic diversity and local content	UNESCO
C9. Media	UNESCO
C10. Ethical dimensions of the Information Society	UNESCO/ECOSOC
C11. International and regional cooperation	UN Regional Commissions/ UNDP/ITU/UNESCO/ ECOSOC

ANEXO J – DIRETRIZES DA OCDE PARA SEGURANÇA DOS SISTEMAS E REDES DE INFORMAÇÃO: EM DIREÇÃO A UMA CULTURA DE SEGURANÇA

GUIDELINES FOR THE SECURITY OF INFO RMATION SYSTEMS AND NETWORKS
TOWARDS A CULTURE OF SECURITY

PREFACE

The use of information systems and networks and the entire information technology environment have changed dramatically since 1992 when the OECD first put forward the *Guidelines for the Security of Information Systems*. These continuing changes offer significant advantages but also require a much greater emphasis on security by governments, businesses, other organisations and individual users who develop, own, provide, manage service and use information systems and networks ("participants").

Ever more powerful personal computers, converging technologies and the widespread use of the Internet have replaced what were modest, stand-alone systems in predominantly closed networks. Today, participants are increasingly interconnected and the connections cross national borders. In addition, the Internet supports critical infrastructures such as energy, transportation and finance and plays a major part in how companies do business, how governments provide services to citizens and enterprises and how individual citizens communicate and exchange information. The nature and type of technologies that constitute the communications and information infrastructure also have changed significantly. The number and nature of infrastructure access devices have multiplied to include fixed, wireless and mobile devices and a growing percentage of access is through "always on" connections. Consequently, the nature, volume and sensitivity of information that is exchanged has expanded substantially.

As a result of increasing interconnectivity, information systems and networks are now exposed to a growing number and a wider variety of threats and vulnerabilities. This raises new issues for security. For these reasons, these Guidelines apply to all participants in the new information society and suggest the need for a greater awareness and understanding of security issues and the need to develop a "culture of security".

I. TOWARDS A CULTURE OF SECURITY

These Guidelines respond to an ever changing security environment by promoting the development of a culture of security – that is, a focus on security in the development of information systems and networks and the adoption of new ways of thinking and behaving

when using and interacting within information systems and networks. The Guidelines signal a clear break with a time when secure design and use of networks and systems were too often after thoughts. Participants are becoming more dependent on information systems, networks and related services, all of which need to be reliable and secure. Only an approach that takes due account of the interests of all participants, and the nature of the systems, networks and related services, can provide effective security.

Each participant is an important actor for ensuring security. Participants, as appropriate to their roles, should be aware of the relevant security risks and preventive measures, assume responsibility and take steps to enhance the security of information systems and networks.

Promotion of a culture of security will require both leadership and extensive participation and should result in a heightened priority for security planning and management, as well as an understanding of the need for security among all participants. Security issues should be topics of concern and responsibility at all levels of government and business and for all participants.

These Guidelines constitute a foundation for work towards a culture of security throughout society. This will enable participants to factor security into the design and use of all information systems and networks. They propose that all participants adopt and promote a culture of security as a way of thinking about, assessing, and acting on, the operations of information systems and networks.

II. AIMS

These Guidelines aim to:

−Promote a culture of security among all participants as a means of protecting information systems and networks.

−Raise awareness about the risk to information systems and networks; the policies, practices, measures and procedures available to address those risks; and the need for their adoption and implementation.

−Foster greater confidence among all participants in information systems and networks and the way in which they are provided and used.

−Create a general frame of reference that will help participants understand security issues and respect ethical values in the development and implementation of coherent policies, practices, measures and procedures for the security of information systems and networks.

−Promote co-operation and information sharing, as appropriate, among all participants in the development and implementation of security policies, practices, measures and procedures.

−Promote the consideration of security as an important objective among all participants involved in the development or implementation of standards.

III. PRINCIPLES

The following nine principles are complementary and should be read as a whole. They concern participants at all levels, including policy and operational levels. Under these Guidelines, the responsibilities of participants vary according to their roles. All participants will be aided by awareness, education, information sharing and training that can lead to adoption of better security understanding and practices. Efforts to enhance the security of information systems and networks should be consistent with the values of a democratic society, particularly the need for an open and free flow of information and basic concerns for personal privacy.

In addition to these Security Guidelines, the OECD has developed complementary recommendations concerning guidelines on other issues important to the world's information society. They relate to privacy (the 1980 *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*) and cryptography (the 1997 *OECD Guidelines for Cryptography Policy*). These Security Guidelines should be read in conjunction with them.

1) Awareness

Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.

Awareness of the risks and available safeguards is the first line of defence for the security of information systems and networks. Information systems and networks can be affected by both internal and external risks. Participants should understand that security failures may significantly harm systems and networks under their control. They should also be aware of the potential harm to others arising from interconnectivity and interdependency. Participants should be aware of the configuration of, and available updates for, their system, its place within networks, good practices that they can implement to enhance security, and the needs of other participants.

2) Responsibility

All participants are responsible for the security of information systems and networks.

Participants depend upon interconnected local and global information systems and networks and should understand their responsibility for the security of those information systems and networks. They should be accountable in a manner appropriate to their individual roles. Participants should review their own policies, practices, measures, and procedures regularly and assess whether these are appropriate to their environment. Those who develop, design and

supply products and services should address system and network security and distribute appropriate information including updates in a timely manner so that users are better able to understand the security functionality of products and services and their responsibilities related to security.

3) Response

Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents.

Recognising the interconnectivity of information systems and networks and the potential for rapid and widespread damage, participants should act in a timely and co-operative manner to address security incidents. They should share information about threats and vulnerabilities, as appropriate, and implement procedures for rapid and effective co-operation to prevent, detect and respond to security incidents. Where permissible, this may involve cross-border information sharing and co-operation.

4) Ethics

Participants should respect the legitimate interests of others

Given the pervasiveness of information systems and networks in our societies, participants need to recognise that their action or inaction may harm others. Ethical conduct is therefore crucial and participants should strive to develop and adopt best practices and to promote conduct that recognises security needs and respects the legitimate interests of others.

5) Democracy

The security of information systems and networks should be compatible with essential values of a democratic society.

Security should be implemented in a manner consistent with the values recognised by democratic societies including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency.

6) Risk assessment

Participants should conduct risk assessments.

Risk assessment identifies threats and vulnerabilities and should be sufficiently broad-based to encompass key internal and external factors, such as technology, physical and human factors, policies and third-party services with security implications. Risk assessment will allow determination of the acceptable level of risk and assist the selection of appropriate controls to manage the risk of potential harm to information systems and networks in light of

the nature and importance of the information to be protected. Because of the growing interconnectivity of information systems, risk assessment should include consideration of the potential harm that may originate from others or be caused to others.

7) Security design and implementation

Participants should incorporate security as an essential element of information systems and networks.

Systems, networks and policies need to be properly designed, implemented and co-ordinated to optimise security. A major, but not exclusive, focus of this effort is the design and adoption of appropriate safeguards and solutions to avoid or limit potential harm from identified threats and vulnerabilities.

Both technical and non-technical safeguards and solutions are required and should be proportionate to the value of the information on the organisation's systems and networks. Security should be a fundamental element of all products, services, systems and networks, and an integral part of system design and architecture. For end users, security design and implementation consists largely of selecting and configuring products and services for their system.

8) Security management

Participants should adopt a comprehensive approach to security management.

Security management should be based on risk assessment and should be dynamic, encompassing all levels of participants' activities and all aspects of their operations. It should include forward-looking responses to emerging threats and address prevention, detection and response to incidents, systems recovery, ongoing maintenance, review and audit. Information system and network security policies, practices, measures and procedures should be co-ordinated and integrated to create a coherent system of security. The requirements of security management depend upon the level of involvement, the role of the participant, the risk involved and system requirements.

9) Reassessment

Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.

New and changing threats and vulnerabilities are continuously discovered.

Participants should continually review, reassess and modify all aspects of security to deal with these evolving risks.

RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS AND NETWORKS

TOWARDS A CULTURE OF SECURITY

THE COUNCIL,

Having regard to the Convention on the Organisation for Economic Co-operation and Development of 14 December 1960, in particular, Articles 1 b), 1 c), 3 a) and 5 b) thereof;

Having regard to the Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data of 23 September 1980 [C(80)58(Final)];

Having regard to the Declaration on Transborder Data Flows adopted by the Governments of OECD Member countries on 11 April 1985 [Annex to C(85)139];

Having regard to the Recommendation of the Council concerning Guidelines for Cryptography Policy of 27 March 1997 [C(97)62/FINAL];

Having regard to the Ministerial Declaration on the Protection of Privacy on Global Networks of 7-9 December 1998 [Annex to C(98)177/FINAL];

Having regard to the Ministerial Declaration on Authentication for Electronic Commerce of 7-9 December 1998 [Annex to C(98)177/FINAL];

Recognising that information systems and networks are of increasing use and value to governments, businesses, other organisations and individual users;

Recognising that the increasingly significant role of information systems and networks, and the growing dependence on them for stable and efficient national economies and international trade and in social, cultural and political life call for special efforts to protect and foster confidence in them;

Recognising that information systems and networks and their worldwide proliferation have been accompanied by new and increasing risks;

Recognising that data and information stored on and transmitted over information systems and networks are subject to threats from various means of unauthorised access, use, misappropriation, alteration, malicious code transmissions, denial of service or destruction and require appropriate safeguards;

Recognising that there is a need to raise awareness of risks to information systems and networks and of the policies, practices, measures and procedures available to respond to those risks, and to encourage appropriate behaviour as a crucial step towards the development of a culture of security;

Recognising that there is a need to review current policies, practices, measures, and procedures to help assure that they meet the evolving challenges posed by threats to information systems and networks;

Recognising that there is a common interest in promoting the security of information systems and networks by means of a culture of security that fosters international co-ordination and co-operation to meet the challenges posed by the potential harm from security failures to national economies, international trade and participation in social, cultural and political life;

And further recognising that the *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* set out in the Annex to this Recommendation are voluntary and do not affect the sovereign rights of nations;

And recognising that these Guidelines are not meant to suggest that any one solution exists for security or what policies, practices, measures and procedures are appropriate to any particular situation, but rather to provide a framework of principles to promote better understanding of how participants may both benefit from, and contribute to, the development of a culture of security;

COMMENDS these *Guidelines for the Security of the Information Systems and Networks: Towards a Culture of Security* to governments, businesses, other organisations and individual users who develop, own, provide, manage, service, and use information systems and networks;

RECOMMENDS that Member countries:

Establish new, or amend existing, policies, practices, measures and procedures to reflect and take into account the *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* by adopting and promoting a culture of security as set out in the Guidelines;

Consult, co-ordinate and co-operate at national and international levels to implement the Guidelines;

Disseminate the Guidelines throughout the public and private sectors, including to governments, business, other organisations, and individual users to promote a culture of security, and to encourage all concerned parties to be responsible and to take necessary steps to implement the Guidelines in a manner appropriate to their individual roles;

Make the Guidelines available to non-member countries in a timely and appropriate manner;

Review the Guidelines every five years so as to foster international co-operation on issues relating to the security of information systems and networks;

INSTRUCTS the OECD Committee for Information, Computer and Communication Policy to promote the implementation of the Guidelines.

This Recommendation replaces the Recommendation of the Council concerning Guidelines for the Security of Information Systems of 26 November 1992 [C(92)188/FINAL].

PROCEDURAL HISTORY

The Security Guidelines were first completed in 1992 and were reviewed in 1997. The current review was undertaken in 2001 by the Working Party on Information Security and Privacy (WPISP), pursuant to a mandate from the Committee for Information, Computer and Communications Policy (ICCP), and accelerated in the aftermath of the September 11 tragedy.

Drafting was undertaken by an Expert Group of the WPISP which met in Washington, DC, on 10-11 December 2001, Sydney on 12-13 February 2002 and Paris on 4 and 6 March 2002. The WPISP met in Paris on 5-6 March 2002, 22-23 April 2002 and 25-26 June 2002.

The present *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* were adopted as a Recommendation of the OECD Council at its 1037th Session on 25 July 2002.