UNIVERSIDADE FEDERAL DO CEARÁ

FACULDADE DE DIREITO

PROGRAMA DE PÓS-GRADUAÇÃO STRICTO SENSU

CURSO DE MESTRADO

CRIMES ELETRÔNICOS: UMA ANÁLISE ECONÔMICA E CONSTITUCIONAL

RENATO LEITE MONTEIRO

Fortaleza – Ceará
2010

UNIVERSIDADE FEDERAL DO CEARÁ

FACULDADE DE DIREITO

PROGRAMA DE PÓS-GRADUAÇÃO STRICTO SENSU

CURSO DE MESTRADO

CRIMES ELETRÔNICOS: UMA ANÁLISE ECONÔMICA E CONSTITUCIONAL

RENATO LEITE MONTEIRO

Dissertação de Mestrado apresentada ao Curso de Mestrado da Faculdade de Direito da Universidade Federal do Ceará, como parte dos requisitos para obtenção do título de Mestre em Direito.

Orientador: Marcio Augusto de Vasconcelos Diniz

Fortaleza – Ceará
2010

UNIVERSIDADE FEDERAL DO CEARÁ

FACULDADE DE DIREITO

PROGRAMA DE PÓS-GRADUAÇÃO STRICTO SENSU

CURSO DE MESTRADO

CRIMES ELETRÔNICOS: UMA ANÁLISE ECONÔMICA E CONSTITUCIONAL

RENATO LEITE MONTEIRO

Dissertação _____ em: 16/08/2010, às 9h.

COMISSÃO EXAMINADORA:

_____

Prof.ª DR. Marcio Augusto de Vasconcelos Diniz (Orientador)
UFC

_____

Profª. DRA Maria Lírida Calou de Araújo E Mendonça
UFC

_____

Prof. DR Juvêncio Vasconcelos Viana
UFC

Dedico essa dissertação a meus pais, minhas irmãs, minha avó, família e amigos. Sem eles, nada disso seria possível. Sem eles, todos meus sonhos seriam apenas sonhos.

AGRADECIMENTOS

O mestrado abriu as portas do mundo para mim. Uma vez, quando ainda pensava em fazer o processo de seleção, encontrei com um mestrando nos corredores da velha Salamanca, mais velho do que eu, com carreira formada e vida em direção. Perguntei como era o curso, se gostava, e ele disse “mudou minha vida, me proporcionou uma visão de mundo que não pude alcançar em minha profissão”. O mesmo aconteceu comigo. Entrei no curso logo após o término da Faculdade de Direito da Universidade Federal do Ceará e desde então não consigo identificar nenhum passo que tomei sem a influência direta das portas que foram abertas pelas pilastras que sustentam essa casa. Viajei o mundo, conheci pessoas, tive oportunidades únicas. Nada disso teria sido possível caso não tivesse ouvido aquelas palavras nos corredores.

Tive amigos/irmãos que influenciaram diretamente minha decisão em tentar o mestrado. Falo dos mestres Péricles Sousa e Pedro Rafael Deocleciano. Irmãos desde a faculdade, nos tornamos mais do que isso após. Vivemos numa relação simbiótica em que um servia de espelho para os demais. E assim fizemos o mestrado, horas noite a dentro escrevendo artigos, discutindo idéias. Esses momentos foram inestimáveis e me ajudaram a construir quem hoje sou.

Os colegas de mestrado foram outra surpresa enriquecedora. Colegas não, amigos. Amigos que sei irão me acompanhar pelo resto da vida. Amigos que me apoiaram nas minhas empreitadas arriscadas. Que sorriram comigo, discutiram comigo. Uma bagagem de valor inestimável.

Os professores que transmitiram seu conhecimento e enriqueceram meu caminho. Além destes, todo o corpo docente e administrativo da instituição, que contribuíram para o renascimento desta e a sua reposição no cenário acadêmico nacional. A Marilene e ao Franklin, em específico, por tudo que fizeram e fazem por mim e por todos. Vocês são peças essenciais nesse jogo de xadrez.

As instituições de fomento FUNCAP, CAPES e CNPQ, que me financiaram durante esses anos, tornando possível a dedicação aos estudos e as viagens. Que essas iniciativas apenas cresçam e ajudem outras mentes famintas de conhecimento.

Ao meu orientador e amigo, Marcio Diniz. Por tudo. Conhecimento, palavras, e-mails, livros, abraços, críticas, compreensão. Você é um exemplo e essas palavras aqui escritas seriam inexistentes se não fosse por você. Muito obrigado por me apoiar em meus planos e entender a distância física pelo qual passei com freqüência desde o início de nossa colaboração. Obrigado pelas orientações, e principalmente pela amizade que aqui nasceu. Como dito uma vez, por você, tudo.

Aos meus amigos, de infância, de faculdade, da vida. Vocês são a certeza que independente de onde eu estiver, sempre terei um voz de compreensão e companheirismo. Gostaria de nomear todos, mas as mais de 100 páginas desse texto seriam insuficientes. Todavia, vou me permitir citar alguns. Henrique, meu irmão, com quem divido a vida, literalmente. Diego, minha voz da razão e da emoção. Pollyanna, minha irmã, um dos amores da minha vida. Leo, meu pai, que sempre me deu apoio, defesa e experiência.

Gostaria de agradecer a algumas pessoas que recentemente entraram na minha vida e foram essenciais na feitura dessa dissertação. Ao meu amigo Lucas Tasquetto, que toda hora gritava em meu ouvido: “escreve isso”. A minha “mãe adotada” em São Paulo, Cecília Tanaka, que me mostrou o caminha das pedras e sempre esteve ao meu lado quando a megalópole me consumia.

A minha família, pilastra e porto seguro. O fator que me faz ir em frente e não ter medo de desbravar novos mundos. A minha mãe, que sempre fez tudo, e mais alguma coisa, para nos dar estudo e tudo que sempre precisamos na vida. Nunca mediu esforços para tirar dela para nós. Uma vencedora que criou três filhos. Por você, tudo. Ao meu pai, exemplo de bondade, sinceridade e honestidade. Por ser meu amigo, além de tudo. Por você, pai, tudo. Minha avó Ocíla, por manter a família. Por tornar possível todos os meus sonhos e sempre acreditar neles mais do que eu. Por ser um exemplo de mulher e perseverança. Vó, por você, tudo. A minhas irmãs, por existirem e compreenderem minha vida atribulada, corrida e inesperada. A toda minha família. Vocês são a razão da minha existência.

A meus tios Paulo Cavalcanti e Celeste Cavalcanti, meus primos Patrícia e Daniel, por terem me acolhido quando fui para São Paulo. Sem nenhuma obrigação, me receberam como filho e eu os adotei como pais e irmãos. Me proporcionaram teto e calor humano. Nunca terei como agradecer o que fizeram e ainda fazem por mim. Sem vocês, esse texto não seria possível. Por vocês, tudo.

A meu irmão Rodrigo. Por me acompanhar, escutar, apoiar. Você é o irmão que somente fui conviver mais de vinte anos depois de nascido. Esse texto é dedicado, na sua maioria, a você. As discussões, conversas, idéias inovadoras e simples, que sempre me deram uma visão de mundo que ninguém mais podia proporcionar. Nenhuma palavra teria maior significado para demonstrar tudo que você fez por mim: obrigado.

O virtual não substitui o real, ele multiplica as oportunidades para atualizá-lo.

Pierre Levy

RESUMO

A sociedade da informação, fruto da proliferação massiva de tecnologias da informação e de comunicação moldou os atuais sistemas econômicos e também o modo de viver das pessoas. A Internet, como maior rede comunicacional, é fator inerente do cotidiano e trouxe consigo inúmeras benesses. Todavia, mudanças massivas ocorreram no âmbito das relações criminosas. Não existe ainda uma noção fidedigna da repercussão social e econômica dos crimes eletrônicos. O objetivo do presente trabalho é tentar entender quais são os incentivos levados em consideração pelos sujeitos ativos desses delitos, que motivos os levam a cometer tais crimes, e que repercussão esses atos podem ter na sociedade. A hipótese levantada é a de que é necessária uma cooperação entre todos os espectros da sociedade, e entidades públicas e privadas, para que seja possível uma atuação eficaz frente aos crimes eletrônicos. Para tanto, foi realizada uma pesquisa documental indireta e uma análise de documentos relacionados ao tema abordado. Ainda, foi feita pesquisa bibliográfica. No desenvolvimento, tratamos sobre a sociedade da informação e as transformações que esta causa na sociedade como um todo, desde a nova conceituação de Estado, por onde adentramos nos quesitos elementares de sua formação, até mesmo políticas de governo. Continuamos ao tentar conceituar os cibercrimes e exibir suas características e dúvidas teóricas. Com esse fim, tentamos delinear o ecossistema dos crimes eletrônicos e procedemos com uma análise econômica da criminalidade com a delimitação dos incentivos que levam pessoas a cometerem crimes comuns, para então tentar entender quais são os motivos dos ofensores virtuais. Por fim, traçamos o atual cenário nacional e internacional no combate aos crimes eletrônicos. Concluímos sobre a necessidade de cooperação e auxílio mútuo entre todos os âmbitos da sociedade como forma efetiva de combate aos crimes eletrônicos.

Palavras-chave: Crimes eletrônicos; Análise econômica; Repressão; Cooperação.

ABSTRACT

The information society, the result of the massive proliferation of information and communication technology, has shaped the current economic system and also the way people live. The Internet, as the largest communication network, is an inherent factor of daily life and brought within many blessings. However, massive changes have occurred when it comes to criminality. There is still no reliable notion of the social and economic impact of electronic crimes. The goal of this work is try to understand which incentives are taken into account by the perpetrators of such offenses, and which motives lead them to commit such crimes, and which repercussion these acts could have in society. The arisen hypothesis is that cooperation is needed among all spectrums of society, and public and private entities so that effective action can be done to prevent electronic crimes. For this, a documentary search was conducted and also an indirect analysis of documents related to the subject. In development of the work, we discuss the information society and the changes it causes in society as a whole, commencing with the new concept of state, where we analyze the basic elements of its foundations and the movements towards electronic government policies. We continue in order to conceptualize cybercrimes and display their characteristics and theoretical questions. To this end, we try to delineate the ecosystem of electronic crimes and proceed with an economic analysis of crime in general with the delimitation of incentives that lead people to commit ordinary crimes, to then try to understand which are the motives taken in consideration by virtual offenders. Finally, we expose the current national and international scenarium when it comes to prevent cybercrimes. We conclude on the need for cooperation and mutual assistance between all spheres of society as an effective model to combat electronic crimes.

Keywords: Electronic crimes; Economic analysis; Repression; Cooperation.

SUMÁRIO

INTRODUÇÃO

A sociedade da informação é um advento do acelerado processo tecnológico pelo qual a sociedade vem passando nos últimos 50 anos. A proliferação massiva de tecnologias da informação e de comunicação moldou os atuais sistemas econômicos e também o modo de viver das pessoas. A Internet, como maior rede comunicacional, é fator inerente do cotidiano e trouxe consigo inúmeras benesses. A quantidade de informação trocada dobra a cada ano. Um jornal de hoje têm mais informações do que um homem comum costumava adquirir durante toda uma vida. Mudanças massivas também ocorreram no âmbito das relações criminosas. Novas modalidades surgiram que se utilizam da internet como meio ou fim. Todavia, ainda não estamos inteiramente preparados para combatê-las. Não existe ainda uma noção fidedigna da repercussão social e econômica dos crimes eletrônicos. Tal fato ensejou a feitura do presente trabalho, numa análise dos fatores sociais, constitucionais e econômicos dos cibercrimes, com foco neste último tópico.

O objetivo é tentar entender quais são os incentivos levados em consideração pelos sujeitos ativos dos crimes eletrônicos, que motivos os levam a cometer tais crimes, e que repercussão esses atos podem ter na sociedade, em um espectro majoritariamente econômico. Para tanto, uma análise dos cenários onde esses crimes acontecem e que grupos são os responsáveis mais freqüentes por tais atos será feita, descrevendo-os. Essa ótica será importante para expor as frentes de combate necessárias para uma atuação preventiva, preemptiva e repressiva efetiva.

A hipótese levantada é a de que é necessária uma cooperação entre todos os espectros da sociedade, e entidades públicas e privadas, para que seja possível uma atuação eficaz frente aos crimes eletrônicos. Incluído no plano cooperativo está a necessidade de liberação, por partes das entidades, de dados precisos referentes aos incidentes de segurança da informação, pois somente assim será possível mensurar adequadamente os danos e prejuízos causados por eles. É necessária a adoção de padrões internacionais e de leis modelos, pois a harmonização e a simetria nos procedimentos investigatórios é um fator premente para a delimitação da autoria e materialidade nesses casos. Imperativo ter por mente que o cenário dos crimes eletrônicos é uma realidade que clama políticas imediatas e pungentes, em face da velocidade

com o que as tecnologias da informação se transformam e a repercussão econômica desses delitos.

Para tanto, foi realizada uma pesquisa documental indireta, ou seja, uma análise de documentos relacionados ao tema abordado. Ainda, foi feita pesquisa bibliográfica, tomando por fonte as mais diversas publicações como boletins, jornais, revistas, monografias, teses, artigos científicos e, principalmente, mídias digitais. Importante enaltecer que a maioria das fontes se encontra em língua estrangeira, majoritariamente em língua inglesa, devido à escassez de material em português, principalmente quanto a tópicos mais específicos e a abordagem econômica.

O texto possui quatro capítulos principais, tendo sempre por foco maior o aspecto econômico e a necessidade de cooperação, hipóteses levantadas pelo presente trabalho científico. Preferimos não adentrar muito em determinados temas por entendermos que não contribuiriam em maior escala para a resposta aos temas aqui propostos. Outros foram propositalmente excluídos, também por escolha, para que fosse possível focar nos problemas principais.

O primeiro capítulo trata sobre a sociedade da informação e as transformações que esta causa na sociedade como um todo, desde a nova conceituação de Estado, por onde adentramos nos quesitos elementares de sua formação, até mesmo políticas de governo, como a governança eletrônica. Discutimos sobre a idéia de consciente coletivo como mola propulsora das inovações e na capacidade colaborativa das pessoas, reverberando para a possibilidade de uma democracia direta e como podemos interpretar os direitos fundamentais nessa nova realidade.

O segundo capítulo adentra mais específico no temas dos crimes eletrônicos, ao tentar conceituá-lo e exibir suas características e dúvidas teóricas quanto à determinação da competência para a persecução e punição destes. Nessa esteira, tentamos delinear o ecossistema dos cibercrimes, discorrendo sobre as principais práticas do mundo virtual e como estas fazem parte de um todo concatenado que pode levar a atos de terrorismo e de guerra, tendo, ainda, como norte dos argumentos, os aspectos econômicos e cooperativos.

No capítulo três iniciamos uma análise econômica da criminalidade com a delimitação dos incentivos que levam pessoas a cometerem crimes comuns, para então tentar entender quais são os motivos dos ofensores virtuais. Que incentivos eles vislumbram ao cometerem

esses delitos e que cálculo de ganho é feito para se chegar à conclusão que eles são um investimento que supera os riscos inerentes. Nesse espectro, discorremos sobre o papel das esferas pública e privada e como estas devem trabalhar em conjunto para que possam combater a criminalidade eletrônica.

No quarto capítulo traçamos o atual cenário nacional e internacional no combate aos crimes eletrônicos. As iniciativas das organizações internacionais e regionais e que corpos normativos existem que enaltecem a figura da cooperação para uma efetiva repressão desses crimes, além de leis modelos que podem ser utilizadas pelas nações na elaboração de suas normas internas, que devem funcionar de forma harmônica com as do plano internacional. Ainda, exibimos a atual conjuntura nacional e enumeramos os órgãos de repressão no Brasil.

Por fim, é feito um apanhado de todo o exposto, tocando em pontos cruciais necessários para uma correta interpretação do estudo, e relembrando exemplos que elucidam o entendimento do problema como um todo, demonstrando a sua importância e emergência, principalmente no âmbito econômico e estrutural responsável pela própria existência da sociedade da informação, para então traçar respostas para os problemas e hipóteses propostas no início do trabalho científico.

1 SOCIEDADE DA INFORMAÇÃO

A sociedade da informação constrói o nosso atual modelo de sociedade, sendo fruto direto das interações entre as pessoas, as empresas e as nações mediante o uso da Internet, das tecnologias da informação e da comunicação, concebendo o arquétipo mercadológico vigente, que se sustenta através dessas ferramentas, e se constrói por elas. Esse novo formato teve início com o advento e proliferação da Internet.

1.1 Histórico da internet

A Internet teve sua origem em um projeto militar elaborado pelos Estados Unidos nos anos 1960, denominado Arpanet, desenvolvido pela Advanced Research Projects Agency (ARPA)[1], ligada ao Departamento de Defesa daquele país. No auge da Guerra Fria, havia o temor real de um bombardeio nuclear pela União Soviética, o que poderia prejudicar as comunicações, a logística e assim levar a um possível contra-ataque americano. Portanto, como forma de se preparar para o pior, foi idealizado um sistema que interligasse várias máquinas em locais diferentes. Em caso de guerra, caso um desses sistemas se tornasse inoperante, os demais continuariam a se comunicar. A idéia era descentralizar os pontos de comunicação e informação. Embora a 3ª Guerra Mundial não tenha sido deflagrada, esse ideal mostrou-se muito útil e eficiente para outras atribuições.

A Internet, em seus primeiros momentos, interligava algumas Universidades e Instituições americanas dedicadas à pesquisa militar e servia apenas para a distribuição de textos entre funcionários das referidas instituições. A Arpanet passou a se conectar com outras redes, incluindo as de outros países a partir de 1973. No final da década de 1980, a National Science Foundation, dos Estados Unidos, criou uma rede própria, deixando a Arpanet de existir em 1990.

Como mencionado, o funcionamento dessa nova forma de comunicação ocorria de modo que existiam vários caminhos para a informação trafegar, caso uma dessas vias ficasse

[1] Disponível em:<http://www.ime.usp.br/~is/abc/abc/node20.html>. Acesso em 25 jul 2010

obstruída ou inoperante, em caso de guerra ou queda de energia, por exemplo, o sistema procuraria automaticamente outro caminho disponível para se comunicar. Nos dias atuais esse ainda é o princípio de funcionamento da Internet. A fragmentação da rede perdura e traz consigo diversas conseqüências, que serão analisadas em momento oportuno.

Ironicamente a eficiência militar da Internet não foi comprovada em solo americano, mas em solo inimigo, dificultando as ações dos Estados Unidos, o país que desenvolveu tal modelo. Isso ocorreu durante a Guerra do Golfo, em 1991. Neste conflito os americanos sofreram com a dificuldade em desabilitar a rede de comando iraquiana, que utilizava um sistema similar.[2]

Em território brasileiro, o seu desenvolvimento teve início com a Rede Nacional de Pesquisa (RNP)[3], uma iniciativa do Ministério da Ciência e Tecnologia com o objetivo de criar uma infra-estrutura de serviços de Internet que possuísse abrangência sobre todo o território nacional. Foi implementada oficialmente a partir de 1989. Até abril de 1995, essa rede se limitava a áreas de educação e pesquisa, data em que deixou de se restringir ao meio acadêmico para se estender aos demais setores da sociedade, consolidando, assim, a internet comercial no país.

A explosão da internet veio com sua exploração comercial através do advento da World Wide Web[4] (WWW), protocolo idealizado por Vincent Cerf, considerado um dos pais da Internet, e criado para viabilizar que plataformas multimídias e providas de usabilidade fossem fornecidas ao usuário comum, tornando a atividade de acesso aos serviços mais fácil, abandonando definitivamente a imagem de rede de caráter meramente acadêmico e militar. Hoje, a internet conta com mais de dois bilhões de usuários[5] e tornou-se algo inerente a vida das pessoas, imprescindível para o correto funcionamento da sociedade como ela se encontra concebida. O mundo é um local interligado por grandes sistemas de informações e de dados, sejam eles direcionados para o âmbito individual, corporativo, militar ou público.

[2] Disponível em:< http://veja.abril.com.br/idade/exclusivo/iraque/capas/materias/iraque01.html>. Acesso em: 25 jul 2010.
[3] Disponível em:< http://www.rnp.br/rnp/historico.html>. Acesso em: 25 jul 2010.
[4] Disponível em:< http://www.icann.org/en/biog/cerf.htm>. Acesso em: 25 jul 2010.
[5] Disponível em:< http://www.internetworldstats.com/stats.htm>. Acesso em 25 jul 2010.

Para demonstrar a grandeza que a Internet atingiu, alguns dados objetivos podem ser expostos [6]: Em 2010, o número de pessoas da geração Y[7] irá sobrepor às oriundas da geração pós-guerra, denominada "Baby Boom", ou geração X; noventa e seis por cento das pessoas da geração Y utilizam redes sociais, ferramentas de agregação de conteúdo e contatos na internet; um em cada oito casais que casaram nos Estados Unidos da América após o ano de 2004 se conheceram através de mídias sociais; A televisão demorou treze anos para atingir cinquenta milhões de usuários. O Facebook[8], maior rede social na Internet atual, atingiu cem milhões de usuários em apenas nove meses e atualmente está com mais de 500 milhões[9] – caso fosse um país seria o quarto mais populoso do mundo; oitenta por cento das empresas americanas utilizam o LinkedIn[10], rede social corporativa, como forma primária de seleção de novos empregados. A Wikipedia[11], enciclopédia virtual e colaborativa, tem mais de treze milhões de artigos e estudos da revista *Nature* demonstram que seus dados são mais precisos do que os da Enciclopédia Britânica[12]; 78% dos consumidores acreditam em recomendações em redes sociais, enquanto apenas 14% confiam em propagandas.

Assim, a utilização da internet por mídias sociais para projetar seus conteúdos é uma mudança fundamental na maneira como nos comunicamos. No Brasil[13], um em cada três brasileiros já está conectado à internet, um total de setenta milhões de pessoas; O brasileiro gasta em média vinte e três horas por mês conectado à internet; setenta e nove por cento dos que usam a internet no Brasil fazem parte de redes sociais, onde gastam em media seis horas por mês, uma população total de quase cinquenta e cinco milhões de usuários, população esta maior do que qualquer estado brasileiro, e ainda maior que toda a população da Argentina; No Brasil, 52% dos usuários de redes sociais já interagiram com marcas nestes ambientes.

---

[6] **Social Media Revolution**. Disponível em:<http://www.youtube.com/watch?v=sIFYPQjYhv8>. Acesso em: 12 mai 2010.
[7] Pessoas nascidas entre os anos de 1980 e 2000.
[8] www.facebook.com
[9] Disponível em:< http://blog.facebook.com/blog.php?post=409753352130>. Acesso em: 21 jul 2010.
[10] www.linkedin.com
[11] www.wikipedia.com
[12] Disponível em: <http://www.nature.com/nature/journal/v440/n7084/full/440582b.html>. Acesso em 14 mar 2010.
[13] **Redes sociais.br.** Disponível em:<http://clickaqui.agenciaclick.com.br/video/redessociaisbr-1>. Acesso em 08 mai 2010.

1.2 Sociedade da informação

Desde os primórdios da civilização, o ser humano tem aplicado a sua singular inteligência no sentido de transformar e adaptar o meio em que vive, tornando-o adequado às suas necessidades. A aplicação dessa inteligência, primeiramente, era precipuamente direcionada a facilitar a atividade agrícola, através da invenção de instrumentos e do aprimoramento das técnicas. Porém, com o tempo, tornou-se necessário ao homem registrar suas idéias, de forma que seu conhecimento fosse preservado e transmitido às gerações vindouras, o que se tornou possível graças à invenção da escrita.

No entanto, o acesso a esse conhecimento escrito era restrito a poucos, tornando-se mais amplo a partir do advento da imprensa, que possibilitou a reprodução de textos em larga escala, possibilitando um acesso cada vez maior a obras escritas.

Tal amplitude no acesso ao conhecimento deu ensejo a diversas transformações na humanidade, resultando em acontecimentos que mudariam o curso da história, tais quais a ascensão da sociedade burguesa em detrimento dos nobres, o Iluminismo e a Revolução Francesa, a Revolução Industrial, as Guerras Mundiais, e o crescente desenvolvimento econômico e tecnológico.

Referidos progressos tecnológicos ocorreram mais diversos campos, porém é imperioso notar que, nos ramos das telecomunicações, da informática e da transmissão de informações, a velocidade de tais avanços parece ser surpreendentemente maior do que em outras searas.

Desde o advento das primeiras unidades de processamento eletrônico de dados (computadores), tal a velocidade e o dinamismo com que ocorrem tais operações, percebeu-se a facilidade com que as informações eram transmitidas, trabalhadas e armazenadas. Ao invés de pilhas de papéis, inúmeros livros e registros, as informações eram armazenadas nestas unidades, sob a forma de *bits*: unidades digitais binárias que eram processadas e interpretadas pelos computadores. Tudo estava ao alcance de um simples comando, o qual era dado à máquina: tão logo fosse dado o comando, o computador iniciava o processamento dos *bits* e estes eram transformados em dados, conhecimento, informações que chegavam prontas ao homem, para que este as usasse conforme bem entendesse.

A praticidade e a facilidade na manipulação e armazenamento desses dados digitais tornaram seu uso uma tendência que incessantemente cresceria conforme os avanços tecnológicos que, a partir daí, surgiriam, dando ensejo a um verdadeiro fenômeno: o fenômeno da digitalização, ou seja, o predomínio do armazenamento e difusão de dados em formato digital.

Tal fenômeno foi impulsionado, a partir das últimas décadas do Século XX, pelo advento dos Computadores Pessoais (PCs), que tornou possível a qualquer indivíduo o usufruto de tais informações digitais. Com isso, ampliou-se o acesso, pelo público, às inovações digitais, tais como os programas de computador (*softwares*) e as bases de dados eletrônicas, que adquiriram *status* de bens.

Com efeito, sabe-se que o homem, na busca por, cada vez mais, desejar aprimorar seu conhecimento, sempre precisou comunicar-se e trocar informações com outros. Daí falarmos em "Sociedade da Informação", que assim pode ser conceituada:

> A expressão "Sociedade da Informação" refere-se a um modo de desenvolvimento social e económico em que a aquisição, armazenamento, processamento, valorização, transmissão, distribuição e disseminação de informação conducente à criação de conhecimento e à satisfação das necessidades dos cidadãos e das empresas, desempenharam um central na actividade económica, na criação de riqueza, na definição da qualidade de vida dos cidadãos e das suas práticas culturais.[14]

Tal necessidade, enquadrada no contexto acima, acabou por pavimentar os caminhos para o surgimento de uma rede que ligasse, em escala global, os computadores, possibilitando a troca de informações entre eles. Essa rede se conduziria através do que José de Oliveira Ascensão chamou de "auto-estradas da informação", definindo-as como "meios de comunicação entre computadores, que seriam caracterizados por grande capacidade, rapidez e fidedignidade"[15], e que efetivamente vieram a se consubstanciar através da Internet.

---

[14] PORTUGAL. **Livro verde para a sociedade da informação em Portugal.** Lisboa: Ministério da Ciência e da Tecnologia, Missão para a Sociedade da Informação, 1997, p. 5. Disponível em <http://www2.ufp.pt/~lmbg/formacao/lvfinal.pdf>. Acesso em: 09 de abr 2010.

[15] ASCENSÃO, José de Oliveira. **Direito da Internet e da sociedade da informação:** estudos. 1. ed. Rio de Janeiro: Forense, 2002, p. 68.

O advento da Internet possibilitou à humanidade avançar a um novo nível de comunicação, de âmbito global, através do qual a troca de informações e dados atinge graus nunca antes concebidos de praticidade e velocidade. Nas palavras de Ascensão, a Internet "apresentou-se com um caráter atrativo, que levou a que os destinatários nela se empenhassem e adestrassem, e por outro lado ficassem dependentes deste modo de comunicação."[16]

Todavia, o termo Ssociedade da Iinformação decorre diretamente da estratégia de reorganização do pós-guerra, caracterizado por uma acelerada industrialização experimentada na segunda metade do século XX, que determinou alterações profundas na relação entre a tecnologia e o homem[17].

De forma mais específico, o termo Sociedade da Informação obteve suas primeiras referencias na década de 1970 nos EUA e no Japão, originárias de discussões sobre o que poderia caracterizar a sociedade pós-industrial e quais seriam suas principais facetas[18]. A Sociedade da Informação compreende, portanto, a informação desempenhando um papel imprescindível na vida econômica, política e social das pessoas, empresas e nações.

Entretanto, a definição para o termo Sociedade da Informação encontra diversas variantes, não sendo universalmente aceita de forma equânime. A mais aceita veicula como idéia principal o fato de que a evolução tecnológica permitiu a penetração das tecnologias da informação e comunicação no cotidiano coletivo, transformando-o completamente. Essa abordagem encontra respaldo em GIANNASI[19]:

> os avanços no processamento, recuperação, e transmissão da informação permitiram aplicação das tecnologias da informação em todos os cantos da sociedade, devido à redução de custos dos computadores, seu aumento prodigioso de capacidade de memória, e sua aplicação em todo e qualquer lugar, a partir da convergência e imbricação da computação e das telecomunicações.

[16] ASCENSÃO, *op. cit.*, p. 69.
[17] Ibid., p. 7.
[18] Ibid., p. 2.
[19] GIANNASI, Maria Júlia. **O profissional da informação diante dos desafios da sociedade atual**. Brasília, 1999. Tese (Doutorado) - Universidade de Brasília, Brasília, p. 21.

Nesse sentido, esse novo conceito de sociedade surgiu como fruto principalmente da penetração e da convergência das tecnologias da informação e comunicação, que aceleraram processos produtivos e de consumo, gerando o desenvolvimento econômico e a disseminação da informação e do conhecimento em volumes nunca antes vislumbrados. Estamos em processo de evolução e revolução constante, de forma cada vez mais rápida.

TOFFLER[20] enumera as premissas para a Sociedade da Informação, no que ele chamou de nova civilização, resultante do terceiro fluxo de mudança na história da humanidade, fato que impõe um novo código de comportamento, visto que "essa nova civilização traz consigo novos estilos de família; modo de trabalhar, amar e viver diferentes; uma nova economia; novos conflitos políticos; e além de tudo isso igualmente uma consciência alterada."

Ainda segundo TOFFLER, mudanças que alteraram por completo o modo de viver da sociedade aconteceram apenas outras duas vezes na história. A primeira quando a espécie humana passou de uma civilização eminentemente nômade para uma sedentária, a partir do domínio das tecnologias agrícolas. A segunda quando deixou de ser eminentemente agrícola para tornar-se uma sociedade industrial, ao se apoderar de novas tecnologias de fabricação de bens de consumo, em especial máquinas a vapor. Frise-se que a distinção básica entre um e outro fluxo é o surgimento de novas formas de criar riquezas, sempre acompanhada de mudanças profundas nos modelos sociais, culturais, políticos, filosóficos, econômicos e institucionais.

Essa nova realidade, caracterizada pelo surgimento e penetração massiva da Internet trouxe em conjunto com as atividades simples e corriqueiras outras formas de comunicação e de troca de informações, em um extenso leque de possibilidades, novas formas de trabalho, mesmo para aqueles que ainda não se encontram inseridos na nova economia. Esse nível de acessibilidade proporciona iniciativas que vão ao encontro dos pilares da democracia, possibilitando uma participação universal e igualitária a projetos e tomadas de decisões, eliminando fronteiras, barreiras sociais, culturais, políticas, econômicas e religiosas.

Portanto, no início do século XXI, a Internet alcança seu apogeu enquanto principal meio de acesso a informações e realização de operações da vida civil, tornando a todos dela

[20] TOFFLER, Alvin. **A terceira onda.** Rio de Janeiro: Record, 1997, p. 28.

dependentes, transformando a informática em ferramenta essencial ao progresso humano. Assim, o que se verifica é que "a Sociedade da Informação em que nos encontramos pode ser identificada, também, como Sociedade da Informática, ou Era Digital, ou Era Informacional."[21]

1.3 Um novo conceito de Estado

As conseqüências decorrentes da Sociedade da Informação são penetrantes ao ponto de alterarem os clássicos conceitos de Estado, criando um Estado Virtual em paralelo ao Estado Real, a um ponto onde não existe diferença entre os dois planos, compartilhando eles dos mesmos elementos constitutivos, principalmente o povo, que, ao ser provido de uma ferramenta de produção de conhecimento multidirecional e colaborativa, contribui para o enriquecimento da inteligência coletiva.

1.3.1 Breve histórico do Estado Moderno

Existem diversas teorias sobre o aparecimento do Estado. Elas podem, todavia, segundo DALLARI[22], ser delimitadas a três posições fundamentais. Para diversos autores, o Estado, assim como a sociedade em si, sempre existiu, visto que desde que o homem surgiu acha-se integrado a uma organização social, dotada de poder e com autoridade para determinar o comportamento de todo um grupo, sendo ele um elemento universal de organização social humana, um princípio unificador, portanto, onipresente na sociedade humana.

Uma segunda ordem de autores admite que a sociedade humana existiu sem a presença do Estado por um período de tempo. Após, este foi constituído para atender as necessidades e conveniências dos grupos sociais. Segundo esses autores, que configuram a maioria dos

[21] BARBOSA, Fábio. **A eficácia do direito autoral face à sociedade da informação:** uma questão de instrumentalização na obra musical? In: BRASIL. Ministério da Cultura. **Direito Autoral.** Brasília: Ministério da Cultura, Coleção Cadernos de Políticas Culturais, 2006. v. 1, p. 366.
[22] DALLARI, Dalmo de Abreu. **Elementos de Teoria Geral do Estado**. São Paulo: Saraiva, 1998, p. 78.

doutrinadores, não houve concomitância geográfica na formação dos Estados, uma vez que este foi surgindo de acordo com as condições de cada região.

A terceira posição, adotada por este estudo, admite o Estado como a sociedade política dotada de certas características bem definidas. Defendem que o conceito de Estado não é um conceito geral válido para todos os tempos, mas um conceito histórico concreto, que surge quando nasce a idéia e a prática da soberania, fato que somente se deu a partir do século XVII, sendo por muitos exposto que o ato ensejador específico se deu em 1648, ano em que foi assinado o Tratado de Paz de Westfália, nas cidades de Munster e Onsbruck, considerado o fator divisor entre o Estado Medieval e o Estado Moderno. O tratado fixou os limites territoriais resultantes das guerras religiosas, mormente a Guerra dos 30 anos entre França e Alemanha.

Nesse ensejo, o território passou a ser considerado elemento constitutivo de um Estado, assim como a soberania sobre a área limítrofe. Decorrente dessas duas características se estabelece o terceiro elemento, qual seja, o povo que se encontra nesse território delimitado e sobre o qual a soberania é exercida, nesse caso no âmbito interno. Quando esta é exercida sobre outros Estados, em equilíbrio, se cria uma relação de independência e convivência. Como conceitua MARTINEZ:

> Pode-se dizer que é até uma questão de lógica que se defina o Estado a partir das relações entre Povo, Território e Soberania. Pois é preciso que haja um mínimo de organização social e política para que as instituições tenham um sentido claro e vivido, e é óbvio, então, que é por obra desse mesmo povo ou de seus lideres que existem tais instituições. Também é de se esperar que esse povo ocupe ou habite um determinado território.[23]

Jorge Miranda[24], todavia, explana que o Estado baseado na tríade povo, território e soberania é apenas um dos tipos possíveis de Estado: seria o Estado nacional soberano que, nascido na Europa, se espalhou recentemente pelo mundo. Para diferenciar, delineia outras

[23] MARTINEZ, Vinício C. **Estado de Direito Político**. Jus Navigandi, Teresina, a. 8, n. 384, 26 jul. 2004. Disponível em: <http://www1.jus.com.br/doutrina/texto.asp?id=5496>. Acesso em: 04 mar. 2010.
[24] MIRANDA, Jorge. **Teoria do estado e da constituição**. Rio de Janeiro: Forense, 2003, p. 19.

características, como complexidade de organização e atuação, institucionalização, coercibilidade e autonomização do poder político, além da sedentariedade[25].

Como já mencionado, iremos adotar nesse estudo a idéia do Estado composto pelos três elementos clássicos, sendo necessária a conceituação da existência deles no âmbito virtual para que possamos moldar o que seria o Estado Virtual ou Estado Cibernético.

1.3.2 Estado virtual

Até o presente momento, o conceito utilizado de Sociedade da Informação foi no sentido amplo, *lato*, necessário para demonstrar a nova formatação que foi dada a sociedade com a utilização massiva e onipresente de tecnologias da informação e de comunicação. Agora, tentaremos expor uma aplicação diferente, a fim de conceituar o que seria o Estado Virtual, onde sociedade da informação (em minúsculo) faz referencia a uma nova concepção de povo, em que os hábitos desta, suas relações sociais e intersubjetivas, não podem mais ser concebidos sem a influência da Internet e das tecnologias da informação.

Na medida em que a sociedade da informação vai se estabelecendo em um país, inicia-se um processo de construção do Estado Virtual através de seus três elementos constitutivos: espaço cibernético, sociedade da informação e natureza autorregulativa. Necessário, todavia, definir o que seria o espaço cibernético. Segundo Pierre Levy, em palestra ministrada no Brasil em 1994 sobre o tema:

> O espaço cibernético é um terreno onde está funcionando a humanidade, hoje. É um novo espaço de interação humana que já tem uma importância enorme sobretudo no plano econômico e científico e, certamente, essa importância vai ampliar-se e vai estender-se a vários outros campos, como por exemplo na Pedagogia, Estética, Arte e Política. O espaço cibernético é a instauração de uma rede de todas as memórias informatizadas e de todos os computadores[26].

[25] MIRANDA, Jorge. Op. cit. p. 22.
[26] LEVY, Pierre. **A emergência do cyberspace e as mutações culturais**. Porto Alegre, 1994. Disponível em: <http://caosmose.net/pierrelevy/aemergen.html>. Acesso em: 20 jul 2010.

O espaço cibernético existe quando agregamos todas as informações produzidas pela sociedade com todos os computadores e tecnologias da informação e da comunicação. Cria-se uma entidade viva e independente, que proporciona ferramentas de comunicação que diferem das demais, visto que torna os atos comunicacionais interativos e construtores de uma nova realidade autopoiética, que se retroalimenta com o que já se encontra no espaço, que armazena todas as informações e conhecimentos de forma infinita. A partir do momento em se tem acesso a isso, cada pessoa pode se tornar uma emissora e construtora de toda a realidade, introduzindo um novo tipo de interação, proporcionando o que pode ser considerado "a emergência de uma inteligência coletiva". Ainda, segundo LEVY:

> o espaço cibernético está se tornando um lugar essencial, um futuro próximo de comunicação humana e de pensamento humano. O que isso vai se tornar em termos culturais e políticos permanece completamente em aberto, mas, com certeza, dá para ver que isso vai ter implicações muito importantes no campo da educação, do trabalho, da vida política, das questões dos direitos, como por exemplo, no direito de propriedade.[27]

O espaço cibernético traz consigo a origem de uma nova arquitetura, de um novo urbanismo. Uma nova política surge porque se trata de uma nova polis que se está constituindo[28]. Temos, portanto os meios de restauração de uma democracia direta e em grande escala, porque, até agora, a democracia direta só podia funcionar em pequena monta, fazendo com que para milhares de pessoas espalhadas em territórios mais distantes não fossem envolvidas. Com o uso de novos instrumentos técnicos é possível efetivar uma democracia direta distinta do sistema de representação.

A exemplo do espaço real, no espaço cibernético também são estabelecidas relações sociais e políticas, no tempo e no espaço, a partir qual o povo que nasce desses relacionamentos passa a tomar decisões de como construir parte de suas vidas, numa sociedade a princípio autorregulada e autônoma, permitindo a troca de informações das mais variadas formas. Completando os elementos do Estado, o povo estaria caracterizado pela Sociedade da informação; o território pelo próprio espaço cibernético; e a soberania pela capacidade de controlar, de exercer poder de decisão e regulamentação sobre este espaço.

[27] Ibid.
[28] Ibid.

1.3.3 Estado online

Várias nações já determinaram como políticas de Estado a inserção digital. Alguns já se autoproclamaram digitais, como Finlândia[29], Coréia do Sul e Estônia. Essa política de estado é encabeçada pelos países como forma de se adequar, principalmente, as novas realidades econômicas. O capitalismo globalizado baseado nas tecnologias da Informação, ou Supercapitalismo[30], é fator determinante para a implementação dessas políticas públicas.

O fato do Estado estar inserido digitalmente não só traz benesses, mas também malefícios que podem levar a um desmantelamento da nação, através de ataques cibernéticos, principalmente a estruturas críticas que funcionam com plano basal de uma sociedade moderna. Atentados contra essas infraestruturas já aconteceram e hoje são objeto de doutrina militares e projetos governamentais, como será abordado mais a frente nesse trabalho

Todavia, ainda são iniciais os estudos sobre os impactos das tecnologias da informação e da comunicação na vida política das sociedades contemporâneas. Não obstante, já é possível afirmar que estas têm influencia muito grande sobre os atuais modelos de gestão governamental, sobre a formulação e o controle de políticas públicas e sobre a tomada das decisões fundamentais de uma nação.

Alguns autores, como SORJ, classificam esses impactos em três níveis: no nível administrativo, pela utilização das tecnologias da informação, sobretudo a *Internet*, para aumentar a eficácia, a eficiência, a qualidade, a transparência e a fiscalização das ações e serviços governamentais - governança eletrônica ou *e-governança*; no nível de gestão, pela formulação de instrumentos que permitam aumentar ou qualificar a participação dos cidadãos na gestão pública e sobre as decisões governamentais (governo eletrônico ou *e-governo*); e no nível político, pela concepção de estruturas e instrumentos de organização política da sociedade (política eletrônica ou *e-política*)[31].

No primeiro nível, destaca-se a utilização da *Internet* na divulgação das atividades dos

[29] Disponível em: <http://www.finlandia.org.pt/public/default.aspx?nodeid=39498&contentlan=17&culture=pt-PT>. Acesso em: 08 jul 2010.
[30] Ver: REICH, Robert B. **Supercapitalismo - Como o capitalismo tem transformado os negócios, a democracia e o cotidiano**. São Paulo: Saraiva, 2008.
[31] SORJ, Bernardo. **A democracia inesperada: cidadania, direitos humanos e desigualdade social**. Rio de Janeiro: Jorge Zahar, 2004, p. 48-49.

órgãos públicos, suas atribuições e competências, incluindo o acompanhamento dos gastos públicos, da qualidade e da eficiência dos serviços públicos prestados. Encontram-se neste âmbito as iniciativas de prestação de serviços *on line*, tais como a emissão de certidões, solicitações de serviços diversos, pagamento de contas, tributos e declaração de impostos, licitações eletrônicas, peticionamento eletrônico e acompanhamento processual, entre outros. Cuida-se, então, da *informatização dos serviços governamentais*, indutores da universalidade do acesso a esses serviços.

No segundo nível encontram-se as iniciativas interativas, de participação na gestão da coisa pública, na definição das prioridades que serão objeto de tratamento pelas políticas governamentais e na possibilidade de influenciar a produção de normas jurídicas. Exemplos atuais podem ser encontrados na formulação do Marco Civil da Internet brasileira[32], que teve suas duas primeiras fases abertas para consulta e seu texto foi produzido de forma colaborativa, com sugestões de todos os espectros da sociedade. Outro exemplo que adotou a mesma metodologia é a reforma da Lei de Direitos Autorais brasileira (Lei 9.610/98). A chamada Lei da Ficha Limpa (Lei complementar 135/2010), que determina que políticos condenados por um corpo colegiado de juízes são inelegíveis, foi um projeto de lei popular que encontrou força na rede social de *microblogging* Twitter[33]. A influência da movimentação popular causada pela participação online foi tamanha que foi fator decisivo na escolha de um dos candidatos a vice-presidência da República do Brasil no pleito eleitoral de 2010, por este ter sido o responsável pelo arregimento virtual[34].

No terceiro nível, instrumentos de participação política direta por intermédio de tecnologias da informação são propostos, combatendo a histórica crise de legitimidade do modelo representativo. Em um quarto nível, afora os propostos pelo autor citado, se encontram as tecnologias da informação e de comunicação que funcionam como estrutura básica para o funcionamento do Estado. Elas sustentam e economia de uma nação e tornam possível a existência de um país devidamente inserido na comunidade internacional, com base no comércio internacional e numa economia de mercado. Essas infraestruturas das tecnologias da informação podem ser encontradas nas redes de energia (*smart grids*), sistemas de

[32] Disponível em: < http://culturadigital.br/marcocivil/>. Acesso em: 28 jul 2010.
[33] www.twitter.com
[34] **Quem indicou Índio da Costa foi o Twitter**. Disponível em:< http://colunistas.ig.com.br/poderonline/2010/07/04/quem-indicou-indio-da-costa-foi-o-twitter/>. Acesso em: 28 jul 2010.

comunicação, de transporte de água, de esgoto. Todos hoje controlados por sistemas automatizados interligados entre si pela Internet[35]. Por serem figuras estruturantes de uma nação, essas infraestruturas são hoje a maior preocupação quando o assunto é ataques cibernéticos.

Os dois primeiros níveis podem ser agrupados numa mesma realidade, denominada de *governo eletrônico*, diferenciando-os de acordo com o serviço público prestado, e o terceiro nível como *democracia eletrônica*. O quarto nível será alvo de discussão pormenorizada em capítulos subsequentes.

1.3.4 O governo eletrônico

Para enfrentar os novos paradigmas do século XXI, o Brasil, principalmente no âmbito do governo federal, lançou suas bases para a criação de uma nova sociedade digital, tendo se preocupado inclusive com os que estão excluídos desta realidade, equipando vários locais públicos com terminais eletrônicos para o acesso livre dos cidadãos.[36]

Registra-se que o Brasil tem desenvolvido uma das mais bem-sucedidas experiências mundiais em governo eletrônico, proporcionando uma significativa melhora no serviço público e tendo muita aceitabilidade pela sociedade, conforme se comprova no fato de 90% (noventa por cento) dos brasileiros estarem fazendo suas declarações anuais do imposto de renda pela Internet.[37]

O tempo atual exige mudanças e, para isto, necessita-se de profundas reflexões para criar novas estruturas jurídicas ante a impossibilidade de manter as atuais. Infelizmente, comprova-se que no campo do Direito há uma insistência na petrificação das idéias, sempre com pouca disposição para mudanças. Mesmo os mais modernos concentram suas idéias e desenvolvem suas teorias numa arquitetura institucional e jurídica em visível declínio, conservando conceitos incompatíveis com os dias atuais.

---

[35] SCADA – Supervisory Control and Data Acquisition, sistema de supervisão é um tipo software que permite monitorar e controlar partes ou todo um processo industrial.

[36] O Decreto Presidencial de 3 de abril de 2000 criou o Grupo de Trabalho em Tecnologia da Informação, com objetivo de implementar o *governo eletrônico*. Disponível em: <http://www.governoeletronico.gov.br >.

[37] Informação disponível em: <http://www.serpro.gov.br/publicacoes/tema/materia04s.htm> . Acesso em: 16 abr. 2010. Ver também: <http://www.redegoverno.gov.br >.

É preciso repensar as estruturas jurídicas com os dados atuais da informática, da virtualidade, dos novos parâmetros temporais, da descentralização, da democracia participativa, da administração transparente e eficaz com custos mínimos do Estado-gestor, enfim, de relevantes instrumentos que surgiram nestas últimas décadas, que são responsáveis por esta gama de transformações no cotidiano.

Vive-se hoje no chamado tempo pontual, instaurado pela informática, que permite a noção do tempo real numa velocidade pura sem horizontes. Como destaca Pierre Lévy, a evolução do pensamento humano vivencia três pólos distintos, quais sejam, o da **oralidade** (circular), o da **escrita** (linear), e o da **informática** (virtual)[38], sendo este último responsável pela entrada em um novo ritmo que não é mais o da história. A condensação no presente da operação em andamento é ainda um desafio para o Direito.

Analisando o Direito sob este prisma, constata-se que a evolução da interpretação das normas jurídicas é semelhante às formas canônicas do saber, elencadas por Pierre Lévy*:* i) narração; ii) interpretação; iii) simulação e previsão. *[39]*

Antigamente, tinha-se uma vinculação rigorosa ao texto escrito, cuja literalidade o aplicador da lei devia se ater; passa-se, então, para uma visão sistêmica, permitindo ir além da literalidade, analisando todo o sistema jurídico; hoje, tem-se normas que incidem não só sobre os fatos, mas também sobre sua previsão, tanto no campo da interpretação quanto da própria lei, que também tem alcançado o campo dos atos simulados.

É preciso captar esta evolução do Direito para compreender a nova legislação que se instaura e, principalmente, para revogar a antiga, que vem contribuindo para o colapso da estrutura fiscal.[40]

---

[38] "A noção de tempo real, inventada pelos informatas, resume bem a característica principal, o espírito da informática: a condensação no presente, na operação em andamento. O conhecimento de tipo operacional fornecido pela informática está em tempo real. Ele estaria oposto, quanto a isto, aos estilos hermenêuticos e teóricos. Por analogia com o tempo circular da oralidade primária e o tempo linear das sociedades históricas, poderíamos falar de uma espécie de implosão cronológica, de um tempo pontual instaurado pelas redes de informática. O tempo pontual não anunciaria o fim 'da aventura humana', mas sim sua entrada em um ritmo novo que não seria mais o da história." LEVY, Pierre. **As tecnologias da inteligência: o futuro do pensamento na era da informática**, 1. ed. Lisboa: Instituto Piaget, 1992, p. 115.

[39] Op. cit., p. 127.

[40] "O aspecto nuclear da questão reside em diagnosticar corretamente o colapso da atual estrutura fiscal, pois que não urdida em consonância com as novas tecnologias de informação e desconforme com os preceitos do atual estádio de globalização financeira. Segundo o respeitável economista, a modernidade exige a substituição dos atuais impostos declaratórios (burocráticos por definição), por impostos de cobrança automática e de elaboração

Sendo a razão de existência do Estado a própria sociedade, suas estruturas devem se modernizar de forma a melhor atender àquela e não obstaculizá-la. Daí a grande preocupação atual com a sociedade digital excluída que não tem condições de se adequar às práticas prevalentes na atualidade.

No Brasil, o governo federal vem trabalhando no sentido de reduzir o percentual excluído desta nova realidade através de programas que têm como objetivo integrar, coordenar e fomentar ações para a utilização de tecnologias de informação e comunicação, de forma a contribuir para a inclusão social de todos os brasileiros nesta nova sociedade e também contribuir para que a economia do País tenha condições de competir no mercado global.

É claro que esta evolução será a longo prazo, porém, o importante é que os primeiros passos já estão sendo dados e que o Brasil está acompanhando os processos de adaptação e estruturação da administração fazendária, decorrentes dos avanços tecnológicos em todo o mundo. Uma das dimensões presentes na relação envolvendo capacidade governativa e informação se faz presente na perspectiva do governo eletrônico (e-gov).

Em linhas gerais, o governo eletrônico expressa uma estratégia pela qual o aparelho de Estado faz uso das novas tecnologias para oferecer à sociedade melhores condições de acesso à informação e serviços governamentais, ampliando a qualidade desses serviços e garantindo maiores oportunidade de participação social no processo democrático.

Considera-se que o governo eletrônico pode ampliar a efetividade dos governos em quatro aspectos: (a) será mais fácil para a sociedade ter suas perspectivas consideradas pelos governos na (re)definição de políticas públicas; (b) a sociedade poderá obter melhores serviços das organizações governamentais, por exemplo, através de atividades desenvolvidas on-line; (c) sociedade contará com serviços mais integrados porque as diferentes organizações serão capazes de se comunicar mais efetivamente entre si; (d) a sociedade será melhor informada porque poderá obter informação atualizada e compreensível sobe o governo, leis, regulamentos, políticas e serviços.[41]

---

menos complexa." ENWEILER, Romano José. **Os desafios de tributar na era da globalização.** Florianópolis: Diploma Legal, 2000. p. 118-119.

[41] JARDIM, José Maria Jardim. **Arquivos, transparência do estado e capacidade governativa na sociedade da informação**. Disponível em: <www.oas.org/udse/espanol/documentos/1hub11.doc>. Acesso em: 26 set 2009.

Tais princípios, porém, esbarram em obstáculos diversos na execução de políticas que os viabilizem na realidade social. No caso neozelandês, por exemplo, há um claro reconhecimento de que oportunidades as mais diversas podem ser perdidas caso o Governo não assuma a responsabilidade de supervisionar e coordenar o desenvolvimento do *e-goverment* em benefício dos cidadãos. Esta perspectiva, porém, pressupõe considerar as conseqüências e desafios uma sociedade cuja desigualdade se expressa, entre outros aspectos, na existência de reconhecer dois segmentos sociais - aqueles que contam com qualificações e ferramentas para usar as novas tecnologias e os que não dispõem destas condições.

O conceito de governança inclui muito mais que o uso da Internet ou a disseminação de quiosques eletrônicos em repartições públicas. A maior premência, neste sentido, seria levar a burocracia a mudar sua cultura, assumindo como objetivos maiores a transparência, o diálogo permanente com a sociedade civil e o aprofundamento da noção de cidadania.

Um exemplo interessante, no caso dos Estados Unidos, é o *Government Printing Office*[42], que proporciona acesso a documentos da Agência de Impressão do Governo, incluindo todas as proposições de regulamentos federais e transcrições diárias das sessões do Congresso.

No Brasil, no âmbito do Governo Federal, através do site "Brasil Transparente"[43], é possível "a consulta pública para os anteprojetos de Emenda Constitucional e de Lei Complementar que reforçam os controles e a responsabilização pela aplicação dos recursos do Orçamento". O site ComprasNet[44] oferece acesso às licitações da Administração Federal em andamento, os resultados de licitações, os contratos do Governo Federal, linhas de fornecimento de material e serviço e publicação do fornecedor.

O Serviço Eletrônico de licitação canadense, o MERX[45], visa também facilitar a interação entre compradores de bens e serviços dentro das comunidades comerciais dos setores público e privado. É o principal canal de distribuição de licitações e documentos de licitação para todos os níveis do governo.

[42] http://www.access.gpo.gov/su_docs/aces/aaces002.html
[43] http://www.brasiltransparente.gov.br
[44] http://www.comprasnet.gov.br
[45] http://www.merx.cebra.com/

1.3.5 A cidadania eletrônica

O Estado atual não pode mais ser visto como "mistificante entidade soberana e mitológica"[46], mas, sim, como uma entidade entre os demais grupos sociais existentes, com a função precípua de administração, sempre voltado para o interesse da sociedade e cuja existência justifica-se no interesse da coletividade.

Na relação atual do Estado com o cidadão-contribuinte não se concebe mais o uso dos termos administrado, súdito, no sentido de submissão, apesar de serem ainda muito utilizados pela doutrina, contudo, talvez, pela força do hábito. O cidadão-contribuinte e o Estado, ambos com responsabilidades e Direitos recíprocos, estando sob a égide da lei, devem agir com transparência, eficiência, legalidade, celeridade, enfim, sempre buscando otimizar suas ações em prol do melhor da sociedade.

Dos vários papéis exercidos por ambos destacam-se, na presente análise, o do Estado, nas funções de arrecadação, fiscalização e controle dos tributos, e o do cidadão-contribuinte, como colaborador das atividades fiscais e responsável pelo pagamento dos tributos. Então, tanto o fisco, como o cidadão-contribuinte, tem suas funções bem definidas no contexto legal, cabendo ao fisco o poder-dever de tributar e ao cidadão-contribuinte o poder-dever de calcular e pagar seus tributos.

Destaca-se o poder do cidadão-contribuinte por sua capacidade de influenciar, condicionar, determinar o pagamento do tributo devido e, na medida em que a lei lhe dá os meios, ir muito mais além do que o mero pagamento, tendo, hoje, obrigações legais que determinam que ele arque com uma série de outros deveres para com o fisco, sem qualquer interferência direta da administração fiscal nestes atos.

1.3.6 A informatização do processo

Os avanços tecnológicos observados nos tempos modernos, notadamente a ampla utilização da informática, vêm revolucionando praticamente todos os campos das atividades

[46] BARROS, Benedicto Ferri de. **Relance de dois séculos de história – com vistas ao momento brasileiro**. In: Caderno de direito tributário e finanças públicas - vol.18, São Paulo: Revista do Tribunais. 1997, p. 308.

humanas. Na seara jurídica, em particular nas atividades ligadas aos processos judiciais, as novas tecnologias eletrônicas despertaram especial interesse. Vislumbrou-se a possibilidade de informatização dos procedimentos no Judiciário como uma das formas de realização de uma Justiça célere e eficiente.

O documento escrito hoje pode ser também virtual; a sede do estabelecimento pode estar na rede mundial e não em uma cidade; dados de auditoria fiscal podem estar numa mídia portátil e não num livro contábil; a declaração do imposto de renda não está necessariamente no papel e, sim, através da internet.

Até mesmo o conceito de tempo tem de ser revisto. A celeridade da informática também influencia os medidores do tempo, destacados na lei como dias, meses, anos, passando agora para o tempo exigido na informática, mensurado em minutos e frações destes. Antes desta realidade virtual, passavam-se horas na fila de uma repartição pública para pegar uma senha, para depois aguardar horas para ser atendido, para depois requerer dita certidão, que por sua vez seria liberada após alguns dias, devendo o interessado buscá-la na mesma repartição, novamente aguardando numa fila que poderia durar mais algumas horas. Isso delata a mudança dos nossos paradigmas temporais: três horas numa fila pode ser tão irritante quanto três minutos em frente à tela do computador aguardando o mesmo documento. Sem dúvida, Norberto Bobbio tem razão quando afirma que o progresso é "célere, irresistível e irreversível"[47]. Não se permite no mundo contemporâneo uma fila interminável para requerer qualquer serviço.

Efetivamente, a informatização do Poder Judiciário, em seus vários níveis, pode melhorar significativamente a qualidade da prestação jurisdicional. A última iniciativa do legislador processual, representada pela edição da Lei n. 11.419/06, completou o ciclo de normas jurídicas voltadas para a informatização completa do processo judicial no Brasil. Com efeito, o diploma legal em questão tratou, de forma razoavelmente detalhada, do uso dos meios eletrônicos na tramitação de processos, na comunicação de atos processuais e na transmissão de peças processuais. A referida introduziu o parágrafo segundo no art. 154 do Código de Processo Civil com a seguinte redação: "todos os atos ou termos do processo podem ser produzidos, transmitidos, armazenados e assinados por meio eletrônico". Assim, restou definida legalmente a mais ampla informatização do processo judicial. A lei chegou a

[47] BOBBIO, Norberto. **Teoria geral da política – a filosofia política e as lições dos clássicos.** Rio de Janeiro: 2000, p.670.

convalidar, desde que tenham atingido a finalidade própria e não tenha havido prejuízo para as partes, os atos processuais praticados por meio eletrônico até a data de sua publicação.

No art. 1º, parágrafo primeiro, do diploma legal referido foi estabelecida a aplicação do processo eletrônico aos feitos civis, penais e trabalhistas, inclusive aqueles em tramitação nos Juizados Especiais, independentemente da instância. A prática de ato processual informatizado, assim entendido como qualquer forma de armazenamento ou tráfego de arquivos digitais, exige o uso de assinatura eletrônica.

Os tribunais foram autorizados a criar, em site na internet, o "Diário da Justiça eletrônico". O instrumento em questão já vem substituindo qualquer outro meio e funciona como divulgação oficial para quaisquer efeitos legais, com exceção dos casos de intimação ou vista pessoal na forma da lei. Está prevista, também, a criação de um portal eletrônico específico a ser utilizado pelos interessados devidamente cadastrados. Assim, nos termos da lei, as intimações realizadas pelo portal dispensarão a publicação no órgão oficial (impresso ou eletrônico) e serão tidas como pessoais para todos os efeitos legais. Mesmo as citações podem ser eletrônicas, ressalvados os processos penais (mencionados na lei como "criminal e infracional"). Nesses casos, a íntegra dos autos judiciais deve estar disponível para o citando.

O meio eletrônico foi definido como padrão para as cartas precatórias, rogatórias, de ordem e para as comunicações oficiais entre os órgãos do Poder Judiciário e desses para os demais Poderes. O Poder Judiciário foi expressamente autorizado a desenvolver sistemas eletrônicos de processamento de ações judiciais com utilização preferencial da internet. A obtenção de autos total ou parcialmente digitais são os objetivos a serem perseguidos.

Deve ser destacado que o art. 8º da Lei do Processo Eletrônico foi o primeiro comando legal na ordem jurídica brasileira a consagrar expressamente a possibilidade do processo totalmente eletrônico (quando se refere aos autos totalmente digitais). Até a edição desse dispositivo legal, o desenvolvimento do processo totalmente virtual ou eletrônico, a exemplo daquele já existente nos Juizados Especiais Federais, buscava fundamento jurídico, como já registrado, na conjugação de normas pontuais sobre a prática de atos processuais em meios eletrônicos (arts. 1º e 2º da Lei nº 9.099/95; art. 8º da Lei nº 10.259/01; art. 225 da Lei nº 10.406/02 e parágrafo único do art. 154 do Código de Processo Civil, introduzido pela Lei nº 11.280/06) e de uma interpretação inteligente, generosa e evolutiva do princípio da documentação dos atos processuais.

Deverão ser realizadas por meio eletrônico todas as comunicações de atos processuais (citações, intimações e notificações), inclusive aquelas dirigidas à Fazenda Pública, no âmbito do processo digital. Os advogados das partes, sem intervenção do cartório ou secretaria judicial, poderão, conforme admite a lei de forma inovadora, distribuir iniciais e realizar a juntada de petições em formato eletrônico.

A lei da informatização do processo judicial reafirmou o reconhecimento jurídico do documento eletrônico e realizou uma série de definições relevantes acerca das relações entre o documento físico e o eletrônico e entre as noções de original e cópia. Com efeito, foi estabelecido que os documentos produzidos eletronicamente (e juntados aos autos digitais com garantia de origem e de autoria) são considerados originais para todos os efeitos legais. Portanto, não parece restar dúvida razoável acerca da possibilidade de um documento existir (juridicamente) tão-somente em formato eletrônico.

O novo parágrafo segundo do art. 154 do Código de Processo Civil, como visto, prevê que todos os atos processuais podem assumir a forma eletrônica. Apesar da regra geral e de amplo alcance, a lei especifica uma série de situações, dentro e fora do processo judicial, onde a informatização é admitida. Eis algumas das hipóteses onde o meio eletrônico foi expressamente autorizado por lei: a) registro de votos e acórdãos; b) fornecimento de documentos em repartições públicas; c) expedição de carta de ordem, carta precatória e carta rogatória; d) atos processuais praticados na presença do juiz; e) na assinatura dos juízes em todos os graus de jurisdição; f) na assinatura da procuração; g) nos livros cartorários e repositórios dos órgãos do Poder Judiciário; h) exibição e envio de dados e documentos necessários à instrução do processo; i) citações, intimações e notificações; j) comunicações oficiais entre os órgãos do Poder Judiciário e desses para os demais Poderes e l) envio de recursos e petições de forma geral.

1.4 Direitos fundamentais na sociedade da informação

Verifica-se que o direito a informação, que encontra a sua demonstração máxima na internet, como acima exposto, é classificado por BONAVIDES como um direito de quarta geração, ou melhor, de quarta dimensão, visto que não se sobrepõem, mas se concretizam:

> São direitos de quarta geração o direito à democracia, o direito à informação e o direito ao pluralismo. Deles depende a concretização da sociedade aberta do futuro, em sua dimensão de máxima universalidade, para qual parece o mundo inclinar-se no plano de todas as relações de convivência.[48]

Dispõe o art. 5º da Constituição Federal Brasileira de 1988 que todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade. O inciso IV do referido artigo dispõe que "é livre a manifestação do pensamento, sendo vedado o anonimato". Na medida em que a internet, por muitos chamada de "terra de ninguém", possibilita uma irreal ausência de identidade aos usuários que assim desejam, muitos deles se utilizam desse subterfúgio para manifestarem opiniões, muitas delas falaciosas, sem que, para tanto, se identifiquem.

O inciso VI dispõe que "é inviolável a liberdade de consciência e de crença, sendo assegurado o livre exercício dos cultos religiosos e garantida, na forma da lei, a proteção aos locais de culto e a suas liturgias". Esse mandamento de eficácia contida não tem obstado a prática de cultos religiosos que contém em seus procedimentos atos que afrontam a vida, a segurança e a imagem. Em redes sociais e em páginas da internet são facilmente encontradas apologias e formas variadas para a prática desses cultos não permitidos em lei.

Talvez o direito mais atingindo com a atual abrangência da internet, principalmente como meio de mídia, seja o assegurado pelo inciso X da CF/88, que afirma "serem invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação". Casos notórios ganharam a cena mundial depois de divulgados em um sítio da internet[49], demonstram como a vida privada está sendo banalizada com os adventos das novas tecnologias.

Afirma o inciso XII que "é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal", tudo em conformidade, ainda com a Lei nº 9.296/96. Entretanto,

---

[48] BONAVIDES, Paulo. **Curso de direito constitucional**. 19ª ed. atual. São Paulo: Ed. Malheiros, 2006, p. 571.

[49] Vídeo polêmico de Daniella Cicarelli ganha mídia internacional. Folha Online. Disponível em: <http://www1.folha.uol.com.br/folha/ilustrada/ult90u64480.shtml>. Acesso em: 18 dez 2007

a fragilidade dos sistemas informáticos, e a possibilidade de interceptação das comunicações, sejam elas por via telefônica, por e-mail, por mensageiros instantâneos, tem tornado a necessidade de decisão judicial algo secundário, em clara afronta ao texto da constituição federal, visto que muitas vezes as demandas nem sequer chegam ao controle jurisdicional, devido a pressões da imprensa[50] e extorsões por parte de indivíduos mal intencionados.

Muito se discute no âmbito jurídico a privacidade do e-mail corporativo e a utilização do e-mail particular em ambiente de trabalho, havendo decisões divergentes nos Tribunais do Trabalho[51]. Todavia, a posição majoritária defende ser inviolável a utilização de sistemas de correios eletrônicos pessoais, sendo, todavia, de propriedade do empregador aquele fornecido e utilizado no ambiente de trabalho.

O inciso XXII afirma "ser garantido o direito de propriedade", pode ser analisado conjuntamente com o inciso XXVII, que trata dos direitos autorais, aos dispor que "aos autores pertence o direito exclusivo de utilização, publicação ou reprodução de suas obras, transmissível aos herdeiros pelo tempo que a lei fixar". Em face do grande poder de transmissão de dados e a fragilidade dos próprios sistemas responsáveis por tais procedimentos, as indústrias cinematográfica, fonográfica e editorial tem sofrido enormes prejuízos com a divulgação ilegal de seus conteúdos proprietários. Entretanto, os maiores prejudicados não os grandes conglomerados industriais, mas sim os atores, músicos e escritores que sobrevivem da sua arte, mas passam a não receber os seus dividendos, pois

---

[50] Palocci ordenou a Mattoso violação do sigilo do caseiro. Folha online. Disponível em: <http://www1.folha.uol.com.br/folha/brasil/ult96u77207.shtml>. Acesso em: 18 dez 2007.

[51] *"Despedida por justa causa. Mau procedimento. Uso indevido de correio eletrônico. Quando se caracteriza. Prova que evidencia a utilização do email funcional, pelo empregado, para difundir informações tendentes a denegrir a imagem da empregadora. Constitui justa causa para a despedida o uso indevido do correio eletrônico fornecido pelo empregador, não se podendo cogitar de infração ao disposto no artigo 5º, inciso XII da CF, já que o serviço de "e-mail" é ferramenta fornecida para uso estritamente profissional. Sentença mantida." (TRT4, Rel. Flavio Portinho Sirangelo, RO nº 00168-2007-203-04-00-3 (RO), jul. 03/09/2008).*
"Correio eletrônico. Monitoramento. Legalidade. Não fere norma constitucional a quebra de sigilo de e-mail corporativo, sobretudo quando o empregador dá a seus empregados ciência prévia das normas de utilização do sistema e da possibilidade de rastreamento e monitoramento de seu correio eletrônico. (...) Comungo do entendimento a quo no sentido de afastar a alegada ofensa aos incisos X, XII, LVI do art. 5º constitucional, por não ferir norma constitucional a quebra de sigilo de e-mail fornecido pela empresa, sobretudo quando o empregador avisa a seus empregados acerca das normas de utilização do sistema e da possibilidade de rastreamento e monitoramento de seu correio eletrônico. Também o julgado recorrido consignou ter o empregador o legítimo direito de regular o uso dos bens da empresa, nos moldes do art. 2º da CLT, que prevê os poderes diretivo, regulamentar, fiscalizatório e disciplinar do empregado, inexistindo notícia acerca de excessiva conduta derivada do poder empresarial." (TST, Rel. Min. Vieira de Mello Filho, Ag. Instr. em RR nº 1130/2004-047-02-40, j. 31/10/2007).

estes não mais são adquiridos mediante contraprestação pecuniária, mas sim gratuitamente através da internet, sem a autorização de seus autores[52].

Caso emblemático no território nacional foi o do filme Tropa de Elite[53], que mesmo antes de chegar aos cinemas já estava disponível na internet para ser copiado e também em todos os camelôs do país, tudo devido à reprodução ilegal da obra através dos chamados programas de transmissão de arquivos. A pirataria na internet já é responsável por um prejuízo anual de R$ 30 bilhões aos cofres públicos[54].

As violações aos incisos abaixo transcritos restam evidenciadas no número de denúncias feitas em relação a usuários e comunidades da Rede Social Orkut[55] que praticam delitos como racismo, apologia a drogas, ao terrorismo, a crimes hediondos, em claro malferimento a direitos fundamentais elencados no art. 5º da Carta Magna brasileira:

> XLI - a lei punirá qualquer discriminação atentatória dos direitos e liberdades fundamentais;
>
> XLII - a prática do racismo constitui crime inafiançável e imprescritível, sujeito à pena de reclusão, nos termos da lei;
>
> XLIII - a lei considerará crimes inafiançáveis e insuscetíveis de graça ou anistia a prática da tortura, o tráfico ilícito de entorpecentes e drogas afins, o terrorismo e os definidos como crimes hediondos, por eles respondendo os mandantes, os executores e os que, podendo evitá-los, se omitirem;
>
> XLIV - constitui crime inafiançável e imprescritível a ação de grupos armados, civis ou militares, contra a ordem constitucional e o Estado Democrático;

O remédio constitucional do *habeas data*, instrumento acrescido à constituição de 1988 e previsto no art. 5º, inc. LXXII, torna-se imprescindível no atual estágio da internet, das telecomunicações e dos bancos de dados, uma vez que a maioria dos bancos de dados das

---

[52] O site Pirate Bay, com sede na Suécia, foi condenado, por entenderem que ele permitia que arquivos ilegais que violavam direitos autorais. **The Pirate Bay é condenado por violar propriedade intelectual.** Disponível em: <http://www.estadao.com.br/noticias/tecnologia,the-pirate-bay-e-condenado-por-violar-propriedade-intelectual,356348,0.htm>. Acesso em: 20, jul 2009.

[53] Inédito, filme "Tropa de Elite" já é vendido em DVD por camelôs do RJ. Folha online. Disponível em: <http://www1.folha.uol.com.br/folha/ilustrada/ult90u320738.shtml>. Acesso em: 18 dez 2007;
Tropa de Elite: Recorde de público pirata. Extra online. Disponível em: <http://extra.globo.com/rio/materias/2007/09/06/297630049.asp>. Acesso em: 18 dez 2007.

[54] Pirataria no Brasil custa por ano R$ 30 bilhões aos cofres públicos. Portal Verdes Mares. Disponível em: <http://verdesmares.globo.com/v3/canais/noticias.asp?codigo=193461&modulo=181>. Acesso em: 18 dez 2007.

[55] www.orkut.com.br

entidades públicas, assim como os registros dos cidadãos, se encontram no mundo virtual, podendo facilmente ser alvos de ataques por criminosos cibernéticos, modificando esses dados, apagando-os e até utilizando-os para fins ilícitos.

O Brasil é, hoje, líder mundial de spams, mensagens indesejadas enviadas por e-mail. O mundo envia 160 bilhões de spams por dia, e desses, 15% (quinze por cento) são provenientes do nosso país. O envio diário de spams representa um gasto diário de 33 bilhões de quilowatts, o que equivale ao consumo médio de 22 (vinte e dois) milhões de casas[56].

Todavia, hoje em dia, podemos vislumbrar duas modalidades de delitos que mais atingem a economia e a soberania de um país como um todo. São elas a fraude eletrônica e o ciberterrorismo. A fraude eletrônica passou a ser uma atividade mais lucrativa do que a perpetrada no mundo real. Sendo, inclusive, mais rentável do que o tráfico internacional de drogas, rendendo em 2004 cerca de 105 bilhões de dólares a mais que o tráfico[57]. No Brasil, os crimes de internet rendem mais do que o tráfico de drogas, segundo fontes da Polícia Federal[58]. Isso fez com que as organizações criminosas nacionais e transnacionais mudassem e rumo a passassem a investir nas modalidades criminosas virtuais. A ingerência dessas organizações na rede evoluiu ao ponto que esta passou a ser utilizada como meio propício para a prática de terrorismo, ameaçando a soberania estatal[59]. A abrangência global e instantaneidade da internet propiciou um meio ideal para os objetivos das organizações criminosas transnacionais.

Nesse contexto, os brasileiros percebam o acesso a Internet como um direito fundamental,[60] a grande maioria da população ainda está fora do mundo virtual, todavia.[61]

---

[56] **McAfee Virtual Criminology Report**. Estados Unidos da América: McAfee, 2009.

[57] SILVESTRE, Paulo. **Crimes digitais fazem mais dinheiro que drogas**. Revista INFO, nov. 2005.

[58] **Crimes na internet rendem mais que tráfico de drogas no Brasil, diz PF**. Disponível em:< http://www1.folha.uol.com.br/folha/informatica/ult124u403907.shtml>. Acesso em: 20 jul 2009.

[59] **Supostos cyber ataques globais: 2009:** EUA culpa a Coréia do Norte por ataques sincronizados aos sites da Casa Branca, Pentágono e Wall Street, assim como diversos outros sites em países diferentes; 2008: Durante a guerra da Ossétia do Sul, Georgia que a Rússia atacou sites oficiais e a Rússia acusou a Georgia de se infiltrar em sua agência de notícias; 2007: Os sites do Governo da Estônia e de mídia foram assaltados virtualmente depois de conflitos com a Rússia sobre um memorial de guerra soviético; 2007: Os EUA culparam a china por ataques aos computadores do Pentágono. Disponível em: <http://tecnologia.terra.com.br/interna/0,,OI3864451-EI4802,00-Hackers+tacam+Casa+Branca+Pentagono+e+Wall+Street.html>, <http://news.sky.com/skynews/Home/UK-News/Cyber-Terrorism-Threat-To-Britain-New-Cyber-Security-Centre-Opened-To-Combat-Cyber-Attack-Threat/Article/200906415319307>. Acesso em: 20 jul 2009.

60 Conforme pesquisa realizada pelo instituto internacional GlobeScan em mais de 26 países, quatro entre cinco adultos consideram o acesso à Internet como direito fundamental do ser humano, tendo 91% dos entrevistados brasileiros concordado com esse ponto de vista. Disponível em:

Reconhecer a fundamentalidade deste direito enquanto milhares de pessoas sequer têm a oportunidade de gozar de suas benesses parece à primeira vista contraditório. É na superação dessa suposta incoerência que repousará as próximas linhas. No arrimo dos ensinamentos de José Afonso da Silva, pode se definir os direitos fundamentais como:

> aquelas prerrogativas e instituições que ele concretiza em garantia de uma convivência digna, livre e igual de todas as pessoas. No qualificativo *fundamentais* acha-se a indicação de que se trata de situações jurídicas sem as quais a pessoa humana não se realiza, não convive e, às vezes, nem mesmo sobrevive, fundamentais *do homem* no sentido de que a todos, por igual, devem ser, não apenas formalmente reconhecidos, mas concreta e materialmente efetivados. [62]

Há no ordenamento jurídico brasileiro, direitos fundamentais formais e materiais. Os primeiros são "as posições jurídicas subjetivas protegidas pela Constituição Formal por estarem nela inscritas".[63] Já os segundos são "pretensões que, em cada momento histórico, se descobrem a partir da perspectiva do valor da dignidade humana"[64]. Conquanto a Constituição da República Federativa do Brasil de 1988 albergue em seu Título II, Capítulos I e II, artigo 5º e seguintes, um conjunto de direitos fundamentais, constata-se que a mesma não teve intuito de exauri-los. Isto porque conforme seu artigo 5º, §2º "os direitos e garantias expressos nesta Constituição não excluem outros decorrentes do regime e dos princípios por ela adotados, ou dos tratados internacionais em que a República Federativa do Brasil seja parte". Essa abertura material do catálogo de direitos fundamentais significa dizer:

> que para além daqueles direitos e garantias expressamente reconhecidos como tais pelo Constituinte, existem direitos fundamentais assegurados em outras partes do texto constitucional (fora do Título II), sendo também acolhidos os direitos

---

<http://www.bbc.co.uk/portuguese/noticias/2010/03/100307_pesquisabbc_internetml.shtml>. Acesso em: 25 jun. 2010.

61 Segundo levantamento efetuado pelo CETIC.br, através da pesquisa sobre o uso das Tecnologias da Informação e da Comunicação no Brasil (TIC), dentre os brasileiros na faixa de renda de 1 (um) salário mínimo apenas 20% são usuários de Internet contra 86% dos que ganham acima de 10 (dez) salários mínimos. Já em relação ao grau de instrução, daqueles que tem o ensino infantil ou são analfabetos apenas 11% são usuários da Internet contra 93% daqueles que têm nível superior. In: COMITÊ GESTOR DA INTERNET NO BRASIL. **Pesquisa sobre o uso das Tecnologias da Informação e da Comunicação no Brasil: TIC domicílios e TIC empresas**. BARBOSA, Alexandre F. (Coord.). São Paulo: CGI, 2010, p. 241.

62 SILVA, José Afonso da. **Curso de direito constitucional positivo**. 31 ed. rev. e atual (até a Emenda Constitucional n. 56, de 20.12.2007). São Paulo: Malheiros, 2008, p 178.

63 MIRANDA, Jorge. **Manual de direito constitucional - Tomo IV**. 3 ed. Coimbra: Coimbra Editora, 2000, p. 9.

64 MENDES, Gilmar Ferreira; COELHO, Inocêncio Mártires; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional**. 4. ed. rev. e atual. São Paulo: Saraiva, 2009, p. 271.

> positivados nos tratados internacionais em matéria de Direitos Humanos. Igualmente – de acordo com a expressa dicção do artigo 5º, §2º, da nossa Carta Magna – foi chancelada a existência de direitos não-escritos decorrentes do regime e dos princípios da nossa Constituição, assim como a revelação de direitos fundamentais implícitos, subtendidos naqueles expressamente positivados. [65]

Questão essencial advinda da assertiva acima é a de quais direitos que não estão expressamente previstos no texto constitucional podem ser considerados como fundamentais sem que isso leve a uma banalização no seu tratamento[66]. Para responder a esta indagação, apoiado na doutrina de Ingo Wolfgang Sarlet, aposta-se na conexão entre o princípio da dignidade da pessoa humana com os direitos fundamentais para a construção de um conceito materialmente aberto de direitos fundamentais. Para o autor:

> o que se pretende demonstrar, neste contexto, é que o princípio da dignidade da pessoa humana assume posição de destaque, servindo como diretriz material para a identificação de direitos implícitos (tanto de cunho defensivo como prestacional) e, de modo especial, sediados em outras partes da Constituição. Cuida-se, em verdade, de critério basilar, mas não exclusivo, já que em diversos casos outros referenciais podem ser utilizados (...). Assim, o fato é que – e isto temos por certo – sempre que se puder detectar, mesmo para além de outros critérios que possam incidir na espécie, estamos diante de uma posição jurídica diretamente embasada e relacionada (no sentido de essencial à sua proteção) à dignidade da pessoa, inequivocamente estaremos diante de uma norma de direito fundamental, sem desconsiderar a evidência de que tal tarefa não prescinde do acurado exame de cada caso. [67]

Para arrematar a problemática sobre o reconhecimento dos direitos fundamentais, lembra-se que tais direitos "têm a ver com a vida, a dignidade, a liberdade, a igualdade e a participação política e, por conseguinte, somente estaremos em presença de um direito fundamental quando se possa razoavelmente sustentar que o direito ou instituição serve a algum desses valores"[68].

---

65 SARLET, Ingo Wolfgang. **Dignidade da pessoa humana e direitos fundamentais na Constituição Federal de 1988**. 6 ed. rev. atual Porto Alegre: Livraria do Advogado, 2008, p. 103

66 Para o Prof. Dr. Ingo Wolfgang Sarlet "não se poderá dispensar um exame acurado no sentido de que sejam guindadas à condição de direitos fundamentais (...) apenas posições jurídicas implícita ou expressamente consagradas que efetivamente sejam de tal sorte relevantes no que diz com seu conteúdo e significado, a ponto de merecerem o *status* de direitos fundamentais, em sentido material e formal, ou mesmo apenas material, quando for o caso". In: SARLET, Ingo Wolfgang. **Dignidade da pessoa humana e direitos fundamentais na Constituição Federal de 1988**. 6 ed. rev. atual Porto Alegre: Livraria do Advogado, 2008, p. 104.

67 SARLET, Ingo Wolfgang. **Dignidade da pessoa humana e direitos fundamentais na Constituição Federal de 1988**. 6 ed. rev. atual Porto Alegre: Livraria do Advogado, 2008, p. 105.

68 SANCHIS, Pietro, 1994 *apud* MENDES, Gilmar Ferreira; COELHO, Inocêncio Mártires; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional**. 4. ed. rev. e atual. São Paulo: Saraiva, 2009, p. 271.

2 CRIMES ELETRÔNICOS

Os crimes informáticos, ou eletrônicos, não são um fenômeno recente, diferente do que se pensa. Apenas tem atraído a atenção da mídia com maior maestria nos dias atuais, em direta decorrência do avanço alcançado pela sociedade da informação.

Os primeiros crimes eletrônicos conhecidos datam dos idos dos anos de 1960, onde algumas práticas que poderiam ser enquadradas como estelionato ocorreram. Os primeiros trabalhos acadêmicos, ainda, datam da década de 1970, onde alguns dos cenários que hoje discutimos já eram alvos de argumentação. Vários crimes aconteceram nos anos de 1980, sistemas inteiros de bancos, controles de tráfego aéreo, pagamento, prisionais, foram acessados indevidamente e alterados, causando diversos danos nos mais diferentes países. Já nessa época, os prejuízos financeiros contabilizados alcançavam a casa dos milhões[69]. O diferencial maior se encontra no fato que esses anos podem ser considerados os românticos da criminalidade informática, pois foi nesse período que a figura do ofensor que se encontra recluso em uma pequena sala escura e prática atos apenas em proveito próprio foi concebida. Atualmente, organizações criminosas transnacionais dominam o ambiente onde esses delitos acontecem.

Nossa legislação atual, apesar de nos encontrarmos duas décadas após o período romântico dos cibercrimes, ainda não alcançou o passo com que estes evoluem, existindo ainda algumas práticas que não encontram respaldo legislativo. Todavia, a maioria delas já pode se enquadrada em tipos penais presentes em nosso ordenamento jurídico. E diversos projetos de lei que alteram o código penal ou sugerem leis diversas estão em tramitação no Congresso Nacional, inclusive emendas constitucionais que tratam sobre matérias afins.

2.1 Conceito de crime informático

Conceituar crimes eletrônicos é um ato perigoso em si. Qualquer definição muito extensa pode englobar práticas que por mais que sejam consideradas indevidas não podem ser tipificadas como

[69] ALBUQUERQUE, Roberto Chancon de. **A criminalidade informática**. São Paulo: Editora Juarez de Oliveira, 2006, p. 35-38.

crimes, em face do princípio da estrita legalidade penal. Ser muito específico também pode engessar ou tornar ineficiente qualquer medida, em face da velocidade com que ocorrem modificações tecnológicas. Algumas conceituações já foram propostas, mas nenhuma delas sem falhas, como há de ser qualquer atividade humana, eminentemente a legislativa.

A Convenção Européia para Cibercrimes funciona como uma lei modelo que deve ser recepcionada pelos Estados signatários com o fim de funcionar de norte para a produção normativa. Seu corpo normativo impõe algumas definições que podem ser empregadas na elaboração de leis no âmbito da matéria.

Destarte a falta de definição específica, existem algumas tentativas de classificação. A mais adotada divide os crimes eletrônicos em puros e impuros. Aqueles corresponderiam aos em que os dados e os sistemas informáticos constituem o objeto do delito. O segundo seria aqueles em que os meios eletrônicos funcionam como ambiente para a prática de delito em que o objeto jurídico tutelado já encontra respaldo legislativo em um tipo penal comum. Nessa classificação poderíamos encontrar separadas várias provisões normativas atuais, sem que houvesse um caráter absoluto em nenhuma delas. Outra classificação divide-os em duas espécies, as comuns e as específicas. Naquela, os meios informáticos são utilizados para praticar condutas que já são consideradas crime pelo direito penal vigente. A conduta ilícita em si já é objeto de punição. Nos crimes eletrônicos específicos seriam enquadradas as situações que ainda não tem seus objetos jurídicos tutelados, como o mero acesso indevido a um sistema computacional sem que haja um dano decorrente desse ato ou o desenvolvimento de um vírus informático.

Por muito tempo o presente autor adotou a primeira classificação, mas no entorno desse trabalho mudou seu posicionamento, inclinando-se para a segunda, sem, ainda, tornar definitiva sua posição. Todavia, será esta a adotada por hora, com base na idéia de uma classificação que aborde todas as condutas ainda não previstas pode ter mais peso para que estas sejam objeto de um projeto de lei por parte de nossos representantes – ou de um projeto que aborde o conceito de democracia direta através da internet.

2.2 Características dos crimes informáticos

Uma das principais características dos delitos eletrônicos é a volatilidade da materialidade desses atos. Por não se tratarem de dados estáticos ou que se encontram em lugar só, estes podem ser facilmente apagados ou alterados, mesmo sem intenção. O ligar de

computador pode modificar por completo um registro que fundamental para a identificação da autoria de um crime, assim também como a demora na sua perquirição pode levar este a se perder, prática comum entre as empresas provedoras de serviços computacionais, que ainda não encontram uma provisão legislativa específica sobre o tema e alegam altos custos para não armazenarem registros de acesso por um longo período. Apesar de quase sempre ser possível resgatar registros, mesmo quando estes foram intencionalmente deslocados, a maioria das investigações é interrompida pelo não fornecimento ou averiguação de informações hábeis a delimitar a materialidade e a autoria de um delito.

Outra característica notória dos crimes informáticos é que estes são não conhecem fronteiras. Ou seja, não estão limitados a uma determinada região geográfica para acontecerem. Seus autores podem estar em um país, o objeto tutelado pode estar em outro e o resultado ser produzido em outro. Essa natureza causa reverberações interessantes no âmbito jurídico, visto ser necessário determinar a jurisdição competente para poder tratar o delito de forma adequada. Todavia, o real fator complicador decorrente está no procedimento investigatório, posto que a extensão sem fronteiras carrega em si a necessidade premente de cooperação entre o corpo policial e jurídico de, por vezes, diversos países, cenário que pode encontrar barreiras burocráticas instransponíveis que inviabilizam qualquer condenação, em face, como mencionando, da volatilidade da prova informática, exaurindo-se por completos os indícios que poderiam levar a responsabilização do agente.

De forma natural, a maioria dos delitos reclama um tempo no espaço que pode ser reconstituído e delimitado. Já os crimes eletrônicos funcionam de forma distinta. Estes podem acontecer em frações de segundos ou por horas seguidas. Uma invasão e a modificação de um sistema informático pode acontecer em um piscar de olhos enquanto que um ataque distribuído de negação de serviço pode levar horas, quiçá dias, recebendo a denominação de crime continuado, até mesmo de dano, pois pode levar a corruptela total de uma estrutura que sustenta o sistema financeiros de um país, por exemplo. Todavia, a velocidade diferenciada pode ser insignificante caso não sejam tomadas as medidas preventivas e repressivas adequadas.

Evitar que crimes informáticos venham a acontecer é matéria que será discutida em tópico específico, mas que merece alguns pormenores no presente momento. Muito se costuma falar da necessidade de atuação individual, do usuário, para proteger seus

computadores, utilizando *softwares* como antivírus ou *firewalls*, e adotando práticas diligentes como desconfiar de comunicações oriundas de remetentes desconhecidos ou de páginas na Internet que estejam classificadas como desconhecidas. Todavia, a sofisticação alcançada pelas modalidades delituosas faz com que todas essas medidas anteriores possam não ser suficientes para evitar maiores danos. Cooperação é a palavra chave e que merece destaque em todos os pontos do presente trabalho. Seja ela sob a alcunha de um ambiente colaborativo ou na acepção literal da palavra. Caso não sejam implementadas medidas cooperativas entre a iniciativa privadas, os órgãos públicos, os usuários comuns e os diversos setores da sociedade, tudo aqui discutido será em vão e os cenários catastróficos poderão ser lugar comum, como já o são em diversas jurisdições e ambientes corporativos. Mais será discutido sobre cooperação em capítulos subseqüentes.

"A internet é um mar sem lei", expressão proferida por diversos profissionais ou pessoas desconhecedoras do intricado palco em que atuam os crimes eletrônicos. Tem origem na aparente dificuldade encontrada para punir ofensores informáticos. E essa imagem errônea também contribui para a proliferação de aventureiros que navegam com intenções maliciosas. Entretanto, a realidade é bem diferente. É muito mais difícil no ambiente virtual não deixar vestígios que podem contribuir para a identificação do agente do que em crimes que acontecem apenas em ambientes reais[70]. A questão da volatilidade da prova já foi aqui discutida. Mas para não deixar nenhuma trilha que leve ao responsável é necessária uma ingerência técnica não compartilhada pela grande maioria dos criminosos virtuais. Mais uma vez, a época romântica dos crimes eletrônicos já passou. Hoje, para se praticar esses delitos não é preciso conhecimento avançado sobre ambientes computacionais. Kits estão à venda a preços módicos em páginas especializadas. Alugar artefatos maliciosos é mais fácil do que adquirir uma música em uma empresa de e-commerce. Portanto, identificar a autoria de um crime informático é plenamente possível e lugar comum. Punir, todavia, ainda é algo dificultoso, pois encontra barreira na legislação branda e inespecífica.

[70] Mais uma vez, frisamos, adotamos a posição de Pierre Levy que não existe diferença entre o real e o virtual.

2.3 Lugar do crime informático

O crime eletrônico não tem lugar, fronteira ou bordas. Pode acontecer em um lugar só ou em vários ao mesmo tempo. Uma conexão pode estar sendo mantida por servidores situados em diversos países. A transmissão de dados pode se originar de uma cidade qualquer e passar pelos maiores conglomerados computacionais do mundo em uma questão de fragmentos de segundos. A natureza fragmentada inerente a Internet possibilita esse cenário mágico e dificultoso. Ferramentas como *proxies*[71] desviam o fluxo informacional e sistemas TOR e Peer-to-Peer[72] fragmentam não só a conexão, mas a própria informação em si. Ela pode, assim, ter tido origem em vários lugares, ter sido enviada para destinos diversos até atingir o seu destinatário final, que mesmo assim pode estar em locais distintos ao mesmo tempo (a redundância de palavras e expressões é proposital). Na concepção clássica de um crime, vários seriam os autores, vários seriam os locais do crime e vários seriam os locais onde o resultado foi produzido. Fica por terra a questão da definição de competência e jurisdição para investigar e processar o delito.

Nessa esteira, a determinação do local do crime e a aplicação do princípio da extraterritorialidade podem encontrar percalços. Vários países e autores tendem a aplicar a teoria da ubiqüidade, ou seja, a competência seria determinada pelo local onde qualquer fase do crime ocorreu, sendo o ato fracionado considerado como um todo. O Brasil adota essa teoria em nosso código penal, principalmente ao discorrer sobre delitos que não aconteceram em território nacional. Todavia, se esta for adotada, vários países podem se considerar competentes para julgar um crime eletrônico. Para a teoria do resultado, o local do crime é aquele onde o resultado foi produzido, onde as conseqüências e os efeitos dos delitos se manifestaram. Mas como vimos, essas manifestações podem, também, ser identificadas em vários locais, possivelmente em países diversos, ao mesmo tempo, nos levando de volta ao questionamento inicial.

Exemplo dado pelo por ALBUQUERQUE[73] demonstra claramente a dúvida acima exposta. Um e-mail contendo um artefato malicioso pode ser enviado de um determinado país

[71] Ferramenta utilizada para controlar o tráfego de informações.
[72] Protocolos de fragmentação de informações que agregam fontes para aumentar a velocidade de transmissão destas.
[73] ALBUQUERQUE, op. cit., p. 66.

para vários destinatários, que irão executá-los em locais diferentes, causando danos (resultados) em vários países. Atos foram praticados em locais diversos com resultados que puderam ser percebidos em jurisdições diferentes.

Em suma, não existem critérios seguros para determinar em que medida o local da prática de um crime ou o local em que um crime se consuma deve ser considerado o local do crime. Várias teorias são adotadas por vários países, de forma diferente, e cada um tem competência para determinar se tem ou não autoridade para processar o delito em seu território. Tratados internacionais podem discorrer sobre a matéria, em nível de cooperação, para que os delitos sejam tratados onde o dano resultante for maior, ou onde possa ser encontrado melhores condições de investigação, para então colher as provas de forma mais adequada e fornecê-las para que as demais jurisdições tomem as medidas que por ventura entenderem necessárias. Assim entende o art. 22 da Convenção Européia para Cibercrimes:

> Art. 22. Jurisdiction: parag. 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 determing the most appropriate jurisdiction for prosecution

A posição defendida no presente trabalho é o da cooperação a nível nacional e internacional e esta prevalece nesse ponto. Caso haja conflito de jurisdição causado pela natureza fragmentária e transnacional dos crimes eletrônicos, esta deve ser suprida por acordos de cooperação e auxílio mútuo entre os países.

`2.4 O Ecossistema dos Crimes Eletrônicos

Muitas pessoas consideram vírus de computadores uma nuance, e enquanto estão cientes das ameaças, acreditam que estão protegidas do número cada vez maior de ataques na forma de *phishing*, forma fraudulenta de tentar adquirir informações sensíveis como nomes de *logins*, senhas e dados creditícios; *pharming*, ou seja, o redirecionamento do tráfego de páginas na internet para outro sítio virtual falso; *worms* e *trojans*, programas maliciosos; *bots*,

coleção de computadores infectados por programas maliciosos; e ataques de negação de serviço (DDoS).

Todavia, a maioria das pessoas não devem subestimar a tenacidade dos responsáveis por tais ataques, e falham em levá-los a sério o suficiente. O fato é: cibercrimes é um negócio extremamente lucrativo, não apenas para os programadores de vírus ou de páginas maliciosas, mas para todas as pessoas que fazem parte da cadeia, que inclusive já ultrapassou o tráfico de drogas em volume de dinheiro oriundo dessas atividades criminosas, fato mencionado no primeiro capítulo. Cibercrimes se tornaram uma indústria impulsionada pelo dinheiro e por intenções maliciosas, e as pessoas necessitam ter consciência das motivações dos criminosos que se aproveitam da falta de conhecimento e manipulam vulnerabilidades no ciberespaço para auferir lucro.

Os usuários finais apenas veem partes dos crimes eletrônicos, e não estão conscientes do que se passa pro trás das cenas dos ataques. O ciclo se inicia com os coletores, cujo trabalho é literalmente coletar endereços eletrônicos (e-mail), que são repassados para terceiros. Isso pode acontecer através de uma infinidade de métodos, entre os quais o de confirmação de e-mails supostamente verdadeiros que são enviados aos usuários. Outro é a coleta robótica, que utiliza programa que selecionam de maneira aleatória companhias ou organizações e constroem bancos de dados de primeiros e segundos nomes, que são alocados em endereços eletrônicos até que recebam confirmação de resposta. Uma vez que a confirmação é feita, o banco de dados está construído.

Esses bancos de dados são então vendidos para o próximo elo da corrente, que paga em valores que variam entre $25,00 até $45,00 por blocos de 1.000 nomes[74]. Esses bancos são vendidos em blocos de milhares e para vários compradores diferentes, resultando em uma atividade muita lucrativa para quem a exerce. Os compradores desses bancos de dados são pagos por programadores de vírus para enviar e-mails contendo seus arquivos maliciosos, como *trojans* e *worms*, que não só enviam informações sigilosas, como também transformam os computadores em máquinas controladas por terceiros, criando as redes zumbis.

[74] Disponível em:< http://www.pcworld.com/businesscenter/article/194843/15_million_stolen_facebook_ids_up_for_sale.html>. Acesso em: 28 jul 2010.

As redes zumbis são massas de computadores controlados por terceiros. Programadores de programas podem contratar essas redes zumbis e utilizarem as máquinas infectadas para enviar quantidades massivas de e-mails que não são filtrados pelos provedores de internet, por terem se originado de fontes diferentes. Redes zumbis podem ser usadas para um fim ainda mais sinistro. Sítios virtuais completos ou servidores podem ser forçados a ser desligados ou ficarem inacessíveis devido a milhares de acessos simultâneos ordenados pelos controladores das redes zumbis, que sobrecarregam as conexões, que não suportam a quantidade de acessos. Sistemas de proteção não detectam facilmente esses ataques pelo fato deles se originarem de várias fontes diferentes.

O aumento dos crimes eletrônicos na última década é um caso econômico de indivíduos respondendo a incentivos monetários e psicológicos. Dois motivos principais podem ser identificados: a) os ganhos potenciais de ataques cibernéticos estão aumentando com o crescimento da importância da Internet; b) os riscos dos responsáveis pelos delitos serem penalizados é pequeno comparado com crimes tradicionais. Em resumo, crimes eletrônicos são mais convenientes e lucrativos, mais baratos de serem executados e menos arriscados do que ilícitos que não utilizam a Internet como meio ou fim. O aumento na atividade de ilícitos digitais, em conjunto com legislações e aparato policial por vezes ineficiente representam desafios críticos para a manutenção da segurança e da confiança nas infraestruturas computacionais.

Ataques modernos englobam um grande espectro de atividades econômicas, onde vários malfeitores se especializam no desenvolvimento de bens específicos (*exploits*, *botnets*, *mailers*) e serviços (distribuição de artefatos maliciosos, monetização de credenciais furtadas, provedores de hospedagem na internet etc). Uma fraude típica na Internet envolve ações de vários desses indivíduos, como desenvolvedores de vírus eletrônicos, coletores de redes zumbis, *spammers* e pessoas responsáveis por lavar o dinheiro envolvido. Analisar o relacionamento entre esses indivíduos é uma peça essencial para discutir as propostas econômicas, técnicas e legais necessárias para entender os crimes eletrônicos.

Ataques cibernéticos podem ser implementados das mais diferentes formas e a sua capacidade de lucro irá depender frequentemente do alvo dos ataques. Para entender como os papeis desempenhados pelos criminosos cibernéticos é necessário descrever o funcionamento da infraestrutura e das operações que estes desempenham. Ao mesmo tempo em que é

possível uma única pessoa executar a maioria desses papeis, é muito mais provável que estes sejam divididos entre várias entidades com especialidades diferentes.

2.4.1 Pesquisadores de vulnerabilidades e desenvolvedores de ferramentas de exploração

Explorar vulnerabilidades de softwares para obter controle de múltiplos computadores é um passo fundamental em empreitadas criminosas de grande monta. Descobrir essas vulnerabilidades e desenvolver programas de computador que as explorem é um dos aspectos mais difíceis dos ataques cibernéticos, quando comparado com outras funções desempenhadas no âmbito dos crimes eletrônicos. Portanto, se transformou em uma tarefa especializada.

Enquanto criminosos avançados podem escrever os seus próprios códigos, a maioria dos malfeitores utiliza ferramentas de terceiros produzidas para comprometer máquinas. Alguns desenvolvedores de software inclusive prestam serviço de assistência e tomam medidas para que seus softwares não sejam alvos de malferimento a direitos intelectuais. Outras ferramentas são desenvolvidas e utilizadas pro grupos criminosos fechados que podem considerar que vendê-las poderia prover vantagens competitivas para os demais.

Em adição, um pesquisador pode simplesmente vender informações sobre vulnerabilidades, permitindo que terceiros escrevam seus próprios programas[75] de exploração. Essa situação acontece com mais freqüência quando este indivíduo não tem ligações fortes com organizações criminosas. O lucro que pode ser gerado através da exploração de uma vulnerabilidade é uma combinação do tamanho da base instalada de computadores infectados e o valor de ataque para controlar cada máquina.

[75] WMF exploit sold underground for $4,000. Disponível em:<http://www.eweek.com/c/a/ Security/Researcher-WMF-Exploit-Sold-Underground-for-4000>. Acesso em: 02 mar 2010.

2.4.2 Distribuidores de programas maliciosos

Uma vez que criminosos cibernéticos tenham acesso a ferramentas de exploração, podem achar computadores vulneráveis para atacar. Tradicionalmente, existem dois métodos para encontrar essas máquinas: a) um criminoso pode sondar redes para identificar computadores desprotegidos; ou b) um criminoso pode enviar e-mails *spam* com arquivos maliciosos anexados. Enquanto esses dois métodos encontram computadores vulneráveis que ainda estão infectados, atualmente, a maneira mais comum de comprometer novos computadores é através de *malwares* baseados na *web*. Nesse tipo de ataque, cibercriminosos passam a controlar servidores de hospedagem de páginas de Internet, transformam a página hospedada em uma controlada por *softwares* maliciosos e atraem usuários de computadores vulneráveis a visitarem tal página.

Para atrair os usuários, cibercriminosos utilizam programas parceiros que pagam a outros pelo montante do tráfego de Internet direcionado para o servidor dominado, chamado de técnica *iFrame*[76]. Um método bem popular para direcionar o tráfego para o servidor malicioso é infectando páginas legítimas e adicionando camadas transparentes que apontam para a página controlada pelos programas indevidos. Em adição, cibercriminosos podem convencer desenvolvedores de páginas de Internet a incluírem códigos maliciosos em seus trabalhos, ou eles podem distribuir pequenos programas grátis, como um contador de acessos, que os desenvolvedores podem incorporar as suas próprias páginas. Oitenta por cento dos *sites* detectados como maliciosos pelos sistemas de varredura como programas antivírus e índices de sistemas de procura são negócios legítimos que foram alterados indevidamente para redirecionar tráfego para páginas maliciosas[77].

Alguns criminosos não têm conhecimento, ou não se importam, como os programas são instalados. Todavia, irão pagar outras pessoas para comprometeram seus computadores e instalaram seus *softwares*[78]. Programas de afiliados não são apenas usados para desvio de tráfego. Desenvolvedores de *trojans, scareware,* controles de comando de *botnets,* e muitos outros tipos de *malwares* normalmente pagam uma rede específica de parceiros por cada

[76] HOWARD, Rick. **Cyber Fraud: Tactics Techniques and Procedures**. CRC Press, 2009.
[77] Security filters often flag legit but infected sites. Disponível em:<http://www.pcworld.com/businesscenter/article/144485/security_filters_often_flag_legit_but_infected_sites.html>. Acesso em: 10 mar 2010.
[78] Web fraud 2.0: Franchising cyber crime. Disponível em:< http://voices.washingtonpost.com/securityfix/2009/06/web_fraud_20_franchising_cyber.html>. Acesso em: 02 jun 2010.

instalação de seus programas. Essas parcerias têm sido bem sucedidas na instalação de *scarewares*, programas que bombardeiam as vítimas com avisos falsos, indicando que seus computadores estão infectados com *malwares* e impõe ao usuário o pagamento de licençsa para o uso do programa corretor. As comissões para os afiliados por vendas completas dos computadores de uma rede variam entre cinqüenta e noventa por cento[79].

Em outra situação, cibercriminosos podem não querer controlar as máquinas após infectá-las, para então poder vendê-las ou alugá-las.

2.4.3 Coletores de redes zumbis

Uma vez que o cibercriminoso explora uma vulnerabilidade, ele ganha controle sobre ela e pode instalar qualquer programa. Um dos primeiros *softwares* que são instalados são os detentores da habilidade de registrar todos os passos dos computadores infectados. Uma rede de computadores comprometidos sob o controle de uma autoridade é chamada de rede zumbi (botnet). Ao controlar a rede zumbi, o cibercriminoso tem vários métodos para monetizar os computadores infectados. Fontes de renda incluem furto de informações privadas, extorsão através de ataques distribuídos de negação de serviço (DDoS), *spamming*, envenenamento de páginas de procura e fraudes através de links maliciosos[80].

Enquanto *spamming*, *phishing* e ataques de negação de serviço (DDoS) podem ser considerados parte do modelo clássico de uma rede zumbi, seus funcionamentos serão descritos com mais detalhes a frente devido ao seu grande uso.

[79] Antiviral “Scareware” Just One More Intruder. Disponível em:<http://www.nytimes.com/2008/10/30/technology/internet/30virus.html?_r=1>. Acesso em: 10 mar 2010.
[80] The economics of botnets. Disponível em:<http://www.viruslist.com/en/analysis?pubid=204792068>. Acesso em: 13 jul 2010.

2.4.4 *Phising* e *Trojans* para furto de identidades

O *phishing* (corruptela dos nomes e-mail e *fishing*, pescar em inglês) iniciou como um método de fraude por e-mail onde o ofensor enviava mensagens eletrônicas aparentemente legítimas contendo links para páginas na internet camufladas na tentativa de obter informações financeiras confidenciais de seus destinatários. Páginas frequentemente camufladas incluíam os serviços PayPal[81], eBay[82] e outras instituições financeiras. Usuários eram enganados ao ponto de fornecerem suas informações confidenciais ao clicar em links nesses e-mails aparentemente oficiais que requeriam a eles que atualizassem seus contatos e informações de acesso ao sistema de Internet Banking. Uma vez que essa informação era fornecida, registrada e armazenadas, as contas dos usuários poderiam ser controladas e movimentadas por terceiros.

Enquanto vários ataques *phising* ainda continuam a atuar dessa maneira[83], outros estão sendo substituídos por *trojans* utilizados para furto de credenciais. Esse tipo de *trojan* utiliza *keyloggers* e *screenloggers* (programas que monitoram os atos do usuário no computador, como o que ele digita e o onde ele clica) instalados nos computadores das vitimas pra coletar informações pessoais. Em adição ao monitoramento passivo, muitos desses *trojans* retiram informações substantivas de suas vitimas. Por exemplo, sempre que a máquina infectada visita um dos domínios de internet especificado no arquivo de configuração do software malicioso (um site de uma instituição financeira, por exemplo), este envia uma requisição a um servidor que fornece um formulário na página de acesso, perguntando ao usuário sobre a informação sensitiva. Esses ataques, denominados de *man-in-the-middle*, ocorrem entre o usuário e a segurança de seu navegador de Internet[84].

Além de informações de bancos e instituições financeiras, esses *trojans* coletam outros subsídios. Alguns permitem que suas centrais de comando e controle distribuam módulos que são injetadas em aplicações populares presentes nos computadores infectados. Essas aplicações incluem painéis de controle, navegadores de internet, softwares de transferência de

---

[81] Serviço de pagamento eletrônico: www.paypal.com
[82] Serviço de leilão eletrônico: www.ebay.com
[83] Examining the impacto f website takedown on phishing. Disponível em:< www.cl.cam.ac.uk/~rnc1/ecrime07.pdf> Acesso em: 30 jul 2010.
[84] GHRING, Philipp. **Concepts against man-in-the-browser attacks**, 2006.

arquivos, clientes de e-mail, mensageiros instantâneos e programas de acesso ao sistema. Após a inserção do módulo, o software malicioso pode monitorar todos os dados que passam pelos programas infectados e podem fazer triagens na busca de informações interessantes, como credenciais para contas eletrônicas de serviços na Internet e senhas de acesso. Uma vez que o *trojan* intercepta informação substancial, a envia para servidores especificados em seus arquivos de configuração[85].

Phishing e *trojans* de furto de identidade estão no centro das atividades de muitos criminosos. Primeiro, para conseguirem instalar seus *trojans* nos computadores, os cibercriminosos precisam de ferramentas de exploração, pagar por programas parceiros (já mencionados) ou comprar redes zumbis de coletores. Eles também precisam pagar provedores de acesso a Internet e registradores de domínios para hospedarem servidores de comando e controle. *Phishers* também precisam utilizar serviços de *spam* para propagandear suas páginas fraudulentas. Finalmente, após as informações terem sido coletadas de usuários insuspeitos, os cibercriminosos precisam vendê-la ou utilizar o serviço de mulas, *cashiers* ou *carders*.

2.4.5 *Spammers*

Enquanto que o *spam* é geralmente associado a e-mails não solicitados (normalmente enviado por uma rede zumbi), ele também pode ser utilizado como ferramenta de vários métodos pelos quais os cibercriminosos contatam seus usuários. O alvo primário do *spam* é convencer os usuários a visitarem páginas específicas na internet, normalmente utilizadas para distribuir *softwares* maliciosos, *phishing*, ou para a venda de mercadores de qualidade ou propriedade não reconhecida. *Spam* também é utilizado para recrutar mulas que serão utilizadas para lavar dinheiro, ou para iniciar uma conversa com fraudadores.

Existe uma grande variedade de ferramentas que os fraudadores podem utilizar para enviar *spam*. A sofisticação desses programas é tamanha que alguns fazem o *download* em servidores de modelos de mensagens e listas atualizadas de destinatários, geradas independentemente e ao final reportam seus resultados ao servidor original. Adicionalmente, podem criar mensagens indistinguíveis

[85] STONE-GROSS, Bret. **Your botnet is my botnet: Analysis of a botnet takeover. Technical Report.** Santa Barbara: University of California, 2009.

das de algums de clientes populares de e-mail, automaticamente gerando e ofuscando imagens, além de por vezes estarem configuradas para executar rotinas previamente programadas.

2.4.6 Ataques de negação distribuída de serviços (DDoS)[86]

Em um ataque de negação distribuída de serviços, o responsável por uma rede zumbi envia comando ordenando os "zumbis" (computadores infectados) a inundarem um alvo com um alto volume de tráfego de internet, essencialmente bloqueando qualquer outro acesso da Internet para a vítima. Como será demonstrado a frente, ataques DDoS frequentemente são usados para expressar certas posições políticas, como os ataques recentes as infraestruturas criticas da Estônia e da Geórgia, ou para danificar adversários nos negócios, tirando da Internet seus sistemas, impossibilitando acessos externos a eles. Todavia, a causa mais comum para o uso de DDoS é a chantagem. Em alguns casos, controladores de redes zumbis apenas lançam um pequeno ataque de negação de serviço e requisita uma quantia de dinheiro para não tirarem do ar o servidor, a página de internet ou negócio alvo. Ou ainda, demandam o pagamento antes mesmo de iniciar o ataque. Alvos comuns são serviços na Internet que necessitam estar sempre acessíveis a seus usuários e que se encontram em locais onde a jurisdição com relação à Internet não é muito desenvolvida ou aplicada[87].

2.4.7 Registradores de domínios intocáveis

A infraestrutura de tecnologia da informação, para realizar as maiores campanhas criminosas, depende da possibilidade das vitimas poderem acessar os servidores utilizados para executar os atos ilícitos, como páginas na Internet distribuidores de *softwares* maliciosos,

[86] "Com o desenvolvimento da rede mundial de computadores e o aperfeiçoamento dos conhecimentos tecnológicos dos *hackers*, os ataques DDoS (*Distributed Denial of Service*) tornaram-se mais freqüentes na Internet. Os ataques DDoS, mais conhecidos como ataques de negação de serviços distribuídos consistem basicamente em impedir o normal funcionamento de determinados serviços na Internet, evitando que usuários legítimos acessem aquele sistema." PINHEIRO. Reginaldo César. *Os Ataques DDoS e os Seus Reflexos no Direito, in Internet Legal – O Direito na Tecnologia da Informação.* Organizador: KAMINSKI, Omar. Ed. Juruá, Curitiba, 2003, p. 165.

[87] Online casinos will experience cyber-extortion during SuperBowl betting. Disponível em:<http://www. ibls.com/internet_law_news_portal_view.aspx?id=1967&s=latestnews>. Acesso em: 25 jan 2010.

servidores para receberem as informações oriundas de *trojans*, servidores de controle e comando de redes zumbis, páginas para *phishing*. Esses servidores podem ser localizados na Internet através de nomes de domínio (*DNS Servers*), e através do contato com servidores de Internet que hospedam esses computadores.

Um profissional de segurança da informação tentando retirar do ar servidores que supostamente estão sendo utilizados para realizar atividades criminosas normalmente entra em contato com provedores de serviço de Internet e registradores de nomes de domínio associadas com esses servidores. Entretanto, remover esses computadores da Internet não é sempre uma tarefa fácil, pois algumas redes zumbis, por exemplo, utilizam vários provedores de acesso a Internet e vários nomes de domínio[88]. Para proceder com a retirada, seria necessário atuar em todas as frontes e ser efetivo nelas. E na maioria dos casos, elas se encontram em países diferentes, com políticas de atuação diversas e que normalmente não colaboram em matérias dessa natureza. Alguns provedores de internet simplesmente não retiram seus servidores do ar, mesmo que seja evidentemente provado que estes estão sendo utilizados para executar atividades maliciosas. Os que agem dessa maneira são os mais utilizados para hospedarem os servidores indevidos[89].

Registradores de domínios intocáveis são um problema persistente. Por exemplo, a ICANN[90] envia várias notificações para esses registradores, em decorrência de reclamações. Todavia, mesmo se a ICANN rescindir a licença de registradores de domínios de alto nível[91] (*top-level domains* - gTLD), todo país tem absoluto controle sobre seus domínios de alto nível[92] (*country-code top-level domains* - ccTLD). Para que seja possível agir de forma efetiva sobre ccTLD maliciosos, melhores procedimentos internacionais são necessários.

[88] Killing the beast ... part II. Disponível em:<http://blog.fireeye.com/research/2009/06/ killing-the-beastpart-ii.html>. Acesso em: 17 jun 2010.
[89] ANDERSON, David.**The aggregate burden of crime**. Journal of Law and Economics, XLI. 1999, p. 611–642.

[90] Organização responsável pela Internet mundial: www.icann.org
[91] Domínios de alto nível são aqueles utilizados primariamente atribuídos aos países ou as instituições, como .com e .gov.
[92] Domínios de alto nível atribuídos aos países individualmente, como o .br.

2.4.8 Provedores de acessos a Internet e de hospedagem intocáveis

Quando um servidor é utilizado para enviar *spam* ou para espalhar *softwares* maliciosos, especialistas de segurança normalmente reportam ao provedor de acesso a Internet, que podem, então, removê-lo da Internet. Servidores protegidos (*bulletproof servers*) fazem parte de uma modalidade de serviços fornecidos por provedores de acesso a Internet que simplesmente ignoram essas requisições de retirada[93]. Além de servidores protegidos, existem outros contratos especiais entre criminosos e provedores de acesso a Internet intocáveis. Uma versão em particular dessas negociações exime os contratantes das cláusulas que proíbem o envio de *spam*. Essas benesses são garantidas a preços bem maiores, que são cobrados dos que irão utilizar esses serviços diferenciados.

A "*Russian Business Network* (RBN)" é uma das organizações mais conhecidas que proviam serviços especiais de hospedagem para interessados. Previamente baseada em São Petersburgo, com a exceção de pedofilia[94], tinha por alvos primários instituições financeiras e seus correntistas. Devido ao fato da RBN raramente atingir vitimas fora do território russo, as agências de segurança locais foram compelidas a atuar, mas ao final a organização foi desbaratada sem que nenhuma pessoa fosse responsabilizada pelos atos ilícitos[95].

Existem diversos provedores de acesso a Internet e de hospedagem que funcionam como portos seguros para atividades de cibercriminosos. Enquanto houver quem esteja disposto a pagar valores superiores por esses serviços diferenciados, irá existir quem os forneça, caso não haja medidas coercitivas efetivas[96].

---

[93] In china, $700 puts a spammer in business. Disponível em:<http://www.computerworld.com.au/article/302617/china_700_puts_spammer_business>. Acesso em: 11 maio 2010.
[94] Russian business network study. Disponível em:< http://www.bizeul.org/files/RBN_study.pdf>. Acesso em: 10 mar 2010.
[95] Op. cit. HOWARD, Rick.
[96] Bad, bad, cybercrime-friendly ISPs. Disponível em:<http://blogs.zdnet.com/security/?p=2764>. Acesso em: 4 mar 2010.

2.4.9 Processadores de pagamento

Registradores de domínio intocáveis e provedores de acesso a Internet e de hospedagem indevidos são parte de um todo maior utilizado por cibercriminosos como infraestrutura, que depois argumentam que estavam provendo serviço a um cliente desconhecido. Outro exemplo dessa infraestutura são os processadores de pagamento que os criminosos eletrônicos precisam para receberem e efetivarem as transações de cartão de crédito dos usuários que compram seus produtos, como *scarewares*. Muitos dessas empresas processadores argumentam que não tinham conhecimento das atividades ilícitas de seus clientes[97].

2.4.10 Furto de identidade, receptação e mulas: a monetização de credenciais furtadas

Para que seja possível monetizar informações recolhidas por *trojans, keyloogers,* e *phishings,* cibercriminosos precisam do auxílio de *cashiers, carders,* ladrões de identidade e muitos outros fraudadores profissionais. O furto de identidade é um termo utilizado para descrever várias tipos de fraude diferentes, incluindo variações onde o impostor se mascara como outra pessoa para evitar qualquer punição por um ilícito que realizou. Existem ainda variações como furto de identidade financeira, onde o fraudador abre uma linha de crédito utilizando informações pessoais de outro. Essa nova linha pode incluir desde cartões de crédito até serviços de telefonia celular. Em outra modalidade, o impostor se apropria de uma conta já existente. Por exemplo, os dados de um cartão de crédito podem ser adquiridos e utilizados pelo ofensor sem a autorização do proprietário.

Um grande número de fatores econômicos molda o cenário do furto de identidade. Primeiro, trata-se de um crime de baixo risco e lucrativo, mas demanda muito trabalho quando executado em grande escala. Criminosos de pequena escala podem oportunamente utilizar os cartões um do outro, ou fazer comprar em seus próprios cartões, e reportarem as

[97] Following the money: Rogue anti-virus software. Disponível em:< http://voices.washingtonpost.com/securityfix/2009/07/following_the_money_trail_of_r.html>. Acesso em: 15 jul 2010.

empresas processadores que as compras foram feitas indevidamente por terceiros. Operações em larga escala requerem uma cooperação de múltiplos atores e especialidades técnicas.

Em fraudes que envolvem novas contas, os fraudadores tentam obter linhas de crédito. Para iniciar esse procedimento de forma efetiva, estes devem obter credenciais em nome das vitimas, conseguir endereços para envio de correspondência e coleta de cartões de crédito e números de telefone para a ativação dos cartões. Impostores podem criar falsas identidades ou obter credenciais reais junto a órgãos do governo, mas essas duas opções demandam altos custos e são de difícil concretização, em decorrência dos avanços nas tecnologias e medidas antifraude. O criminoso precisa, assim, manter vários endereços de envio de correspondência diferentes, ou então utilizar um esquema conhecido como "furto de identidade sintética", onde nomes bem similares aos das vitimas são utilizados[98], de modo que o proprietário do endereço destino irá aceitar as variações como erros, e não como uma fraude. Uma vez que essa infraestrutura é montada, o fraudador pode efetuar o pedido de crédito ou de outras contas, redirecionando-as para os endereços destino de terceiros.

A monetização criminosa de contas recebe um procedimento similar, com desafios técnicos semelhantes. Um método comum para monetizar contas correntes é com a utilização de *cashiers* e mulas. O *cashier* usa a conta furtada para transferir valores da conta furtada para a conta da mula. A mula, então, transfere uma porcentagem do dinheiro para o *cashier*, normalmente através de uma transferência de difícil rastreamento.

Mulas são frequentemente vitimas de esquemas também[99]. Um método comum de recrutamento de mulas é ter como alvo pessoas desempregadas e a elas são oferecidas vagas como processadores de pagamento ou como compradores de bens para terceiros[100], sem o conhecimento destas do *background* ilícito.

Enquanto a monetização de credenciais furtadas pode ser fácil para um fraudador experiente, ainda é algo complexo quando operada em larga escala. A série de passos envolvidos na extração de valores de bancos e cartões de crédito e a alta probabilidade de

[98] HOOFNAGLE, Chris Jay. **Identity theft: Making the known unknowns known**. Journal of Law and Technology, vol. 21, 2007.
[99] The growing threat to business banking online. Disponível em: <http://voices.washingtonpost.com/securityfix/2009/07/the_pitfalls_of_business_banki.html>. Acesso em: 22 jul 2010.
[100] Russian business network study. Disponível em:< http://www.bizeul.org/files/RBN_study.pdf>. Acesso em: 10 mar 2010.

apreensão enfrentada por estes criminosos explica porque falhas massivas de segurança onde milhares de identidades são vazadas resultam em apenas pequenos casos de furto de identidade. Até mesmo quando informações vazadas envolvem dados pessoais e de cartão de crédito de milhões de indivíduos, a logística necessária funciona como freio para evitar efeitos exponenciais.

2.4.11 Organizações criminosas, terrorismo virtual e guerra virtual

No fim do século 20, todo o mundo estava fascinado e aterrorizado com o "bug do milênio". Devido a uma falha na capacidade de armazenamento dos computadores, a mudança do ano de 1999 para o ano 2000 poderia resultar em falhas nos softwares. Estas poderiam dar inicio a reações em cadeia devido ao fato dos computadores serem responsáveis pelo controle de sistemas públicos, como o fornecimento de energia, de água e telecomunicações. O terror foi tão grande que pessoas chegaram a estocar comida e outros suprimentos para evitar um possível colapso na sociedade. O setor de tecnologia da informação respondeu com uma ação massiva destinada a traçar todos os sistemas que poderiam gerar problemas durante a troca de milênios. Como resultado, nenhum acidente significativo ocorreu.

Fato é que o mundo encontra-se interligado através de tecnologias computacionais de toda a sorte. Combinadas, essas tecnologias e infraestruturas compõem a infraestrutura global de informação, que é primariamente usada para compartilhar informações e dados. Essa infraestrutura funciona como ponte de comunicações entre comunidades, negócios, indústrias, distribuição de bens, serviços médicos, operações militares, como também controle de tráfego aéreo e marítimo.

A infraestrutura de informação sustenta toda a economia e a superioridade militar. Ao mesmo tempo em que facilita a troca de conhecimento e cultura, proporciona conectividade nacional, internacional e global através de uma grande gama de sistemas. A camada de serviços sobrepõe as demais e a transferência de informações suporta a globalização de valores, negócios e culturas, criando um espaço de comunicação menor e altamente acessível aos interesses dos participantes. Tudo isso compõe a rede massiva de servidores conhecida

como internet, gerenciada por milhares de organizações e bilhões de indivíduos. A infraestrutura global de informações é utilizada para melhorar a processos, tornando-os mais eficientes, e comunicações entre os entes que constroem a internet, e assim compartilham e consolidam dados críticos na esperança de manutenção de seus esforços.

Este é o motivo pelo qual tal infraestrutura é tão importante para o estilo de vida moderno. E também porque se torna um alvo viável para aqueles em busca de imposição de suas agendas e esferas de influência no resto da humanidade. Um tipo de grupo que deseja impor suas vontades sobre os demais é o de entidades terroristas. O terrorismo não mais tem se mantido em suas formas tradicionais de violência, já migrando para o uso de tecnologias computacionais e redes para iniciar tais ataques. Como no caso no "bug do milênio", e de exemplos mais recentes, é necessário conscientização entre os profissionais de tecnologia da informação e pessoas do meio que o terrorismo através do uso de computadores e da internet, conhecido como cyber terrorismo, é uma ameaça real.

Atos de terrorismo acontecem desde a antiguidade, quando povos, antes de entrarem em conflitos, agiam em território inimigo para fragilizá-lo. Na história moderna, temos exemplos claros, como os que deram início à primeira guerra mundial, com o assassinato do Arquiduque Francisco Ferdinando, do Império Austro-húngaro.

Podemos conceituar terrorismo como o uso ilícito ou ameaçador de força ou violência por um indivíduo ou um grupo organizado contra pessoas ou propriedades, com a intenção de intimidação ou de coação a sociedades, governos e entidades, por razões políticas e ideológicas.

A mídia de massa reporta diariamente ataques terroristas pelo mundo. Esses ataques podem acontecer a qualquer tempo, em qualquer lugar, em qualquer país. O método de ataque na maioria dos casos é o mesmo: um grupo ou um indivíduo explode um alvo, que pode ser feito remotamente ou através de ataque suicida. Um denominador comum entre esses eventos trágicos é que os atores representam apenas uma pequena porção da sociedade e a maioria das vítimas são inocentes que se encontravam nas proximidades do alvo atacado.

Desde setembro de 2001, com os atentados terroristas ao World Trade Center, e mais uma séria de atentados em grandes metrópoles do mundo ocidental, o mundo vive em uma sociedade do medo. A idéia de que a figura do terrorista que pode estar em qualquer lugar é alardeada pela mídia e incrustada no inconsciente coletivo. Guerras foram iniciadas, grupos

perseguidos e pessoas presas, sem o direito a um devido processo legal ou o acesso a direitos fundamentais. O terrorismo passou a ser objeto de conversa, discussões e estudos em todas as esferas e vimos surgir novas modalidades, como o cyber terrorismo.

Nos mesmos moldes organizacionais, o crime organizado, em uma conceituação básica, é toda organização criada para transcender as regras estatais com o intuito de auferir lucros através do cometimento de ilícitos, perpetrando atividades que vão desde o tráfico de drogas, armas e pessoas até a corrupção ativa e passiva de membros do governo. Diferente de outras atividades, o crime organizado segue um regramento interno rígido e estruturado, com hierarquia e princípios próprios, que devem ser seguidos por todos os seus membros. Assemelha-se a figura de um Estado paralelo ou de uma corporação, muitas vezes provendo a comunidade em que atua o que o Estado legítimo não consegue. A complexidade atingida por esses grupos é tamanha que muitas vezes têm âmbito de atuação internacional, nos moldes da empresas multinacionais, com ramificações em vários países e continentes.

A Academia Nacional de Polícia Federal do Brasil enumera algumas características do crime organizado: 1) planejamento empresarial; 2) antijuridicidade; 3) diversificação de área de atuação; 4) estabilidade dos seus integrantes; 5) cadeia de comando; 6) pluralidade de agentes; 7) compartimentação; 8) códigos de honra; 9) controle territorial; 10) fins lucrativos. [101]

No Brasil, assim como em outros lugares do mundo, a tutela criminal aplicada às organizações criminosas é diferenciada em vários aspectos, recebendo lei própria[102], com institutos únicos, como a possibilidade de delação premiada e o tratamento mais grave dado ao preso em decorrências desses ilícitos. Nesse ínterim, não são poucas as ligações entre grupos terroristas com o crime organizado. Muitas dessas entidades criminosas são fundadas para financiar atos terroristas através de seus ilícitos. Algumas vezes, as próprias organizações criminosas preferem atos de terrorismo. Nos moldes organizacionais, se assemelham quando comparamos entidades terroristas de âmbito internacional, como a Al-Qaeda e o Hamas, que detém, inclusive, poder legítimo dentro de governos nas regiões onde atuam.

Temos visto nos últimos tempos o uso massivo de tecnologias da informação por organizações terroristas. Este fato deu ensejo ao nascimento de uma nova classe de ameaças

[101] Polícia de prevenção e repressão a entorpecentes – Departamento de Polícia Federal, 2001
[102] Lei 10.217/01

que recebeu o nome de “cyber terrorismo”. O terrorismo virtual é o uso calculado de violência ilegal contra qualquer tipo de propriedade digital, para intimidar ou exercer coerção contra governos ou a sociedade, em busca de objetivos políticos, religiosos ou ideológicos. Este novo termo pode ser diferenciado da sua forma tradicional visto que o “terror” físico não ocorre nos mesmos moldes e os esforços são focados para o ataque de sistemas de informação e suas fontes.

Quando observado pela perspectiva de habilidades e técnicas, existe pouca diferença com relação a conceito clássico de “*crackers*”, especialistas em sistemas de informação e em tecnologias que utilizam seus conhecimentos para fins maliciosos. Ambos necessitam e utilizam um arsenal de técnicas para burlar a segurança de sistemas alvos.

Por uma perspectiva motivacional, no entanto, cyber terroristas são claramente diferentes, operando sob uma agenda política e ideológica para apoiar seus atos. Isto pode resultar em esforços mais focados e determinados para atingir certos objetivos e uma escolha mais criteriosa de alvos de ataques. No entanto, a diferença não é apenas esta e outros fatores devem ser levados em consideração. Primeiramente, o fato de cyber terroristas serem parte de um grupo organizado pode significar que eles têm fundos financeiros para patrocinarem suas empreitadas. Isso pode levar a contratação de “*crackers*” ou “*hackers*” para executarem ataques em nome de organizações terroristas, dessa maneira terceirizando a necessidade de *expertise* técnico. Nessa situação, os “*hackers*” são contratados e não precisam acreditar ou serem seguidores da “causa” terrorista, pois irão apenas executar os ataques em troca de retorno financeiro.

Grupos terroristas e partidos políticos agora usam a internet para uma gama variada de propósitos. A título de exemplo, entidades terroristas sempre tiveram dificuldade em repassar suas mensagens e ideologias políticas para o público geral sem que houvesse alguma forma de censura. Agora podem usar a internet para este propósito específico. Em 1997, um grupo terrorista peruano conhecido como MRTA tomou a embaixada japonesa no Peru, fazendo um grande número de reféns. Durante o tempo que estiveram dentro do prédio, o sítio virtual do grupo recebeu notícias dos membros do movimento revolucionário que se encontravam dentro da embaixada, atualizando o mundo dos acontecimentos e revelando o drama com fotos do que acontecia.[103]

[103] http://www.nadir.org/nadir/initiativ/mrta/

Rebeldes chechenos têm usado a internet para combater os Russos em uma guerra de propaganda. Em uma situação, clamavam terem conseguido derrubar um caça militar russo, fato negado pelo governo, até que uma foto dos destroços do jato foi colocada em sua página oficial, levando o governo russo a admitir o evento.

Publicações Azzam, empresa com sede em Londres, que recebeu esse nome em homenagem ao mentor de Osama Bin Laden, é uma página dedicada à guerra santa e ligada a Al Qaeda. Supostamente, essa página, que vendia de livros a filmes relacionado a Jihad, arrecadava fundos para o Taliban no Afeganistão e para guerrilheiros que combatem russos na Chechena. Após os acontecimentos de 11 de setembro, a Azzam foi pressionada ao ponto de não mais vender seus produtos pelo seu site, informando em uma mensagem alternativas aos interessados nas comprar, tudo para assegurar a continuidade no financiamento e no envio de verbas para as causas terroristas. Em 2002, a página principal da Azzam voltou ao ar, oferecendo as mesmas opções de financiamento, produzindo conteúdo em várias línguas para poder se proteger das leis de censura do ocidente[104].

Cyber terroristas empregam o chamado hacktivismo com intuitos ilícitos. Hacktivistas estão frequentemente envolvidos em *defacing*[105] de páginas de inimigos políticos ou com idéias contrastantes as defendidas pelos grupos que representam.

A emergência do cyber terrorismo significa que um novo grupo de potenciais atores (*non-state actors*) que utilizam computadores e tecnologia de telecomunicações podem ser adicionados ao conceito tradicional de "cyber criminosos" e já atuam efetivamente no mundo. Todavia, este novo grupo executa seus ilícitos não somente por motivos econômicos, mas ideológicos e políticos na maioria das vezes e seus atos podem gerar conseqüências muito mais drásticas do que os atos tradicionais de terrorismo. Enquanto o terrorismo tradicional detém uma limitação geográfica de onde os danos são causados, como no caso de uma explosão o local onde esta ocorreu, o cyber terrorismo pode atingir proporções nacionais e internacionais.

Estes atos podem ser interpretados como atos de guerra caso a responsabilidade por eles seja atribuída a um Estado ou a uma entidade específica, no que poderia ser enquadrado nos moldes do conceito de "guerra virtual". Todavia, até o presente momento, não existe um

[104] http://www.azzam.com/
[105] Ato de alterar deliberadamente e sem permissão a página virtual de uma entidade, organização ou indivíduo.

acordo internacional sobre o que constitui um ato de guerra virtual, todavia, várias fontes informam que mais de 120[106] países estão utilizando a Internet para fins políticos, militares econômicos e de espionagem. Segundo a Agência Nacional de Segurança americana, guerra virtual seria:

> [T]he employment of Computer Network Operations (CNO) with the intent of denying adversaries the effective use of their computers, information systems, and networks, while ensuring the effective use of our own computers, information systems, and net-works. These operations include Computer Network Attack (CNA), Computer Network Exploitation (CNE), and Computer Network Defense (CND).[107]

Todavia, devido às características particulares do ciberespaço, principalmente a sua natureza sem fronteiras, existe uma dificuldade para identificar ataques e agressores; o intervalo entre os ataques e suas detecções é imprescindível para sua apuração; a natureza das conseqüências dos ataques é imprevisível e pode vir a ser calamitosa; existe uma multiplicidade de potencias ataques, com as mais diversas motivações; a contestabilidade de eventuais respostas pode ter embasamento dúbio. Devido a isso, uma política geral baseada na retaliação e dissuasão que demonstre punições severas em resposta a um tipo particular de ataque pode não ser suficiente para deter ataques cibernéticos e, em algumas circunstâncias, poderá vir a ser contra produtivo, pois podem reverberar para além dos limites geográficos de um país.

2.4.12 Eventos

Atos de cyber terrorismo e de guerra virtual são uma realidade, e não algo com que precisamos nos preocupar em um futuro próximo. Podemos mencionar vários casos recentes. Em 2003, antes da invasão norte-americana do Iraque, um ataque cibernético as instituições financeiras desse país foi planejado e estava pronto para ser colocado em ação Não o foi

[106] McAfee's 2008 Virtual Criminology Report. Disponível em: < http://resources.mcafee.com/content/NAMcAfeeCriminologyReport>. Acesso em: 12 jan 2010.
[107] Disponível em: <http://www.counterterror.net/DOD36001.pdf>. Acesso em 25 jul 2010.

devido ao receio que este ultrapassasse as fronteiras do país, causando reverberações que poderiam atingir conglomerados bancários com correntistas interessados na guerra[108].

Em agosto de 2006, Israel desmantelou o sistema de defesa aéreo Sírio pela internet, durante o bombardeio a um suposto centro nuclear sírio, causando efeitos colaterais a sua rede doméstica.

Em maio de 2007, a Estônia sofreu uma série de ataques de negação de serviço. O sistema financeiro ficou paralisado por dias. O suposto motivo seria a retirada de uma estátua russa proveniente da época da União Soviética. A gravidade foi tamanha que uma nova organização internacional foi criada com o objetivo maior de combater esse tipo de criminalidade. Ligada a OTAN, O Centro de Excelência de Defesa Cibernética Cooperativa (Cooperative Cyber Defense Centre of Excellence - CCDCOE) hoje detém a competência para investigar, evitar e reprimir atos que podem ser classificados como de guerra virtual dentro do âmbito de atuação da Organização do Tratado do Atlântico Norte.

Em janeiro de 2008, um agente da CIA informa em relatório que o governo americano tem conhecimento de pelo menos 04 cidades no mundo que tiveram seu sistema elétrico atingido por ataques cibernéticos. Todavia, mais de 170 casos de incidentes de segurança da informação em *smart grids* já foram reportados, inclusive com a detecção de softwares espiões[109]. Além desse fato, o próprio exército americano já demonstrou que estruturas que utilizam os sistemas SCADA[110] podem parar de funcionar caso estejam conectados a internet e venham a ser alvos de ataques[111]. Hoje, quase todas as infraestruturas críticas de uma nação utilizam sistemas SCADAS para o seu gerenciamento.

Em junho de 2008, centenas de computadores de escritórios tibetanos foram invadidos por estrangeiros que buscavam informações sobre os movimentos de libertação e os seus responsáveis. Em agosto do mesmo ano, Rússia lançou uma operação militar contra a

---

[108] MONTEIRO, Renato Leite; SANTOS, Coriolano. **Estruturas críticas: o próximo alvo**. Disponível em: < http://www2.oabsp.org.br/asp/comissoes/crimes_eletronicos/noticias/proximo_alvo.pdf>. Acesso em: 10 dez 2009.

[109] Stuxnet renews power grid security concerns. Disponível em: < http://www.computerworld.com/s/article/9179689/Stuxnet_renews_power_grid_security_concerns?taxonomyId=17&pageNumber=2>. Acesso em: 26 jul 2010.

[110] SCADA - Supervisory Control and Data Acquisition. Sistema de gerenciamento utilizado para controlar a redes computacionais de grande escala.

[111] Simulated attack points to vulnerable U.S. power infrastructure. Disponível em:<http://www.computerworld.com/s/article/9039678/Simulated_attack_points_to_vulnerable_U.S._power_infrastructure>. Acesso em: 20 set 2009.

Geórgia, lançando-se na disputa sobre a província da Ossétia do Sul, região fronteiriça de ambos os países. Ao mesmo tempo em que o exército russo adentrava em terreno georgiano, uma opressão cibernética foi iniciada de forma coordenada, atingindo os serviços de comunicação oficial do Governo da Geórgia, impossibilitando que, mesmo durante um conflito armado, informações oficiais fossem veiculadas pelos veículos governamentais. Um site foi criado chamado "StopGeorgia". Nele, o usuário poderia fazer o download de um software e seguir determinadas instruções que levariam a uma torrente de acessos simultâneos aos veículos de comunicação oficial do Governo.

Em janeiro de 2009, durante a ofensiva militar à faixa de Gaza, a infraestrutura de internet Israelense foi atacada por mais de 500.000 computadores, em um trabalho que, segundo o governo israelense, foi executado por membros da antiga União Soviética, a manda do Hamas e do Hezbollah. No mesmo conflito, membros da força de defesa israelense invadiram a rede de TV do Hamas, chamada de Al-Aqsa, e exibiram um desenho animado mostrando a morte de líderes do Hamas com a seguinte legenda: "O tempo está acabando"[112].

Em fevereiro de 2009, computadores do sistema de controle aéreo americano foram invadidos, causando potencial risco a sua malha aérea. No mesmo mês, a cidade de Mumbai na Índia sofreu uma série de ataques terroristas que foram inteiramente coordenados através da internet e pelo uso de telefones que se comunicavam entre através do padrão de Voz pela Internet – VOIP. Em março do mesmo ano, pesquisadores americanos descobrem uma rede de computadores espiões denominada de Ghost Net ou Titan Tains, que eles acreditam pertencer à China e foi implementada em servidores governamentais de mais de 100 países.

Em abril de 2009, uma séria de artigos do Wall Street Journal denunciaram o crescimento na vulnerabilidade a ataques cibernéticos da rede elétrica americana e também revelaram intrusões por estrangeiros desconhecidos aos bancos de dados do projeto do caça americano F-35, roubando dados que ordem dos bilhões de dólares. Em junho, as eleições iranianas sofreram uma série de protestos e atos pela internet, em face da suposta fraude no pleito eleitoral. A internet passou a ser a única fonte de dados, que eram fornecidos pelos próprios usuários através de redes sociais e de ferramentas de microbloging.

[112] Israelis Take Over Hamas' TV Station. Disponível em: <http://www.wired.com/dangerroom/2009/01/israelis-take-o/>. Acesso em: 8 nov 2009.

Em 04 de julho de 2009, enquanto os americanos celebravam o seu feriado mais importante, os sistemas da Casa Branca, Departamento de Defesa, do Serviço Secreto e da Agência de Segurança Nacional, além da Bolsa de Valores de Nova York e a Nasdaq, sofreram ataques continuados de negação de serviço, que os tiraram do ar. Ataques similares aconteceram na Coréia do Sul e suspeita-se de autoria da Coréia do Norte.

Suspeita-se que 03 blecautes ocorridos no Brasil nos anos de 2006, 2007 e 2009 possam ter sido obra de ingerências cibernéticas aos sistemas de controle computacional das redes de geração e transmissão de energia[113]. No último evento, 18 estados ficaram sem energia por horas, atingindo mais de 70 milhões de pessoas. O fato ocorreu dois dias após a veiculação de um documentário em uma rede de televisão americana, quando foi afirmando que os apagões ocorridos no Rio de Janeiro e Espírito Santo, respectivamente em 2006 e 2007, teriam sido ocasionados por invasões cibernéticos. Tal informação já havia sido mencionada pelo Presidente Obama quando do lançamento da CyberSpace Policy Review[114], em abril de 2009.

2.4.13 Formas de combate ao cyberterrorismo

Por ser uma categoria dos crimes eletrônicos, e uma ramificação do terrorismo tradicional, o cyber terrorismo pode ser enfrentado através das mesmas ferramentas utilizadas para combater estes ilícitos. Todavia, por se utilizar de um meio específico, a internet e as infraestruturas de tecnologia da informação, alguns enfoque especializados são necessários para uma maior efetividade.

Vários órgãos internacionais, entre eles a ONU, OEA e OTAN têm fóruns permanentes de discussão e ferramentas específicos para o estudo e a repressão ao cyber terrorismo, como uma novel forma de terrorismo. No âmbito brasileiro, o Gabinete de Segurança Institucional de Segurança da República – GSI/PR é um órgão da Presidência da República que possui várias competências, entre elas a prevenção e o gerenciamento de crises. Possui uma estrutura interna seccionada, com vários órgãos subordinados, entre eles o Departamento de Segurança da Informação e Comunicações – DSIC. O DSIC tem como

[113] Sistemas SCADA.
[114] Disponível em: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

atribuição operacionalizar as atividades de segurança da informação e comunicações na administração pública federal, nos seguintes aspectos: (i) regulamentar a segurança da informação e comunicações para toda a administração pública federal; (ii) ser o ponto de contato junto a OEA para assuntos de terrorismo cibernético; (iii) manter o centro de tratamento e resposta de incidentes na redes de computadores do governo federal.

A portaria número 34 do Conselho de Defesa Nacional[115], de 5 de agosto de 2009 instituiu o Grupo de Trabalho de Segurança das Infraestruturas Críticas da Informação, no âmbito do Comitê Gestor de Segurança da Informação - CGSI. Essa portaria levou em consideração o fato de Infraestruturas Críticas como sendo as instalações, serviços, bens e sistemas que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade. Vislumbrou a necessidade de assegurar dentro do espaço cibernético ações de segurança da informação como fundamentais para garantir disponibilidade, integridade, confidencialidade e autenticidade da informação e comunicações no âmbito da Administração Pública Federal, direta e indireta. Entreviu a possibilidade real de uso dos meios computacionais para ações ofensivas através da penetração nas redes de computadores de alvos estratégicos e o ataque cibernético como sendo uma das maiores ameaças mundiais na atualidade.

Nessa ínterim, a repressão a crimes eletrônicos tradicionais com efetividade, a especialização de delegacias e aperfeiçoamento do judiciário são medidas necessárias para combater essa criminalidade, que atualmente funciona como fonte de renda para organizações criminosas, que por sua vez fazem parte e também financiam o cyber terrorismo.

Podemos averiguar que os cyber ataques oferecem a entidades terroristas uma quantidade quase que infinita de alvos com danos em potencial bem maiores do que as atividades tradicionais. No uso de bombas, os impactos são limitados a localidade física e as comunidades que ali residem e se encontram. Nesse contexto, o público em geral apenas observa os acontecimentos e não é diretamente afetado pelos atos. Ainda, atos de violência não são necessariamente as medidas mais efetivas para expor uma ideologia ou uma política, visto que a atenção da mídia se volta para a destruição em si ou a perda de vidas do que a causa que motivou os atos terroristas.

[115] Anexo 01

A habilidade do cyber terrorismo de afetar uma população mais extensa pode proporcionar aos grupos envolvidos uma maior influência no que diz respeito a atingir os seus objetivos, ao mesmo tempo em garante que danos de longo prazo não venham a acontecer, algo que poderia desviar atenção à causa do grupo. Por exemplo, em um cenário onde ocorre um ataque de negação de serviço, se a parte ameaçada ceder às demandas terroristas, a situação poderia, na maioria dos casos, retornar ao *status quo ante*. Isso já não é possível em ataques tradicionais onde mortes e destruições acontecem.

Cyber terroristas operam com uma agenda política, ideológica ou religiosa. Essas motivações resultam em ataques mais específicos e direcionados a sistemas mais críticos. Estes atos coletivos podem causar mais danos do que uma ação isolada de um "cracker". Afora o fato que entidades terroristas podem ter acesso a financiamentos para empregar "hackers" para atuação em seus nomes.

Algumas conclusões podem ser extraídas desses eventos: (i) a ausência de sintomas de determinados fenômenos não implica que estes inexistem. Mas se esses fenômenos se tornarem eventuais e se transformarem em uma fonte contumaz de danos, fazem-se necessárias medidas preventivas; (ii) toda tecnologia pode ser utilizada para o benefício de todos, mas também como ferramenta de destruição; (iii) tecnologia da informação, e conectividade principalmente, é uma maravilha da civilização do século 20/21. Ela transformou tragicamente todos os aspectos do comportamento humano. Tecnologia da informação beneficia a humanidade como um todo, mas também pode – e o é – ser utilizada por indivíduos para atingir objetivos distintos do da maioria da população; (iv) estes indivíduos já começaram a criar danos significativos a aplicações de tecnologia da informação e suas respectivas infraestruturas. Atualmente, os esforços dos especialistas de segurança já começaram a render lucros, e o número de crimes de computadores passou a ter um crescimento menos acelerado, mas em uma variedade maior; (v) atualmente, terrorismo se tornou a forma generalizada de violência para expressar descontentamento público, e a internet tem sido utilizada como meio para proliferação da agenda política desses atos de terroristas.

Gostemos ou não, nós desenvolvemos uma significante dependência das tecnologias da informação. A internet está disponível 24 horas por dia e cyber terroristas poderão atacar a qualquer momento, de qualquer lugar. Isso significa que qualquer organização e/ou país pode

sentir os efeitos dos ataques de cyber terroristas. Apenas o futuro irá mostrar os riscos que nós já enfrentamos com o cyber terrorismo.

3 REPERCUSSÃO ECONÔMICA DOS CRIMES ELETRÔNICOS

Para que possamos planejar adequadamente o nível de recursos necessários para combater os crimes eletrônicos é necessário um melhor entendimento dos custos que estes causam. Ao mesmo tempo, para podemos entender os incentivos vislumbrados pelos cibercriminosos, é igualmente importante investigar os procedimentos de ataque virtual.

3.1 A economia da criminalidade: análise lato sensu

O panorama básico da economia aplicada aos estudos de atos ilícitos parte do pressuposto que os perpetradores desses atos respondem a incentivos. O crime é considerado uma escolha social, apesar dos aspectos éticos e morais, ou até desvio de comportamento dos indivíduos responsáveis. Sobre esse pressuposto, Gary Becker[116] desenvolveu um modelo que considera os custos e ganhos que motivam o crime, e as opções para controle da criminalidade, o seu custo social. Becker modela a opção do ofensor como uma função dos ganhos com o ato ilícito, a probabilidade de apreensão e a severidade e o tipo da punição. Seu objetivo é minimizar o custo social líquido produzido pelos crimes, visto que os custos imputados às vitimas e ao judiciário superam qualquer benefício auferido pelos criminosos, gerando um desequilíbrio na economia. Becker demonstra que para maximizar o rendimento social agregado, as sanções ótimas opostas a criminosas devem ser na forma de multas. Ele argumenta que multas pecuniárias têm mais eficiência na repressão do que penas de restrição de liberdade, visto que essa ainda inclui um custo para o Estado.

O modelo de Becker foi expandido para uma miríade de cenários. Uma das extensões fundamentais é o mercado de ofensas e o análise do seu equilíbrio associado. O modelo de mercado consiste no (i) suprimento de ofensas (taxa de crimes, por exemplo); (ii) demanda – provisão de bens ilegais e serviços como drogas, desvio de produtos furtados etc; e (iii) demanda negativa – vítimas em potencial de ações penais que demandem intervenção pública,

[116] BECKER, Gary S. Crime and punishment: An economic approach. Journal of Political Economy, vol. 1968, p. 169.

como aplicação correta dos provimentos legais e administração da justiça, ou de proteção privada.

O suprimento de ofensas consiste no estudo dos benefícios e custos aos ofensores, como oportunidades de ganhos, aversão pessoal a crimes e percepção individual sobre a probabilidade de apreensão. Interações sociais também são consideradas uma parte fundamental, pois influenciam as taxas de crimes na sociedade[117]. Uma das conclusões dos estudos de Becker é que os gastos em atividades com o objetivo de redução de crimes devem ser consideradas a longo prazo, visto que taxas de criminalidade são influenciadas por taxas anteriores[118], então qualquer estratégia para combater crimes pode levar gerações para obter qualquer resultado observável. Outro ponto importante é a expectativa de aumento das taxas de crimes em medida proporcional ao desequilíbrio social de uma comunidade por duas razões: (i) aqueles nas camadas inferiores têm poucos custos para cometer crimes; (ii) a presença de indivíduos que auferem altas rendas promove alvo altamente lucrativos.

O estudo de demandas públicas para a aplicação da lei lida diretamente com a distribuição ótima de recursos para o sistema jurídico. As medidas utilizadas para a otimização dos problemas são normalmente baseadas nas rendas sociais agregadas. Todavia, alguns incluem conceitos de justiça. A maioria dos modelos parte de um plano social que tem a opção de influenciar a probabilidade de apreensão e condenação de um indivíduo, a severidade de uma punição e as sanções imputadas aos ofensores. Na prática, entretanto, não existe nenhum plano social e os responsáveis pela correta aplicação da lei estão apenas preocupados com o seu bem-estar social, o que pode levar a corrupção[119].

Vitimas em potencial também têm incentivos para se protegerem, para assim reduzirem o risco de vitimização, e adquirirem seguros, para então reduzirem as perdas caso venham a ser vitimadas[120]. Uma das questões principais nesse âmbito é se a proteção privada reduz os níveis de crimes, ou apenas desvia os riscos para vitimas menos protegidas. O estudo do mercado de ofensas assume que a freqüência com que cada tipo de crime acontece reflete

[117] GLAESER, Edward; SACERDOTE, Bruce; SCHEINKMAN, Jose. **Crime and social interactions**. Quarterly Journal of Economics, 2:507–548, 1996.
[118] SAH, Raaj K. **Social osmosis and patterns of crime**. Journal of Political Economy, vol. 99. 1991, p.1272–1295.
[119] FRIEDMAN, David. **Why not hang them all: the virtues of inefficient punishment**. Journal of Political Economy, vol.107. 1999, p. 259–269.
[120] LAKDAWALLA, Darius; ZANJANI, George. **Insurance, self-protection, and the economics of terrorism. Journal of Public Economics**, vol. 89. 2005, p. 1891–1905.

em um equilíbrio implícito entre o fornecimento e a demanda desses atos[121]: o fornecimento agregado de atos ilícitos, taxa de criminalidade, por exemplo, é proporcional ao retorno esperado por ofensa, o que por sua vez decresce com a proteção privada utilizada por vitimas em potencial, e pelas sanções legais esperadas.

Modelos de mercado também têm sido utilizados para estimar o custo social da criminalidade[122]. Mercados marginais podem levar a um alto nível de crimes. Visto que as trocas são ilegais, é impossível celebrar contratos explícitos e que possam ser resolvidos pelo judiciário, levando a disputas que terminam em violência. Outra análise de mercado considera o público como provedores de oportunidades para os criminosos, e vitimas em potencial[123]. Uma das conclusões é que estes respondem as oportunidades e a provisão destas oferecidas pelo público determina as taxas de criminalidade. Enquanto que a maioria dos modelos de mercado leva em consideração grupos desorganizados, lidar com a criminalidade organizada requer modelos diferentes, em face desta representar uma entidade que tenta funcionar como um monopólio, e restringe o fluxo de transações ilegais. Em adição, participam na elevação artificial de preços e na depreciação dos esforços para aplicação da lei[124].

3.2 O custo social dos crimes eletrônicos

Existe uma falta de entendimento sobre a precisa magnitude do cibercrime e os seus impactos devido ao fato que estes nem sempre são detectados ou reportados. Razão para que estes não sejam denunciados incluem impacto financeiro no mercado, reputação ou danos a marca, preocupação com possíveis processos judiciais, o fato que reportar uma falha envia um sinal verde para novos ataques, inabilidade em fornecer informações, receios com relação à perda de emprego por parte dos profissionais responsáveis pela segurança da empresa, e uma perceptível falta de imposição da lei por parte do Estado.

---

[121] EHRLICH, Isaac. **On the usefulness of controlling individuals: an economic analysis of rehabilitation, incapacitation, and deterrence**. American Economic Review; vol. 71. 1981, p. 307–322.
[122] ANDERSON, David.**The aggregate burden of crime**. Journal of Law and Economics, vol. XLII. 1999, p. 611–642.
[123] COOK, Philippe. **The demand and supply of criminal opportunities**. Crime and Justice. vol.7. 1986, p. 1–27.
[124] GAROUPA, Nuno. **The economics of organized crime and optimal law enforcement**. Economic Inquiry. vol.38. 2000, p. 278–288.

Dados relativos aos custos dos crimes eletrônicos são fáceis de obter em alguns dos casos de falha de segurança mais notórios. Por exemplo, a falha de segurança da empresa TJX custou aproximadamente 200 milhões de dólares[125]. A companhia Heartland teve um prejuízo total de quase 40 milhões de dólares devido a sua falha que expôs milhares de históricos médicos. Todavia, muitos desses custos vieram de forma indireta, quando a empresa se deparou com processos judiciais e potenciais pedidos de responsabilidade civil[126].

Além de dados oriundos de grandes falhas de segurança, é muito difícil obter registros confiáveis de casos menores. Em particular, a metodologia utilizada pelos cibercriminosos, previamente descritas nesse trabalho, têm por alvo usuários de uma grande variedade de cenários, com acesso a diferentes serviços financeiros. No entanto, enquanto cada caso individual pode aparentar singelo e menos significante, o montante acumulado de fraudes eletrônicas pode se espalhar por diversas entidades e não serão identificados por nenhuma instituição isoladamente. Várias são as estimativas feitas por diferentes entidades nas mais diversas jurisdições[127]. Todavia, estudos indicam que perdas podem superar a cifra de 01 trilhão de dólares anuais[128]. Enquanto que essas estimativas são valiosas, elas não são de inteira confiança, pois detém grandes diferenças sem explicação aparente e alguns institutos não informam suas fontes ou a metodologia utilizada para realizarem suas estimativas[129]. Além disso, várias empresas de segurança recebem incentivos para inflarem artificialmente essas estimativas[130].

Atualmente, umas das estatísticas mais confiáveis internacionalmente são as catalogadas e coletadas pelo Inter Crime Complaint Center (IC3). O relatório anual de 2009 revelou que o número de denúncias online atingiu um recorde nesse ano, recebendo um total

---

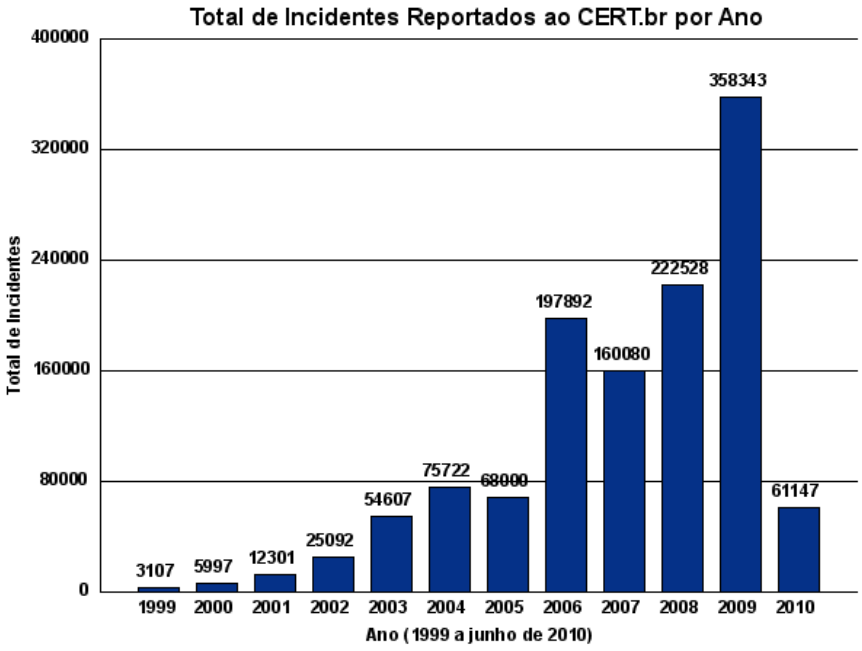
[125] TJX hacker was awash in cash; his penniless coder faces prison. Disponível em: <http://www.wired.com/ threatlevel/2009/06/watt>. Acesso em: 15 jun 2009.
[126] Payment Processor Breach May Be Largest Ever. Disponível em:<http://voices.washingtonpost.com/securityfix/2009/01/payment_processor_breach_may_b.html>. Acesso em: 15 jun 2009.
[127] ITU Study on the Financial Aspects of Net- work Security: Malware and Spam. Disponível em:<http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ itu-study-financial-aspects-of-malware-and-spam.pdf>.Acesso em: 15 jun 2009.
[128] Unsecured Economies - Protecting Vital Information. Disponível em:< http://resources.mcafee.com/content/NAUnsecuredEconomiesReport>. Acesso em: 08 set 2009.
[129] A ONG Safernet (www.safernet.org.br) detém valiosos dados com relação à segurança eletrônica no Brasil, mas não divulga suas fontes e a metodologia aplicada.
[130] ITU Study on the Financial Aspects of Net- work Security: Malware and Spam. Disponível em:<http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ itu-study-financial-aspects-of-malware-and-spam.pdf>.Acesso em: 15 jun 2009.

de 336.665 reclamações, um aumento de 23% se comparado ao ano anterior. O valor total das fraudes virtuais superou os 559 milhões de dólares[131]. A média individual foi de 931 dólares. Apesar de servirem como demonstração da gravidade dos crimes eletrônicos, essas estimativas são apenas uma pequena fração das reais perdas por diversas razões: muitas empresas preferem não reportar os ataques, pelos motivos acima expostos; vitimas podem não ser conhecidas e o IC3 compila dados apenas dos Estados Unidos da América – EUA.

O Reino Unido estimou perdas no montante a 610 milhões de libras com relação a prejuízos oriundos de fraudes de cartão de crédito, que incluem práticas onde o ilícito se deu sem a presença física dos cartões. Estes números representam um crescimento contínuo desde que começaram a ser medidos, em 2004. Enquanto que neste ano as fraudes realizadas com a presença de cartões físicos eram similares a de quando estes eram inexistentes, agora fraudes virtuais são a fonte primária dessas modalidades de delitos, sofrendo um aumento de 243%. No mesmo período, o total de transações de comércio eletrônico sozinhas aumentou 524%.

No Brasil, o instituto responsável pela coleta de dados e por receber denúncias de falhas de segurança e crimes eletrônicos é o CERT.br[132] (Computer Incident Response Team do Brasil). O ano de 2009 recebeu um total de 358.343 denúncias, número superior ao recebido por organizações americanas. O crescimento voluptuoso da economia brasileira e fragilidade dos sistemas informáticos que a sustenta foi um dos motivos ao crescimento massivo da criminalidade eletrônica em território nacional.

[131] IC3 2009 Annual Report on Internet Crime Released. Disponível em:<http://www.ic3.gov/media/2010/100312.aspx>. Acesso em: 10 jul 2010.
[132] http://www.cert.br/stats/incidentes/



Enquanto que os relatórios dessas instituições podem fornecer dados sólidos para podermos estimar as perdas oriundas de crimes eletrônicos, muito precisa ser feito para que prospecções confiáveis sejam feitas. Atualmente, não temos identificar de forma precisa o real cenário do problema. Podemos apenas afirmar categoricamente que este existe, mas sem estimativas reais não podemos mensuras se as ações tomadas pelas iniciativas públicas e privadas estão surtindo efeito.

Uma maneira possível para melhorar o conhecimento sobre os custos reais dos cibercrimes é compelir, através de leis e fiscalização freqüente (*enforcement*), bancos, instituições financeiras, provedores de serviços de internet e demais empresas a revelarem os registros e os custos associados com ataques a seus sistemas, incluindo o volume de dinheiro envolvido nos delitos. Alguns estados americanos já dispõem de legislação que determinam que qualquer falha de segurança deve ser reportada, sob pena de responsabilidade civil no montante das perdas caso seja descoberta posteriormente que a instituição não informou o incidente[133]. Reportar irá facilitar a elucidação das falhas e as tendências, assim como criar

[133] Disponível em: http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html

um mercado para a prevenção de fraudes, onde as instituições podem encontrar meios para proteger seus usuários[134].

3.3 Potencial de arrecadação dos crimes eletrônicos

Para que seja possível desenvolver um modelo econômico dos crimes eletrônicos também é necessário estimar os benefícios em potencial. Isso irá ajudar a entender os incentivos vislumbrados por criminosos em potencial e o perda social total: em quanto a margem de lucro sobre as vítimas supera os perigos oriundos de um sistema legal e de segurança.

Enquanto que alguns casos podem fornecer um material basal sobre diferentes atividades, ainda é nebuloso o quão representativo esses são com relação a essa economia marginal, visto que apenas uma fração dos incidentes são reportados, investigados e processados. Para obter um melhor panorama do real valor que adentra essa economia é necessário mais transparência por parte das instituições, tanto públicas quanto privadas, ao reportar suas perdas decorrentes de crimes eletrônicos. Estimar os ganhos dos cibercrimes é diferente do que trabalhar os danos pecuniários, visto que estes se estendem não só as informações perdidas, mas também estão distribuídas entre recuperação destas, processos judiciais, depreciação de valor de marcas e outros efeitos colaterais. Caso as instituições sejam obrigadas a informar essas perdas diretas nós possamos estimar o real fluxo de dinheiro que sustenta a economia marginal dos crimes eletrônicos.

3.4 Proteção pública

Proteção pública pode influenciar o suprimento de ofensas ao reduzir os incentivos para atos de cibercriminosos. As principais variáveis que a aplicação da lei e legislação podem influenciar são: (i) a probabilidade de apreensão de cibercriminosos; (ii) e as penalidades associadas com os cibercrimes. Com relação à probabilidade de apreensão,

[134] Op. cit. HOOFNAGLE, Chris Jay.

diversos fatores contribuem para natureza pouco arriscada do cibercrimes. Por exemplo, é altamente improvável que os aplicadores da lei se envolvam com casos que envolvem o furto de identidade, visto que a maioria das vitimas não reporta esses ilícitos para as autoridades[135]. Esse também pode ser caso o caso de furto de contas bancárias, porque a vitima normalmente resolve o problema através de um contato com o banco sem qualquer continuação de procedimentos para com o incidente. Até quando um consumidor tenta contatar a polícia, algumas autoridades ainda são relutantes em receber as denúncias. Algumas entendem que a vitima seria a instituição financeira. Ou em caso que o furto se deu em jurisdição diversa, elas podem requerer que o ofendido protocole a reclamação em outro lugar. Por outro lado, entidades privadas não recebem nenhum incentivo para reportarem incidentes de segurança.

O cenário é mais complicado para as prioridades das autoridades e *expertise*. Em um nível local, a polícia normalmente não tem recursos ou conhecimento para de forma efetiva identificar responsáveis por crimes eletrônicos. Isso leva um problema de interação entre as entidades públicas e privadas, quando estas, em muitos casos, realizam funções eminentemente públicas para que casos sejam resolvidos. Na esfera federal, apenas casos de grande monta são investigados, e os demais arquivados por falta de justa causa. Em 2003 foi estimado que cibercriminosos têm uma chance em setecentos de serem pegos por autoridades policiais[136], enquanto que em delitos comuns mais graves a probabilidade aumenta de um para cinco[137]. Essa falta de resposta das autoridades leva ainda mais as vitimas a não reportarem seus incidentes.

Mesmo que as autoridades decidam investigar e iniciar um procedimento judicial, a natureza sem fronteiras desses tipos de crimes aumentam as ambigüidades de jurisdição e as dificuldades associadas ao processo. A maioria das penalidades no Brasil atribuídas a crimes eletrônicos são brandas e não levam a penas alternativas. Como referenciado anteriormente, as penas mais eficientes são as monetárias, modalidade que encontra pouco respaldo na jurisdição brasileira. Nos casos em o responsável recebe uma pena de restrição de liberdade, afora o fato de essa pena ser mais cara para o Estado, o aprisionamento pode contribuir para o comportamento malicioso ao agregar uma comunidade de pessoas que podem compartilhar

[135] Identity theft survey report. Disponível em:<http://www.ftc.gov/os/2003/09/synovatereport.pdf>.Acesso em: 05 mai 2010.
[136] **Underreporting of identity theft rewards the thieves.** Gartner Group Research ID: M-20-3244, 2003.
[137] Porque a Lei Não Deve Almejar a Justiça, mas sim o Bem Estar. Disponível em:<http://www.redel.com.br/~dennisww/lei1.htm>. Acesso em: 30 jul 2010.

técnicas e criar redes criminosas. Dois casos clássicos podem servir de ilustração. John Draper, um dos mais famosos *phreakers*, *crackers* que utilizam seus conhecimentos para acessos sistemas telefônicos, foi preso nos EUA em 1972 devido a fraudes tarifárias. Ao sair da prisão, informou que adentrando no sistema prisional teve que ensinar a todos no estabelecimento como ele praticava as suas fraudes. O método se espalhou e as companhias telefônicas registrarem perdas ainda maiores[138]. Da mesma maneira, Max Butler iniciou suas atividades como um hacker recreativo. No entanto, quando invadiu computadores do Pentágono, ele foi apreendido e preso. Na prisão ele conheceu um fraudador profissional que o introduziu ao mundo do *carding*. Ao cumprir sua pena, ele começou a atacar sistemas de bancos, mercados e outros *crackers* pra furtar números de cartões de créditos, que eram então vendidos para *carders*[139].

3.5 Proteção privada

No molde de cooperação entre entidades públicas e privadas, a indústria de segurança computacional pode contribuir para a redução nas ofensas virtuais ao aumentar o custo para o início e a manutenção de ataques cibernéticos. Enquanto que a indústria de segurança computacional tem tradicionalmente focado em tecnologias de prevenção, firewall, antivírus, encriptação, autenticação etc, existe um mercado emergente para a detecção de ataques e a recuperação destes. Entidades privadas já foram responsáveis por muitos casos de desbaratamento de organizações criminosas cibernéticas. Do mesmo jeito, várias empresas estão utilizando monitoramento de marcas e soluções antifraude, que incluem sistemas de desligamento, que consistem em rastrear servidores maliciosos e entrar em contato com os provedores responsáveis para que o conteúdo ofensivo seja retirado. Uma das questões principais, já levantadas nesse trabalho, é se proteção privada diminui os níveis de crimes ou apenas desviam para vitimas menos protegidas.

[138] Interview with John Draper. First episode of stop H*Commerce. Disponível em:<http://www.stophcommerce.com>. Acesso em: 25 jul 2010.
[139] Kevin Poulsen. Superhacker max butler pleads guilty. Disnponível em:<http://www.wired.com/threatlevel/2009/06/butler_court/>. Acesso em: 25 jul 2009.

3.6 Moldando os incentivos dos tomadores de decisões

Provedores de serviços de internet têm abordagens diferentes ao gerenciarem o nível de segurança dos seus usuários, o que é diretamente relacionado à sua hierarquia e princípio de interconexão. A Internet atual consiste em múltiplas semi-autônomas redes que compartilham um número IP[140] em comum e uma estrutura global de roteamento do tráfego que provê diretamente ou indiretamente conectividade a essas redes. Essas redes são classificadas em três tipos de acordo com a natureza de suas conexões com outras redes.

Operadores de redes de tipo 01 frequentemente têm cobertura internacional e são proprietários da infraestrutura que forma a sua coluna vertebral (*backbone*) está interconectada através de livre pareamento para obter acesso a tabela completa de roteamento do tráfego de Internet. Por definição, provedores de serviço de internet do tipo 02 têm que celebrar contratos com pelo menos um operador de tipo 01 para poderem prover acesso global a seus consumidores. O tipo 03 foca mais nos mercado locais e seus clientes são provedores de acesso menores.

Provedores de serviços de internet do tipo 01 normalmente investem em bandas de acesso largas com significante aparato de segurança para garantir a manutenção do serviço e proteger contra uma variedade de possíveis falhas[141]. Como resultado, os incentivos para responder a problemas de segurança específicos que afetam com mais freqüência provedores de menor escala são menores. Por exemplo, o tráfego de *malwares* pode não representar um fardo muito grande a ponto de iniciar contramedidas, em particular, em face do custo com serviços de recebimento destas denúncias[142]. Enquanto provedores grandes podem atuar como recebedores de notificações de abuso, dados mostram que apenas uma pequena porcentagem é contatada após efetuarem denúncias.

Provedores de acesso a internet motivados podem aplicar um grande número de medidas para melhorar a segurança de suas redes, por exemplo: (i) atuar preventivamente, ao

[140] Internet address - IP: número atribuído a cada conexão de internet, permitindo sua individualização.
[141] Design principles & observations of routing behavior. Presentation at the SAHARA Retreat, Bi-annual Meeting, University of California, Berkeley, Networking & System Group, June 2002. Disponível em:<http://sahara.cs.berkeley.edu/jun2002-retreat/chuah_talk.pdf.>. Acesso em: 28 jul 2010.
[142] EETEN, Michel Van; BAUER, Johannes. **Economics of malware: security decisions, incentives and externalities**. Technical report, STI Working Paper, 2008.

proteger clientes de ataques ao oferecerem softwares de segurança de forma mais acessível; (ii) resposta ativa, aplicando quarentena automática e conserto de falhas ao serem detectadas; (iii) defesa da rede, através de um monitoramente local e tráfego de rede interconectado; (iv) e colaboração, implementado defesas de rede compartilhadas e criar grupos de combate conjuntos.

Todavia, é importante notar que até mesmo os provedores de internet mais vigilantes não têm sempre condições de proverem segurança a seus usuários sem iniciativas colaborativas. Primeiro, muitas ameaças não se manifestam na camada de conexão, mas sim na camada de aplicativo, a exemplo do que acontece no furto de credenciais através de *phishing*. Segundo, muitos países, como o Brasil, têm leis de privacidade estritas que proíbem provedores de acesso à internet monitorarem as ações de seus usuários, de forma que estes somente podem atuar após o recebimento de notificações de abuso. Tecnologias que reduzem identificam automaticamente essas ameaças podem reduzir a logística das denúncias.

Com relação a empresas e usuário domésticos, é necessário avaliar os possíveis papeis que estes podem exercer no combate a crimes eletrônicos. É importante mencionar que diferentes classes de usuários têm diferentes níveis de incentivos para investir em segurança.

O sucesso de esquemas de cibercrimes depende frequentemente da falta de investimentos em segurança entre usuários residenciais e pequenos negócios. Aqueles raramente estão cientes dos riscos e falham em se adequar as medidas de segurança necessárias em face da complexidade de medidas efetivas[143]. Por exemplo, eles podem abrir arquivos maliciosos anexados a e-mails ou não instalarem atualizações das assinaturas de vírus, mesmo tendo consciência que tais atos podem levar em perdas financeiras e infortúnios. Ainda, a grande maioria de usuários a quem são oferecidos serviços diferenciados de segurança escolhem manter os planos básicos por questões financeiras. Outro motivo é a falta de responsabilização quando usuários e negócios são atingidos negativamente por máquinas comprometidas[144]. Infelizmente, usuários residenciais combinados com a falta de ações preventivas podem resultar em um aumento substancial no dano coletivo.[145]

---

[143] ACQUISTI, Alessandro; GROSSKLAGS, Jens. **Privacy and rationality in individual decision making**. IEEE Security & Privacy. vol. 3. 2005, p. 26–33.
[144] Managing online security risks. Disponível em: <http://www.nytimes.com/library/financial/columns/060100econ-scene.html>. Acesso em: 28 jul 2010.
[145]GROSSKLAGS, Jens; CHRISTIN, Nicolas; CHUANG, John. **Secure or insure? A game-theoretic analysis**

Usuários também podem agir de forma passiva por estarem protegidos dos danos que podem originar de cibercrimes. Por exemplo, a legislação consumeirista protege a responsabilização dos consumidores pelo furto de suas contas bancárias. Decisões em sentido contrário ainda são raras, mesmo quando provado a culpa da vitima. Todavia, existem sim alguns incentivos para que estes apliquem medidas de segurança em suas redes, de forma que evitem os inconvenientes e as eventuais perdas monetárias.

Grandes empresas, incluindo instituições financeiras e de comércio eletrônico normalmente investem em segurança para protegerem seus procedimentos operacionais e segredos industriais. Elas podem contar com a cooperação dos provedores de acesso a Internet para se defenderem de ataques de larga escala. Também estão interessadas em manter políticas de segurança bem estritas, que normalmente incluem operarem em redes separadas.

Em contraste, empresas também têm incentivos para obscurecer os cibercrimes como furto de identidade e de credenciais, com receio que o valor de suas marcas seja atingido. Em adição, a exposição de perdas severas devido a incidentes de segurança pode levar a ensejos regulatórios indesejados pelo mercado. Altos níveis de fraude podem diminuir a credibilidade de instituições financeiras, iniciando um movimento em cadeia que pode levar a uma instabilidade em todo mercado.

Ainda, como mencionado, usuários maliciosos pagam por serviços diferenciados a provedores de internet fraudulentos, recebendo em retorno a possibilidade de conduzirem suas atividades por mais tempo sem que seus conteúdos sejam retirados ou atingidos.

A indústria de *software* é um caso interessante na análise dos cibercrimes. Enquanto que a maioria das empresas é responsabilizada pela segurança de seus produtos, a prática atual na indústria de software é a não imputação de responsabilidade pela qualidade do *software* através do contrato de utilização de licença (*user license agreement*). São raras as decisões judiciais em sentido contrario.

---

of information security games. World Wide Web Conference (WWW'08). China. 2008, p. 209–218.

4 REPRESSÃO AOS CRIMES ELETRÔNICOS

O ciberespaço é uma das grandes fronteiras legais do nosso tempo. Entre 2000 e 2008, a Internet expandiu a uma taxa anual de 290% a um nível global, e atualmente há uma estimativa que mais de 2 bilhões[146] de pessoas estão na grande rede. O impacto da Internet nas sociedades foi tão rápido e profundo que códigos de ética, o senso comum de justiça, e a legislação penal foram expandidos para poderem acompanhar o passo. Para que seja possível estabelecer padrões éticos no ciberespaço, as normas criminais precisam ser claras e específicas, no lugar de se basearem em analogias e vagas interpretações da legislação existente. Perpetradores e ofensores poderão, então, ser condenados por seus atos e não por interpretações extensivas das provisões existentes, ou por normas especificamente promulgadas com esse objetivo, cobrindo cibercrimes de forma acidental e periférica.

Atualmente, a questão de como enfrentar os crescentes desafios legais colocados pelos crimes eletrônicos e outras questões que envolvem segurança da informação e de redes está sendo amplamente discutida, como pode ser visto nos vários projetos de lei e determinações a seguir. Existem dois níveis distintos que podem corresponder a esses desafios: provisões gerais ou abordagens internacionais através de organizações internacionais. Ou ainda soluções individuais feitas por países de forma isolada ou em grupos de uma determinada região geográfica. Ambos têm vantagens e desvantagens.

O cibercrime é por natureza sem fronteiras e, potencialmente, transnacional. Ofensores podem ter por alvo usuários em qualquer lugar do mundo, fator determinante para a necessidade de uma cooperação internacional de agências responsáveis pela imposição da lei e figura essencial para investigações de natureza internacional. Estas dependem de meios confiáveis de cooperação e na efetiva harmonização de leis. A cooperação efetiva primeiramente necessita uma harmonização da lei penal substantiva para prevenir portos seguros para os cibercrminosos. Ainda, é necessário harmonizar os instrumentos de investigação para assegurar que todos os países envolvidos em investigações internacionais detêm o mínimo necessário para realizar corretos procedimentos investigatórios. Finalmente, a efetiva cooperação das agências requer leis penais processuais pragmáticas e rápidos, devido a própria natureza probatória decorrente dos delitos eletrônicos. A importância da

[146] Ver: http://www.internetworldstats.com/stats.htm

harmonização reflete na necessidade de uma estratégia nacional para cibercrimes e outras questões relacionadas à segurança da informação e de redes para que assim possam participar no processo global de harmonização.

A importância em atingir um padrão único não deveria, em tese, necessitar de novas leis. Modelos se estratégias são desenvolvidas para prevenir conflitos entre as abordagens legislativas diferentes. Para que possamos assegurar o *compliance* com *standards* internacionais é possível a aplicação de provisões já existentes, como a Convenção Européia para Cibercrimes. Nesse sentindo, a Convenção de Tunis para a Sociedade da Informação[147], em seus parágrafos 40 e 42, assim proclama:

> 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 mususe of information technologies` and regional initiatives including, but not limited to, the Council of Europe's Convention on Cybercrime".
>
> We affirm that measures undertakem 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 Declarations of Human Rights and the Geneva Declaration of Principles".

Enfrentaremos a seguir algumas iniciativas já existentes nos âmbitos nacionais, regionais e internacionais para combater o avanço dos crimes eletrônicos.

4.1 A Convenção do Conselho Europeu para Cibercrimes[148]

Em 2001, a Convenção do Conselho Europeu para Cibercrimes[149] foi uma iniciativa histórica na luta contra os crimes eletrônicos. Entrou em vigor em primeiro de julho de 2004 e até o presente momento 31 Estados a ratificaram e outros 12 a assinaram, mas ainda não a

[147] Tunis Agenda for the Information Society. Disponível em: <www.itu.int/wsis/index.html>. Acesso em 25 jul 2010.
[148] Anexo 08
[149] Disponível em: http://www.conventions.coe.int.

incorporaram ao ordenamento jurídico interno, entre eles o Brasil[150]. A convenção está dividida em quatro capítulos.

O capítulo um trabalha o uso de termos, incluindo definições sobre sistemas computacionais, registros de computadores, provedores de serviço e tráfego de informações. O capítulo dois trata sobre medidas que podem ser aplicadas em um nível nacional, incluindo seções sobre leis penais substantivas, leis processuais e princípios jurisdicionais. A seção sobre leis penais substantivas discorre sobre ofensas contra confidencialidade, integridade e disponibilidade de sistemas e registros computacionais, como acesso ilegal, interceptação indevida, interferência nos registros e nos sistemas e mal uso de serviços. Delitos relacionais a computadores incluem fraude e falsificação, pedofilia, ofensas a direitos autorais e outros decorrentes. A seção sobre leis processuais penais inclui provisões que podem ser aplicadas as de natureza substantiva e a outros crimes eletrônicos, além da correta coleta de evidências relacionadas à cibercrimes.

O capítulo três trata cooperação internacional e inclui princípios gerais relacionados a cooperação, extradição, assistência mutua e fornecimento espontâneo de informações. Contém procedimentos pertinentes a requisição pela aplicação desses princípios na falta de acordos internacionais aplicáveis, a confidencialidade e limitação de uso das informações, além de medidas acautelatórias e de limitação de poderes de investigação, e finaliza ao traçar uma rede forense que funcionaria vinte e quatro horas por dia, sete dias pro semana. O capítulo quatro contém provisões finais, que têm por objeto adequar a convenção aos tratados do Conselho Europeu.

Ao ratificar ou aceitar a convenção, países acordam em assegurar que suas leis domésticas irão criminalizar as condutas descritas nas seções substantivas e processuais, além de estabelecer ferramentas procedimentais necessárias para investigação e persecução penal de tais crimes. A Convenção sobre Cibercrimes tenta utilizar uma linguagem tecnológica neutra para que possa ser aplicada tanto para tecnologias atuais e futuras. Os Estados podem excluir condutas que considerem insignificantes. As ofensas devem ser cometidas com dolo específico, ou seja, o dano intencional tem que ser objeto da conduta delituosa.

---

[150] Disponível em:< http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=9/2/2006&CL=ENG>. Acesso em: 25 jul 2010.

Como dito, coordenação e cooperação internacional são necessárias para a persecução penal de cibercrimes e outras questões relacionadas a segurança da informação. Por isso, governos devem tomar passos inovadores para enfrentarem essas sérias ameaças.

4.2 O G8

Os Estados do G8[151] estabeleceu um grupo de Crimes de Alta Tecnologia em 1997. Nesse ano, em convenção e Washington D.C. os países adotarem dez princípios para combater crimes de computadores para assegurar que não haja portos seguros para esses criminosos em qualquer lugar do mundo.

Em reunião na mesma cidade no ano de 2004, os ministros do G8 disponibilizaram um comunicado conjunto afirmando que com o advento da Convenção Européia para Cibercrimes, os Estados deveriam realizar medidas para encorajar a adoção dos padrões legais estabelecidos nela, além de se manifestarem proclamando que as agências de segurança possam responder rapidamente as sérias ameaças oriundas de ameaças virtuais e incidentes de segurança.

4.3 A União Européia

O conselho da União Européia adotou uma proposta em 2003 para uma plataforma de decisões do conselho para ataques contra sistemas informáticos (*Council Framework Decisions on attacks against information systems*)[152][153], que entrou em vigor em 2005. Essa plataforma suplementa a Convenção Européia sobre Cibercrimes e inclui normas que tratam sobre acesso ilegal a sistemas de informações, interferência ilegal no sistema e nos registros deste.

---

[151] Canadá, França, Alemanha, Itália, Japão, Rússia, Reino Unido, Estados Unidos.
[152] Disponível em:< http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/l33193_en.htm >. Acesso em: 25 jul 2010.
[153] Anexo 02

Ainda, em maio de 2007, o conselho se pronunciou sobre uma proposta legislativa contra furto de identidade, chamada de "*Towards a general policy on the fight against cybercrime*"[154]. Os delegados assim se pronunciaram:

> The increasing prevalence of cybercrime across Europe, spanning large-scale attacks in Estônia, identity theft in Spain, illegal content and high-profile online child abuse incidents in Áustria, Germany, Italy and the UK, highlights the need for concerted action. Indeed successful operations such as `Operation Koala` and the global hunt for the ˜Vico˜ paedophile depends on regional and internacional cooperation. The conclusions of today's meeting represent an important step by the EU to establish the cooperative links upon which success is built.

4.4 Grupo de Cooperação Econômica da Ásia-Pacífico (APEC)[155]

Em reunião em 2002, no México, os lideres da APEC se comprometeram a estabelecer um corpo legislativo abrangente sobre seguridade informática e cibercrimes. Pronunciamentos similares foram feitos em outras oportunidades, quando os Ministros renovaram seus compromissos, declarando que encorajavam todas as economias a estudarem a Convenção Eupeia para Cibercrimes além de outros instrumentos legais, como a resolução número 55/63 da Assembléia Geral das Nações Unidas de 2000.

O grupo de trabalho em telecomunicações e informações da APEC adotou em 2002 a estratégia de cibersegurança para implementar os objetivos enaltecidos pelos ministros. Essa estratégia envolve principalmente a capacidade para o desenvolvimento de corpos legislativos voltados para o combate de crimes eletrônicos e agências efetivas nesse para esse intuito. Também foi reconhecido a Convenção Européia como o primeiro instrumento legal multilateral sobre cibercrimes. Muitos assuntos são discutidos nesse contexto, como *spam*, segurança de redes sem fio, *malware*, exercícios de treinamento, *botnets*, aparelhos móveis, entre outros. Outras discussões envolvem a construção de legislações, conhecimento específico sobre a matéria em times de resposta a incidentes (CIRTs) e forense computacional.

---

[154] Disponível em:< http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF >. Acesso em: 25 jul 2010.
[155] http://www.apec.org/

4.5 Organização dos Estados Americanos (OEA)

A Organização dos Estados Americanos sempre tomou a dianteira em assuntos relacionados a crimes eletrônicos. Os Ministros da Justiça dos Estados Membros recomendaram em 1999 o estabelecimento de um grupo de estudos sobre cibercrimes[156]. Em 2004, o quinto encontro de Ministros da Justiça e Procuradores Gerais das Américas (REMJA), em Washington D.C., aprovou diversas conclusões e incluiu as seguintes recomendações:

> Member States should evaluate the advisability of implementing the principles of the Council of Europe's Convention on Cybercrime (2001), and consider the possibility of acceding to that convention

Em 2005, prolataram a seguinte recomendação:

> Strongly encourage States to consider the possibility of becoming Parties to this Convention in order to make use of effective and compatible laws and tools to fight cybercrime, at domestic level ando n behalf of international cooperation

Outras recomendações foram feitas nesse sentido e uma resolução adotada na sessão plenária de 2007. Vários organismos regionais se pronunciaram de forma semelhante, entre eles a Associação das Nações do Leste Asiático (ASEAN), a Liga Árabe, a União Africana, a Organização para o Desenvolvimento e Cooperação Econômica (OECD)[157].

[156] www.oas.org/juridico/english/cyber.htm.
[157] www.oecd.org/sti/security-privacy.

4.6 Organização das Nações Unidas

A Organização das Nações Unidas ainda não detém nenhuma convenção ou tratado que trate especificamente sobre crimes eletrônicos. Todavia, essa matéria há muito vem sendo discutida tanto no cerne de outras normas internacionais quanto em fóruns específicos sobre a temática. No 12º Congresso das Nações Unidas para Prevenção e Justiça Criminal, que aconteceu abril de 2010, em Salvador, Brasil, restou entendido ser o ciberespaço o 5º espaço comum, após terra, mar, ar e espaço sideral. Além, foi corroborado o entendimento da necessidade de cooperação e de normas para a prevenção e punição a crimes eletrônicos:

> Cyberspace, as the fifth common space – after land, sea, air and outer space, is in great need for coordination, cooperation and legal measures among all nations. Deterrence against cyberthreats may best be achieved through a global United Nations framework. A Cyberspace Treaty, including cybersecurity and cybercrime, should be the framework for peace and security in Cyberspace. The fast growth of cyberspace has implied the opening of new opportunities for criminals to perpetrate crime. Cyberthreats are global problems and they need a global harmonization involving all stakeholders. International law is necessary to make the global community able to deter the urgent and increasing cyberthreats. In order to reach for a common understanding of cybersecurity and cybercrime among countries at all stages of development, a United Nations Cyberspace Treaty should be established that includes solutions aimed at addressing the global challenges. Serious crimes against peace and security in cyberspace should be established as crimes under international law, whether or not they were punishable under national law. The Council of Europe has in 2001 established a regional convention on cybercrime, which could be used as a guideline or reference for a new treaty or protocol on the global level. But this convention is based on criminal conducts in the 1990s, and do not necessary be suitable for the 2010s. And some countries do not accept all principles in the convention, and must be respected for their opinions. The new criminal conducts should be covered in a Cyberspace Treaty. The reports and recommendations of the High-Level Experts Group (HLEG) in 2008, may be thus be used as a guideline or as a reference.[158]

A decisão mais importante nesse sentido é a Resolução 55/63 da Assembléia Geral de 2000[159] e a Resolução 56/121[160] da Assembléia Geral sobre o combate ao mal uso de tecnologias da informação ("*Combating the criminal misuse of information technologies*"). Elas convidam os Estados membros a desenvolverem leis nacionais, políticas e práticas de

[158] Anexo 05
[159] Anexo 06
[160] Anexo 07

combate a crimes eletrônicos e que para tanto levem em consideração o trabalho da Comissão da ONU para Prevenção de Crimes e Justiça Criminal.

4.7 Cenário Brasileiro

Existem hoje mais de 70 projetos[161] de lei que, de uma maneira ou outra, discorrem sob aspectos na internet, sejam eles no âmbito constitucional, civil ou penal. Vários deles têm por objeto crimes eletrônicos. Entre os que se destacam nesse âmbito estão o PL 84/99[162], de autoria do Senador Luiz Piauhylino, que dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências.

Todavia, a iniciativa mais ousada e abrangente é o Marco Civil da Internet Brasileira[163], que diferente das anteriores, não tenta implementar a regulamentação no âmbito penal, mas sim fazê-lo no âmbito civil, possibilitando a construção de ferramentas que tornam possível a persecução criminal de ilícitos na Internet. Os motivos ensejadores de um marco civil regulatório da internet brasileira são os mais distintos. Desde a variada jurisprudência oriunda das mais diferentes lides processuais país afora até a necessidade de balizas de responsabilidade para as empresas provedoras de serviço e dos usuários, que em muitos casos se encontravam em limbo permeado por ativistas digitais, juristas e empresários, com pensamentos e posições singulares com relação ao modo como a grande rede deve ser tratada.

Alguns assuntos ganham mais destaque no texto oriundo da discussão digital sobre o texto de lei. Entre eles estão a garantia da liberdade de expressão, a neutralidade da rede, a responsabilidade das empresas provedoras de serviço de internet e a tempo de guarda dos registros de acesso e de conexão.

As maiores discussões sobre textos legislativos que envolvem a internet mundo afora envolvem a neutralidade da rede, ou seja, a característica inata desta de não receber filtragens anteriores, seja de conteúdo, seja de quantidade, seja de padrões. Essa é a temática central da

[161] Anexo 09
[162] Anexo 10
[163] Anexo 11

discussão no âmbito americano, em um grande embate entre a FCC[164] e Google e as grandes empresas provedoras de serviços de internet, que defendem certos filtros de conteúdo, principalmente em conexões de banda larga móvel e questões que envolvem direitos autorais. No Brasil, a discussão margeia a possibilidade de censura prévia, algo rechaçado pela maioria, ou pelo menos por aqueles que detêm algum conhecimento do funcionamento intrínseco da rede.

Uma das principais características da internet atual, a chamada Web 2.0, é a sua natureza colaborativa, participativa, possibilitando que cidadãos expressem suas opiniões e funcionem como entes modificadores, como no caso da metodologia empregada para a elaboração do Marco Civil da Internet Brasileira.

Um dos mais fortes fatores que levaram a proliferação da internet e dos serviços de internet nos EUA foi a não responsabilização destes pelo conteúdo produzido pelos usuários, bandeira que este Marco Civil vem a defender. Todavia, algumas iniciativas do governo brasileiro vão de encontro ao princípio da livre iniciativa e da livre concorrência, mormente no âmbito da internet. Iniciativas como o plano nacional de banda larga com a restauração da Telebrás como estatal responsável pela implementação das diretrizes estabelecidas não coaduna com as benesses que podem ser conseguidas caso esta empreitada seja implementada pela iniciativa privada, com os devidos incentivos públicos.

O art. 6º do anteprojeto de lei determina que "*O acesso à Internet é direito do cidadão, fundamental ao exercício da cidadania, às liberdades de manifestação do pensamento e de expressão e à garantia do acesso à informação*". Apesar de ser algo que eleve a internet ao patamar de direito fundamental, em similitude aos previstos no art. 5º da CF, cabe perguntar se seria esta a grafia correta. Seria o "acesso à internet" ou "o direito à inclusão digital" que deveria ser um direito fundamental? Não basta ter acesso à internet, é necessária uma infraestrutura para que os direitos do cidadão venham a ser corretamente exercidos através e com a rede.

O anteprojeto de lei engloba diversas outras matérias, como o tempo de armazenamento dos registros de internet por parte dos provedores de serviço e de acesso, a necessidade de retirada do conteúdo somente com ordem judicial expressa, ferramentas educacionais, limites mínimos a prestação de serviços adequados, responsabilidade do

[164] Agência reguladora de telecomunicações americana

intermediário e do provedor de hospedagem. Todavia, ainda se encontra sob intensa discussão no âmbito da internet e do Ministério da Justiça[165], para então prosseguir para as casas do Congresso Nacional.

4.7.1 Órgãos de repressão

Apesar da ineficiência da maioria dos órgãos de repressão, o Brasil já dispõe de algumas iniciativas públicas de combate específico a crimes eletrônicos. Entre eles se destaca o Departamento de Segurança da Informação e Comunicações – DSIC**,** vinculado ao Gabinete de Segurança Institucional da Presidência da República, responsável, como já mencionado anteriormente, pela segurança as infraestruturas críticas de tecnologia da informação necessárias para a manutenção do aparato estatal. Com relação a órgãos públicos investigação, em face da proliferação massiva do cibercrimes, diversas delegacias especializadas foram criadas. Todavia, a maioria carece de profissionais com conhecimento suficiente para realizar medidas efetivas e também de aparato técnico mínimo para procederem corretamente com as investigações. Até o presente momento, existem as seguintes delegacias:

- **Divisão de Repressão aos Crimes de Alta Tecnologia (DICAT):** divisão especializada em crimes tecnológicos que tem como atribuição assessorar as demais unidades da Polícia Civil do Distrito Federal. Como Divisão, a DICAT não atende ao público, não registra ocorrências nem instaura inquéritos policiais. A finalidade da DICAT é prestar apoio às Delegacias de Polícia do DF nas investigações de crimes que envolvam o uso de alta tecnologia, como computadores e internet, agindo sob provocação das destas ao necessitarem de auxílio nessa matéria. Desse modo, a vítima de crime cibernético no Distrito Federal pode procurar qualquer uma das Delegacias de Polícia (as não especializadas) para efetuar registro da ocorrência. Por fim, a DICAT recebe denúncias de crimes cibernéticos (que são repassadas aos órgãos

[165] http://culturadigital.br/marcocivil/

competentes) e presta esclarecimentos sobre condutas a serem adotadas por vítimas de crimes cibernéticos no DF, quando informados ou solicitados por e-mail;

- **Núcleo de Repressão a Crimes Eletrônicos (NURECCEL) da Polícia Civil do Espírito Santo[166];**
- **Divisão de Repressão aos Cibercrimes (DRC) da Delegacia Estadual de Investigações Criminais (DEIC) - Goiânia/GO;**
- **Delegacia Especializada de Repressão a Crimes contra a Informática e Fraudes Eletrônicas – DERCIFE da Polícia Civil de Minas Gerais [167];**
- **Delegacia Virtual do Pará[168];**
- **Polícia Civil - Núcleo de Combate aos Cibercrimes (Nuciber) da Polícia do Paraná[169];**
- **Polícia Civil de Pernambuco - Delegacia interativa[170];**
- **Polícia Civil do Rio de Janeiro - Delegacia de Repressão aos Crimes de Informática (DRCI)[171];**
- **Delegacia de Repressão aos Crimes Informáticos (DRCI) da Polícia Civil do Rio Grande do Sul[172];**

[166] Endereço: O Núcleo funciona do edifício-sede da Chefia de Polícia Civil, 2º andar, localizado na Av. Nossa Senhora da Penha, 2290 – Bairro Santa Luiza – Vitória/ES, ao lado do DETRAN.
Telefone: (27) 3137-9078 ou fax (27) 3137-9077
E-mail: nureccel@pc.es.gov.br
WebSite: http://www.pc.es.gov.br/nureccel.asp
[167] Endereço: Av. Antônio Carlos, 901 - Lagoinha - Belo Horizonte - MG
Telefone: (31) 3429-6024 | Horário de Atendimento: 08:30 às 18:30 horas
E-mail: dercifelab.di@pc.mg.gov.br
[168] WebSite: http://www.delegaciavirtual.pa.gov.br
E-mail: comunicacao@policiacivil.pa.gov.br
[169] Rua José Loureiro, 376 – 1º. Andar – sala 1 – Centro – Curitiba-PR
E-mail: cibercrimes@pc.pr.gov.br
Telefone: (41) 3883-8100
[170] WebSite: http://ww8.sds.pe.gov.br/delegaciainterativa/default.jsp
E-mail: policiac@fisepe.pe.gov.br
[171] Endereço: Rua Professor Clementino Fraga nº 77 - Cidade Nova (prédio da 6ª DP), Rio de Janeiro, RJ
Telefone: (21) 3399-3203 / 3200
E-mails: drci@policiacivil.rj.gov.br / drci@pcerj.rj.gov.br
[172] End.: Av. Cristiano Fischer,1440 - Jardim do Salso - Porto Alegre/RS - CEP 91410-000 (prédio do DEIC)

- **Polícia Civil de São Paulo - 4ª. Delegacia de Delitos Cometidos por meios Eletrônicos – DIG/DEIC[173].**

Ao início da elaboração da presente dissertação, era da opinião do autor a necessidade de uma justiça especializada para lidar com crimes eletrônicos e matérias ligadas ao direito eletrônico como um todo. Todavia, durante a reflexão sobre o texto passou a entender que em face da natureza interdisciplinar da matéria o que realmente deve ser efetivado são políticas de ensino e aprofundamento em disciplinas concernentes a sociedade da informação como um todo. Além do acima mencionado, ferramentas forenses adequadas devem fazer parte dos instrumentos dos órgãos de repressão e investigação. Se assim não estiverem aparelhados, todo o esforço legislativo e normativo será em vão.

---

drci@pc.rs.gov.br
www.twitter.com/drci_rs
Gabinete: (51) 3338-1624
Secretaria: (51) 3338-2093

[173] Avenida Zack Narchi,152 - Carandiru, São Paulo-SP OBS: perto da antiga detenção do Carandiru, próximo ao Center Norte, estação do metrô do carandiru
Telefone: (11) - 6221-7030 / 6221-7011 - ramal 208
E-mail: 4dp.dig.deic@policiacivil.sp.gov.br

CONCLUSÃO

Na era da informação em que vivemos, as tecnologias nos proporcionam, ao mesmo tempo, prosperidades e perigos. Nos conectam como nunca antes e são vitais para a nossa atual concepção de sociedade e moldam o estilo de vida com o qual nos acostumamos. Todos e tudo está interligado, mesmo que esse fato não seja do nosso conhecimento. Desde o simples ato de sair de casa para ir ao trabalho até o tomar um copo de água, passando pelo pagamento de contas ou o andar pelas calçadas de uma grande cidade. Não podemos mais nos desvincular da rede que entremeia nosso dia-a-dia, ao ponto de não conseguimos distinguir o virtual do real, partindo do pressuposto que existe uma diferença entre essas duas facetas.

A sociedade da informação trouxe consigo a efetiva aplicação das dimensões de direitos fundamentais, entre elas a quarta dimensão, com a globalização, na idéia de interligação e expansão das fronteiras da sociedade, e a quinta dimensão, com o Direito à Informação elevado a um patamar nunca antes vislumbrando. Passamos agora por uma nova dificuldade, que seria como garantir o Direito à Informação correta e fidedigna, dentro mar de informações que nos são disponibilizadas.

Uma sociedade interligada traz embutida em si a utópica idéia de uma sociedade una, de um governo único, de um povo singular. Fato é que as distancias desapareceram, barreiras foram derrubadas, entrepostos extintos, línguas tornaram-se irrelevantes. A teia cibernética que carrega consigo todo o liame de informações mudou o conceito de Estado, onde as clássicas balizas território, povo e soberania tiveram que ser revisitados, moldando novos termos que ainda estão longe de receberem conotações definitivas. Não temos como prever como estará a sociedade em dez anos, mas ameaças já existentes devem ser, de forma imperativa, estudadas, trabalhadas e combatidas. Não podemos, sob a desculpa que se trata de uma matéria nova, incipiente, aguardar para tomar providências. Crimes eletrônicos já representam uma grande parcela da criminalidade atual. Isso é fato. Tanto que já ultrapassara o tráfico de drogas em valor de arrecadação. Como reverter esse quadro é único questionamento a ser feito.

No âmbito brasileiro, a legislação atual já cobre a grande maioria das condutas ilícitas perpetradas através de meios eletrônicos. Mas a velocidade com que a sociedade da informação se reformula é exponencialmente maior do que a impressa por nossos

representantes do Poder Legislativo. Novas práticas surgem a cada dia e desafiam os profissionais que atuam nesse setor. Para isso, projetos de lei estão em andamento para suprir as lacunas ainda existentes, inclusive utilizando-se da característica colaborativa da grande rede para promover a discussão com a população e perpetrar o caráter democrático do processo legislativo. Iniciativas como o Marco Civil da Internet e a reforma da Lei de Direitos Autorais utilizam massivamente as ferramentas que a web proporciona, tornando possível o usufruto de uma consciência coletiva para tentar acompanhar as inovações do mundo digital.

Entretanto, ainda vislumbramos diariamente o malferimento a direitos fundamentais no uso da grande rede. Racismo, apologia e segregação. Quebra de sigilo, invasão de privacidade e intimidade. Todas são práticas contumazes na Internet que apesar de já terem previsão legislativa e punições condizentes não diminuem sua incidência, pelo contrário. Como forma de evitar essas condutas muitos defendem a figura de um Estado de vigília, da figura de um Grande Irmão, de uma sociedade espiã, preventiva e preemptiva. Que a neutralidade inerente a Internet seja abolida, em clara colisão a direitos como a liberdade de expressão, manifestação e locomoção. Isso é inadmissível. O espaço virtual não pode ser tratado de forma diferente ao real, pois os dois são uma extensão do outro, e travam uma relação simbiótica. Outras soluções devem ser concebidas e já foram.

Entidades de combate especializadas, forças de trabalho, aparelhamento das instituições, políticas de educação, inclusão digital, todas são medidas que já são praticadas pelo governo e pela iniciativa privada, mas não são suficientes. Elas não têm impedido o cometimento massivo dos crimes eletrônicos, que por suas próprias características, como a dificuldade de identificação da autoria e fragilidade e efemeridade das provas necessárias para a materialidade do ilícito, necessitam de tratamento diferenciado. A natureza sem fronteiras e a proliferação massiva de mídias digitais e da tecnologia da informação apenas contribuem para o aumento exponencial dessa criminalidade. Crimes que atingem indivíduos não são os mais freqüentes, como costuma pensar o imaginário popular. Pessoas jurídicas já são as mais atingidas e as perdas pecuniárias são praticamente imensuráveis, visto que muitas das vitimas não revelam os delitos as autoridades, mas já ultrapassaram o tráfico de drogas e se tornaram uma das modalidades criminosas mais lucrativas. As falhas de segurança e o furto de propriedade imaterial, ativo mais valioso na sociedade da informação, somam perdas na ordem dos bilhões de dólares anuais. Os crimes não são mais praticados por indivíduos que trabalham de forma isolada e por interesses simplórios. São agora fruto de um complexo

sistema organizado por entidades criminosas multinacionais, que atuam em todos os setores, desde o simples provimento a internet até a fundação de empresas legítimas que servem de fachada para a execução de ilícitos digitais.

A internet está diretamente atrelada ao comércio, local e internacional, e é peça chave para o desenvolvimento de uma nação. E pode ser fator desencadeador de um equilíbrio entre as nações, com base na abertura de portos virtuais que proporcionam as nações verdadeiro entrepostos comerciais onde podem transacionar seus bens. Todavia, crimes eletrônicos causam as empresas privadas a perda de bilhões de dólares anuais. Milhões de consumidores, que utilizam a internet para pagamentos, compras e outras atividades básicas, já foram vitimados. Privacidades foram violadas, identidades e valores furtados, vidas reviradas, tornando as ameaças virtuais uma das mais sérias que uma nação pode enfrentar atualmente.

As ameaças provenientes de crimes eletrônicos não são apenas de caráter financeiro ou moral, mas também de ordem estrutural. A maior ameaça recai sobre as estruturas da informação criticas que sustentam nossa sociedade. Sistemas financeiros, de energia, água, comércio. Todos são hoje controlados estritamente por sistemas eletrônicos que estão suscetíveis a ataques cibernéticos de grande monta, que podem partir não apenas de Estados em conflito, mas de entidades não estatais, que pelos mais diversos motivos, ideológicos, políticos ou partidários, podem iniciar ataques oriundos de qualquer parte do mundo, ao mesmo tempo, tornando quase impossível determinar a correta autoria. A fragmentação com que a Internet foi concebida, fruto de um cenário bélico do período de guerras, contribui para a dificuldade com que ataques de grande monta e bem elaborados sejam identificados. Ataques como esses já aconteceram e há muito tempo ultrapassaram a barreira das histórias de ficção. Nações inteiras já foram colocadas fora do mapa virtual, com repercussões bem maiores no mundo real.

Nesse mundo interconectado, as vulnerabilidades são compartilhadas, assim como a responsabilidade pela proteção e combate. O Governo tem responsabilidade primária nesse trabalho, visto que as redes de infraestruturas da informação são ativos críticos para a manutenção de um Estado. Todavia, o setor privado compartilha dessa responsabilidade, por ser proprietário e responsável pelo gerenciamento e operacionalidade dessas infraestuturas, bens necessários para o correto funcionamento de uma sociedade moderna. Para tanto, é necessário parcerias e cooperação entre as entidades públicas e privadas, de âmbito nacional e

internacional, para garantir a segurança dessas infraestruturas como forma de manutenção da economia e da privacidade como direito fundamental estruturante.

Organizações criminosas, entidades terroristas, estatais ou paraestatais, utilizam a internet e as tecnologias da informação para atuarem. Moldam suas estruturas de funcionamento em semelhança ao funcionamento da grande rede: fragmentada e independente. Uma célula criminosa independe de outra para existir, e ao mesmo tempo trabalha em harmonia com as demais, utilizando a Internet para sustentar esse molde de existência. A internet é hoje a arma mais valiosa para que essas organizações perpetrem seus objetivos e atinjam seus alvos. Nunca foi tão fácil para elas se comunicarem de forma anônima e de difícil percepção, ao mesmo tempo em que encontraram um terreno ávido de interessados e colaboradores que podem ser colhidos em qualquer parte do mundo. Não é mais preciso a presença física para agir. Os alvos não são mais unos e podem atingir proporções nunca antes imaginadas, engatilhados de qualquer lugar do planeta. E as infraestruturas críticas da informação se tornaram alvos preferenciais, pois podem causar danos massivos e exibir para o mundo de forma mais contundente as ideologias de entidades responsáveis por tais atos.

Na esteira da necessidade de atuação mútua de todas as esferas, é vital que exista uma cooperação entre a comunidade internacional. A inexistência de fronteiras para o cometimento de ilícitos através da internet somente pode ser contida caso os países se ajudem, em conjunto com as Organizações Internacionais como Nações Unidas, OTAN e Interpol. No âmbito sul sul-americano, o Conselho de Segurança da União do Cone Sul – UNASUL, já discute medidas de efetivação de políticas de combate a crimes eletrônicos. Tratados internacionais como a Convenção Européia de Cibercrimes e a recomendação da ONU para o combate a guerra virtual são iniciativas normativas internacionais que devem ser aprimoradas e expandidas. Os países signatários devem ser transparentes quanto a suas políticas para tecnologias da informação e estratégias ofensivas e defensivas para com atos ilícitos no meio eletrônico.

A guerra virtual já é uma realidade e por isso conceitos clássicos devem ser revistos, como a concepção do que pode ser considerado um ato de guerra e quando uma retaliação pode ser autorizada dentro do Direito Internacional. Normativas humanitárias e cartas de comportamento para esses períodos devem ser revisitados para coadunarem com as novas realidades. Identificar quem são os atores internacionais responsáveis por atos bélicos deve

ser uma máxima primária antes da realização de qualquer contra medida. A Internet facilitou a proliferação de entidades não-estatais e a atuação de Estados através de indivíduos ou entidades tende a se tornar algo freqüente que deve ser combatido com eficientes métodos de investigação. Estados devem ter em mente que a errônea atribuição de responsabilidade pode desencadear reverberações e flutuações econômicas que tem a capacidade atingir não só a relação bilateral, mas também toda uma miríade de nações que interdependem entre si em face do comércio internacional.

Nesse ínterim, nenhum setor da sociedade detém capacidade para garantir, de forma isolada, a manutenção das infraestuturas críticas da informação. Para tanto, é necessário não só a cooperação entre entidades, mas também o auxílio dos cidadãos e indivíduos que compõem a sociedade moderna. Por muitas vezes, o elo mais fraco para o cometimento de um crime eletrônico, seja ele de pequena ou grande monta, é o usuário, que não toma as precauções necessárias e age de forma negligente, tornando seus sistemas, e os demais, vulneráveis.

Políticas públicas de combates a crimes eletrônicos devem levar em consideração as características basais da grande rede e o respeito a direitos fundamentais. Neutralidade, fragmentação, colaboração, libertação. Privacidade, intimidade e sigilo. Pilares que não podem ser afastadas, pelo contrário, devem funcionar como norte interpretativo na atuação do poder público em qualquer âmbito que envolva a internet, a sociedade moderna e as tecnologias da informação. Cooperação com todos os setores deve ser o emblema de qualquer iniciativa sobre a temática. Tendo isso em foco, e a concepção que é necessária uma atuação conjunta das entidades públicas, privadas e de todos os indivíduos, podemos agir de forma equânime quanto a prevenção e combate de todas as modalidades que existam ou que por ventura venham a existir de crimes eletrônicos.

BIBLIOGRAFIA

ACQUISTI, Alessandro; GROSSKLAGS, Jens. **Privacy and rationality in individual decision making**. IEEE Security & Privacy. vol. 3. 2005.

ALBUQUERQUE, Roberto Chancon de. **A criminalidade informática**. São Paulo: Editora Juarez de Oliveira, 2006.

ALEXY, Robert. **Teoria de los derechos fundamentalas.** Madrid: Centro de Estúdios Constitucionales, 1993;

Análise técnico-jurídica do "substitutivo" ao projeto de lei para a tipificação de condutas realizadas mediante o uso de ferramentas tecnológicas, ambientes e sistemas informatizados, ou contra estes. São Paulo: Ordem dos Advogados do Brasil - OAB, 2008.

ANDERSON, David.**The aggregate burden of crime**. Journal of Law and Economics, XLI. 1999.

ARAS, Vladimir. **Crimes de informática. Uma nova criminalidade**. Jus Navigandi, Teresina, ano 5, n. 51, out. 2001. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp ?id=2250>. Acesso em: 18 dez. 2007. Disponível em: < http://www.cybercrime.gov/>. Acesso em: 15 dez 2007.

ASCENSÃO, José de Oliveira. **Direito da Internet e da sociedade da informação:** estudos. 1. ed. Rio de Janeiro: Forense, 2002.

Antiviral "Scareware" Just One More Intruder. Disponível em:<http://www.nytimes.com/2008/10/30/ technology/internet/30virus.html?_r=1>. Acesso em: 10 mar 2010.

Bad, bad, cybercrime-friendly ISPs. Disponível em:<http://blogs.zdnet.com/security/?p=2764>. Acesso em:4 mar 2010.

BARBOSA, Fábio. **A eficácia do direito autoral face à sociedade da informação:** uma questão de instrumentalização na obra musical? In: BRASIL. Ministério da Cultura. **Direito Autoral.** Brasília: Ministério da Cultura, Coleção Cadernos de Políticas Culturais, 2006. v. 1.

BARROSO, Luís Roberto. **Interpretação e aplicação da Constituição: fundamentos da dogmática constitucional transformadora.** 6ª ed. ver. Atual. e ampl. São Paulo: Saraiva, 2004;

BECKER, Gary S. Crime and punishment: **An economic approach**. Journal of Political Economy, vol. 1968.

BLANE, John V. **Cybercrime and Cyberterrorism: Current Issues.** Novinka Books, 2003;

BOBBIO, Norberto.**Teoria do Ordenamento Jurídico.** 6ª ed. Brasília: UnB, 1995;

_____. **Estado, governo, sociedade – para uma teoria geral da política,** tradução de Marco Aurélio Nogueira. 9 ed. São Paulo: Paz e Terra, 2001;

BONAVIDES, Paulo. **Curso de direito constitucional**. 19ª ed. atual. São Paulo: Ed. Malheiros, 2006;

BRENNER, Susan W. **Cyberthreats: the emerging fault lines of the nation state**. Estados Unidos da América: Oxford, 2008.

CANOTILHO, J. J. Gomes. **Direito Constitucional**. 7 ed. Coimbra: Almedina, 2003.

CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES (CSIS); GLOBAL ORGANIZED CRIME PROJECT. **Cybercrime Cyberterrorism Cyberwarfare: Averting an Electronic Waterloo (Csis Task Force Report).** Center for Strategic & International Studies, 1998;

CANTU, Javier Livas. **El Estado Cibernetico**: La Unidad Del Derecho, La Politica Y La Economia. Senado de la Republica, 2003.

COLARIK, Andrew M., **Cyber Terrorism: Political and Economic Implications.** Idea Group Publishing, 2006;

Convention on Cybercrime. Disponível em: <http://conventions.coe.int/Treaty/en/ Treaties/Html/185.htm>. Acesso em: 15 dez 2007.

COOK, Philippe. **The demand and supply of criminal opportunities**. Crime and Justice. vol.7. 1986.

Cyberspace policy review: assuring a trusted and resilient information and communications infrastructure. Estados Unidos da América: Casa Branca, 2009.

Crimes na internet rendem mais que tráfico de drogas no Brasil, diz PF**. Disponível em:< http://www1.folha.uol.com.br/folha/informatica/ult124u403907.shtml>. Acesso em: 20 jul 2009.**

DALLARI, Dalmo de Abreu. **Elementos de Teoria Geral do Estado**. São Paulo: Saraiva, 1998.

Design principles & observations of routing behavior. Presentation at the SAHARA Retreat, Bi-annual Meeting, University of California, Berkeley, Networking & System Group, June 2002. Disponível em:<http://sahara.cs.berkeley.edu/jun2002-retreat/chuah_talk.pdf.>. Acesso em: 28 jul 2010.

EETEN, Michel Van; BAUER, Johannes. **Economics of malware: security decisions, incentives and externalities**. Technical report, STI Working Paper, 2008.

EISENBERG, José. **Internet, Democracia e República**. DADOS – Revista de Ciências Sociais, vol. 46, no. 3, Rio de Janeiro: IUPERJ, 2003.

EHRLICH, Isaac. **On the usefulness of controlling individuals: an economic analysis of rehabilitation, incapacitation, and deterrence**. American Economic Review; vol. 71. 1981.

ELDER, Lt Gen Bob**. Mission: Warfighting. Air Force Cyber Operations Co**mmand. United States Air Force, 2007.

ENWEILER, Romano José. **Os desafios de tributar na era da globalização.** Florianópolis: Diploma Legal, 2000.

Examining the impact of website takedown on phishing. Disponível em:< www.cl.cam.ac.uk/~rnc1/ecrime07.pdf> Acesso em: 30 jul 2010.

FALCÃO, Raimundo Bezerra. **Hermenêutica.** São Paulo: Malheiros, 1997;

FARIA, José Eduardo (Org.). **Direitos Humanos, Direitos Sociais e Justiça**. São Paulo: Malheiros, 1994;

FERRAL, Bard R. **Cybercrime, Cyberterrorism, Cyberwarfare: Averting an Electronic Waterloo. An article from: Journal of Criminal Law and Criminology.** Northwestern University, School of Law, 2005;

Following the money: Rogue anti-virus software. Disponível em:< http://voices.washingtonpost.com/ securityfix/2009/07/following_the_money_trail_of_r.html>. Acesso em: 15 jul 2010.

FRIEDMAN, David. **Why not hang them all: the virtues of inefficient punishment**. Journal of Political Economy, vol.107. 1999.

GAROUPA, Nuno. **The economics of organized crime and optimal law enforcement**. Economic Inquiry. vol.38. 2000.

GIANNASI, Maria Júlia. **O profissional da informação diante dos desafios da sociedade atual**. Brasília, 1999. Tese (Doutorado) - Universidade de Brasília, Brasília.

GHRING, Philipp. **Concepts against man-in-the-browser attacks**, 2006.

GLAESER, Edward; SACERDOTE, Bruce; SCHEINKMAN, Jose. **Crime and social interactions**. Quarterly Journal of Economics, 2:507–548, 1996.

GROSSKLAGS, Jens; CHRISTIN, Nicolas; CHUANG, John. **Secure or insure? A game-theoretic analysis of information security games.** World Wide Web Conference (WWW'08). China. 2008.

HÄBERLE, Peter. **Hermenêutica Constitucional – a sociedade aberta dos interpretes da constituição: contribuição para a interpretação pluralista e "procedimental" da constituição.** 1ª ed. Porto Alegre: Sergio Antonio Fabris, 2002;

IC3 2009 Annual Report on Internet Crime Released. Disponível em:<http://www.ic3.gov/media/2010/100312.aspx>. Acesso em: 10 jul 2010.
Identity theft survey report. Disponível em:<http://www.ftc.gov/os/2003/09/synovatereport.pdf>.Acesso em: 05 mai 2010.

In china, $700 puts a spammer in business. Disponível em:<http://www.computerworld.com.au/ article/302617/china_700_puts_spammer_business>. Acesso em: 11 maio 2010.

Interview with John Draper. First episode of stop H*Commerce. Disponível em:<http://www.stophcommerce. com>. Acesso em: 25 jul 2010.

IT Security and crime prevention methods. Interpol, 2000.

ITU Study on the Financial Aspects of Network Security: Malware and Spam. ICT Applications and Cybersecurity Division Policies and Strategies Department. ITU Telecommunication Development Sector. Internation Telecommunication Union, 2008.

ITU Toolkit for cybercrime legislations. ICT Applications and Cybersecurity Division Policies and Strategies Department. ITU Telecommunication Development Sector. Internation Telecommunication Union, 2009.

Israelis Take Over Hamas' TV Station. Disponível em: <http://www.wired.com/dangerroom/2009/01/israelis-take-o/>. Acesso em: 8 nov 2009.

"iWar": A new threat, its convenience – and our increasing vulnerability. Organização do Atlântico Norte - OTAN. Disponível em:<http://www.nato.int/docu/review/2007/issue4/english/analysis2.html>. Acesso em: 29 jul 2009.

HOOFNAGLE, Chris Jay. **Identity theft: Making the known unknowns known**. Journal of Law and Technology, vol. 21, 2007.

HOWARD, Rick. **Cyber Fraud: Tactics Techniques and Procedures**. CRC Press, 2009.

JANCZEWSKI, Lech J.; COLARIK, Andrew M. **Cyber Warfare and Cyber Terrorism.** 1 ed. IGI Global, 2007;

JARDIM, José Maria Jardim. **Arquivos, transparência do estado e capacidade governativa na sociedade da informação**. Disponível em: <www.oas.org/udse/espanol/documentos/1hub11.doc>. Acesso em: 26 set 2009.

KANT, Immanuel. **Fundamentos da Metafísica dos Costumes,** in: **Os Pensadores – Kant (II)**, Trad. Paulo Quintela. São Paulo: Abril Cultural, 1980;

Kevin Poulsen. Superhacker max butler pleads guilty. Disnponível

em:<http://www.wired.com/threatlevel/2009/06/butler_court/>. Acesso em: 25 jul 2009.

Killing the beast ... part II. Disponível em:<http://blog.fireeye.com/research/2009/06/ killing-the-beastpart-ii.html>. Acesso em: 17 jun 2010.

KLANG, Mathias. **Human Rights in the Digital Age.** Routledge Cavendish, 2004;

KOOPS, Bert-Jaap; BRENNER, Susan W. **Cybercrime and Jurisdiction: Volume 11: A global survey.** 1 ed. Asser Press, 2006;

LAKDAWALLA, Darius; ZANJANI, George. **Insurance, self-protection, and the economics of terrorism. Journal of Public Economics**, vol. 89. 2005.

LEWIS, James A. **Cibersecurity - Assessing our vulnerabilites and developing an effective defense**. Estados Unidos da América: Center for strategic and international studies (CSIS), 2009.

LEVY, Pierre. **A emergência do cyberspace e as mutações culturais**. Porto Alegre, 1994. Disponível em: <http://caosmose.net/pierrelevy/aemergen.html>. Acesso em: 20 jul 2010.

LEVY, Pierre. **As tecnologias da inteligência: o futuro do pensamento na era da informática**. 1. ed. Lisboa: Instituto Piaget, 1992

LIMA, Paulo Marco Ferreira. **Crimes de computador e segurança computacional**. Campinas: Millenium, 2008.

Livro verde para a sociedade da informação em Portugal. Lisboa: Ministério da Ciência e da Tecnologia, Missão para a Sociedade da Informação, 1997, p. 5. Disponível em <http://www2.ufp.pt/~lmbg/formacao/lvfinal.pdf>. Acesso em: 09 de abr 2010.

Managing online security risks. Disponível em: <http://www.nytimes.com/library/financial/columns/060100econ-scene.html>. Acesso em: 28 jul 2010.

MARTINEZ, Vinício C. **Estado de Direito Político**. Jus Navigandi, Teresina, a. 8, n. 384, 26 jul. 2004. Disponível em: <http://www1.jus.com.br/doutrina/texto.asp?id=5496>. Acesso em: 04 mar. 2010.

McAfee multipoint strategy to fight cybercrime. Estados Unidos da América:McAfee, 2008.

McAfee Virtual Criminology Report. Estados Unidos da América: McAfee, 2005.

McAfee Virtual Criminology Report. Estados Unidos da América: McAfee, 2006.

McAfee Virtual Criminology Report. Estados Unidos da América: McAfee, 2007.

McAfee Virtual Criminology Report. Estados Unidos da América: McAfee, 2008.

McAfee Virtual Criminology Report. Estados Unidos da América: McAfee, 2009.

MIRANDA, Jorge. **Teoria do estado e da constituição**. Rio de Janeiro: Forense, 2003.

MONTEIRO, Renato Leite; SANTOS, Coriolano. **Estruturas críticas: o próximo alvo**. Disponível em: < http://www2.oabsp.org.br/asp/comissoes/crimes_eletronicos/noticias/proximo_alvo.pdf>. Acesso em: 10 dez 2009.

NEWMAN, John Q. **Identity Theft the cybercrime of the millennium.** Loompanics Unlimited, 1999;

Payment Processor Breach May Be Largest Ever. Disponível em:<http://voices.washingtonpost.com/securityfix/2009/01/payment_processor_breach_may_b.html>. Acesso em: 15 jun 2009.

PINHEIRO, Emeline Piva. **Crimes virtuais: uma análise da criminalidade informática e da resposta estatal**. Disponível em: <http://www.buscalegis.ufsc.br/revistas/index.php/buscalegis/article/viewFile/29397/28953>. Acesso em: 29 jul 2009.

PRADO. Luiz Régis. **Bem jurídico – penal e Constituição.** 2ª ed. rev. e atual. São Paulo: Editora Revista dos Tribunais, 1994;

Quem indicou Índio da Costa foi o Twitter. Disponível em:< http://colunistas.ig.com.br/poderonline/2010/07/04/quem-indicou-indio-da-costa-foi-o-twitter/>. Acesso em: 28 jul 2010.

Online casinos will experience cyber-extortion during SuperBowl betting. Disponível em:<http://www.ibls.com/internet_law_news_portal_view.aspx?id=1967&s=latestnews>. Acesso em: 25 jan 2010.

Redes sociais.br. Disponível em:<http://clickaqui.agenciaclick.com.br/video/redessociaisbr-1>. Acesso em 08 mai 2010.

REICH, Robert. **Supercapitalismo: como o capitalismo tem transformado os negócios, a democracia e o cotidiano**. Rio de Janeiro: Campus, 2008.

RICHARDS, James R. **Transnational Criminal Organizations, Cybercrime, and Money Laundering: A Handbook for Law Enforcement Officers, Auditors, and Financial Investigators.** CRC, 1998;

PINHEIRO. Reginaldo César. **Os Ataques DDoS e os Seus Reflexos no Direito, in Internet Legal – O Direito na Tecnologia da Informação**. Organizador: KAMINSKI, Omar. Ed. Juruá, Curitiba, 2003.

PROGRAMME, Octopus . **Organised Crime in Europe: The Threat of Cybercrime, Situation Report 2004 (Economy and Crime).** Council of Europe, 2005;

Russian business network study. Disponível em:< http://www.bizeul.org/files/RBN_study.pdf>. Acesso em: 10 mar 2010.

SAH, Raaj K. **Social osmosis and patterns of crime**. Journal of Political Economy, vol. 99. 1991.

SARLET, Ingo Wolfgang. **A Eficácia dos direitos fundamentais.** 6ª ed. ver. atual. e ampl. Porto Alegre: Livraria do Advogado Ed., 2006;

_____. **Dignidade da pessoa humana e direitos fundamentais na Constituição Federal de 1988.** 2ª ed. rev. Atual. Porto Alegre: Livraria do Advogado Ed., 2002;

SCHWARZENEGGER, Christian; SUMMERS, Sarah. **The Emergence of EU Criminal Law: Cyber Crime and the Regulation of the Information Society (Studies in International & Comparative Criminal Law).** Hart Pub, 2008;

Security filters often flag legit but infected sites. Disponível em:<http://www.pcworld.com/businesscenter/ article/144485/security_filters_often_flag_legit_but_infected_sites.html>. Acesso em: 10 mar 2010.

Security threat report: 2009. Estados Unidos da América: Sophos, 2009.

SILVESTRE, Paulo. **Crimes digitais fazem mais dinheiro que drogas**. Revista INFO, nov. 2005.
SOBRAL, Carlos Eduardo. **Repressão à crimes cibernéticos**. Ministério da Justiça, Departamento de Polícia Federal, 2008.

SILVA, José Afonso da. **Curso de direito constitucional positivo**. 31 ed. rev. e atual (até a Emenda Constitucional n. 56, de 20.12.2007). São Paulo: Malheiros, 2008.

Simulated attack points to vulnerable U.S. power infrastructure. Disponível em:<http://www.computerworld.com/s/article/9039678/Simulated_attack_points_to_vulnerable_U.S._power_infrastructure>. Acesso em: 20 set 2009.

Social Media Revolution. Disponível em:<http://www.youtube.com/watch?v=sIFYPQjYhv8>. Acesso em: 12 mai 2010.

SORJ, Bernardo. **A democracia inesperada: cidadania, direitos humanos e desigualdade social**. Rio de Janeiro: Jorge Zahar, 2004.

STONE-GROSS, Bret. **Your botnet is my botnet: Analysis of a botnet takeover. Technical Report.** Santa Barbara: University of California, 2009.

Stuxnet renews power grid security concerns. Disponível em: < http://www.computerworld.com/s/article/9179689/Stuxnet_renews_power_grid_security_concerns?taxonomyId=17&pageNumber=2>. Acesso em: 26 jul 2010.

The economics of botnets. Disponível em:<http://www.viruslist.com/en/analysis?pubid=204792068>. Acesso em: 13 jul 2010.

The growing threat to business banking online. Disponível em: <http://voices.washingtonpost.com/securityfix/2009/07/the_pitfalls_of_business_banki.html>. Acesso em: 22 jul 2010.

The National Strategy to Secure Cyberspace. Disponível em: <http://www.dhs.gov/interweb/assetlibrary/National_Cyberspace_Strategy.pdf>. Acesso em: 29 jul 2009

TJX hacker was awash in cash; his penniless coder faces prison. Disponível em: <http://www.wired.com/threatlevel/2009/06/watt>. Acesso em: 15 jun 2009.

TOFFLER, Alvin. **A terceira onda.** Rio de Janeiro: Record, 1997.

Tunis Agenda for the Information Society. Disponível em: <www.itu.int/wsis/index.html>. Acesso em 25 jul 2010.

Underreporting of identity theft rewards the thieves. Gartner Group Research ID: M-20-3244, 2003.

Understanding cybercrime: a guide for developing countries. ICT Applications and Cybersecurity Division Policies and Strategies Department. ITU Telecommunication Development Sector. Internation Telecommunication Union, 2009.

Unsecured Economies - Protecting Vital Information. Disponível em:< http://resources.mcafee.com/content/NAUnsecuredEconomiesReport>. Acesso em: 08 set 2009

YAR, Majid**. Cybercrime and Society.** Sage Publications Ltd, 2006;

WALL, David. **Crime and the Internet.** Routledge, 2001.

Web fraud 2.0: Franchising cyber crime. Disponível em:< http://voices.washingtonpost.com/securityfix/2009/06/web_fraud_20_franchising_cyber.html>. Acesso em: 02 jun 2010.

WESTBY, Jody R. ed., **International Guide to Combating Cybercrime**. American Bar Association, Section of Science & Technology Law, Privacy & Computer Crime Committee, ABA Publishing, 2003.

_____. ed., **International Guide to Cyber Security**. American Bar Association, Section of Science & Technology Law, Privacy & Computer Crime Committee, ABA Publishing, 2004.

_____. ed., **International Guide to Privacy**. American Bar Association, Section of Science & Technology Law, Privacy & Computer Crime Committee, ABA Publishing, 2004.

_____. **ITU Model Cybercrime Law: Project Overview.** ICT Applications and Cybersecurity Division. Policies and Strategies Department, BDT International Telecommunication Union, 2007.

_____. **ITU Toolkit for Cybercrime Cybercrime Legislation**. International Telecommunication Union, 2008.

WMF exploit sold underground for $4,000. Disponível em: <http://www.eweek.com/c/a/Security/Researcher-WMF-Exploit-Sold-Underground-for-4000>. Acesso em: 02 mar 2010.

APÊNDICE 01 - Portaria 34 do Conselho de Defesa Nacional

DECRETO Nº 6.924, DE 5 DE AGOSTO DE 2009

Institui o Prêmio de "Boas Práticas na Aplicação, Divulgação ou Implementação da Lei Maria da Penha".

O PRESIDENTE DA REPÚBLICA, no uso da atribuição que lhe confere o art. 84, inciso VI, alínea "a", da Constituição,

D E C R E T A :

Art. 1º Fica instituído o Prêmio de "Boas Práticas na Aplicação, Divulgação ou Implementação da Lei Maria da Penha", a ser concedido, anualmente, pelo Governo Federal às pessoas físicas ou jurídicas cujos trabalhos ou atuação mereçam especial destaque no enfrentamento à violência doméstica e familiar contra a mulher, com base na Lei Maria da Penha.

Art. 2º A Secretaria Especial de Políticas para as Mulheres da Presidência da República publicará as instruções necessárias para a concessão do Prêmio de "Boas Práticas na Aplicação, Divulgação ou Implementação da Lei Maria da Penha", no prazo de trinta dias contados da publicação deste Decreto.

Art. 3º Este Decreto entra em vigor na data de sua publicação.

Brasília, 5 de agosto de 2009; 188º da Independência e 121º da República.

LUIZ INÁCIO LULA DA SILVA
Dilma Rousseff

Presidência da República

CASA CIVIL
INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO

DESPACHO DO DIRETOR-PRESIDENTE

Entidade: AR SERPRO, vinculada à AC SERPRO RFB.
Processo nº.: 00100.000016/2003-45

Acolhe-se o Parecer AUDIT-ITI 105/2009 que opina pelo deferimento do pedido de credenciamento de novas Instalações Técnicas da AR SERPRO vinculada à AC SERPRO RFB, localizadas na Rua de Laranjeiras, 57, Centro, Aracajú - SE e Rua Olívia Guedes Penteado, 941, Capela do Socorro, São Paulo - SP, com Políticas de Certificados de Assinatura Digital Tipo PC SERPRORFB A1 e PC SERPRORFB A3 para pessoas físicas e jurídicas. Em vista disso, e consoante com o disposto no item 3.2.1, do DOC-ICP-03, defere-se o credenciamento. Publique-se. Em 5 de agosto de 2009.

PEDRO PAULO LEMOS MACHADO
Substituto

GABINETE DE SEGURANÇA INSTITUCIONAL

PORTARIA Nº 36, DE 5 DE AGOSTO DE 2009

Disciplina, no âmbito da Agência Brasileira de Inteligência - ABIN, a utilização do Cartão de Pagamento do Governo Federal - CPGF para suprimento de fundos de caráter ostensivo na modalidade de saque.

O MINISTRO DE ESTADO CHEFE DO GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA, no uso das atribuições que lhe conferem os incisos I e II do parágrafo único do art. 87 da Constituição e considerando o disposto na Lei nº 9.883, de 7 de dezembro de 1999, nos arts. 1º e 6º da Lei nº 10.683, de 28 de maio de 2003, no Regimento Interno da ABIN e nos incisos I e II do § 6º do art. 45 do Decreto nº 93.872, de 23 de dezembro de 1986, resolve:

Art. 1º Fica autorizada no âmbito da Agência Brasileira de Inteligência - ABIN, a utilização do Cartão de Pagamento do Governo Federal - CPGF para suprimento de fundos de caráter ostensivo na modalidade de saque, até o limite máximo de trinta por cento do total da despesa anual do órgão efetuada com suprimento de fundos.

Art. 2º A utilização do CPGF ficará restrita ao pagamento de despesas eventuais e de pequeno vulto, conforme disposto na legislação, efetuadas por todas as unidades e frações da estrutura organizacional da ABIN.

§ 1º O previsto no **caput** se aplicará ao pagamento de despesas com:

I - prestadores de serviços, pessoas físicas e jurídicas;

II - material de consumo, inclusive combustíveis, lubrificantes e cópias reprográficas, quando o fornecimento não for contemplado por contrato específico;

III - estacionamento, pedágios e tarifas eventuais e obrigatórias; e

IV - fornecimento eventual de alimentação e gêneros alimentícios, quando não for contemplado por contrato específico.

§ 2º Em situações excepcionais, outras despesas não previstas no § 1º poderão ser pagas, a critério do Secretário de Planejamento, Orçamento e Administração da ABIN e autorizadas pelo ordenador de despesas da Agência.

Art. 3º O servidor suprido na forma do art. 1º prestará contas da aplicação dos recursos e justificará quanto à impossibilidade de realização do pagamento via Cartão de Pagamento do Governo Federal - CPGF, observado o prazo estabelecido pelo ordenador de despesas.

Art. 4º Esta Portaria entra em vigor na data de sua publicação.

JORGE ARMANDO FELIX

DESPACHO DO CHEFE
Em 5 de agosto de 2009

O MINISTRO DE ESTADO CHEFE DO GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA assinou a Portaria nº 030 - GSIPR/CH/ABIN, de 05 de agosto de 2009, alterando o Art 5º da Portaria nº 037 - GSIPR/CH/ABIN, de 17 de outubro de 2008, que aprovou o Regimento Interno da Agência Brasileira de Inteligência - ABIN.

Publicado de acordo com o Art. 9º da Lei nº 9.883, de 07 de dezembro de 1999.

JORGE ARMANDO FELIX

ADVOCACIA-GERAL DA UNIÃO
PROCURADORIA-GERAL FEDERAL
SUBPROCURADORIA-GERAL FEDERAL

PORTARIA Nº 768, DE 5 DE AGOSTO DE 2009

Atribui à Procuradoria Regional Federal da 5ª Região as competências que especifica e dá outras providências.

O **SUBPROCURADOR-GERAL FEDERAL**, no uso da atribuição que lhe foi delegada pelo Procurador-Geral Federal, nos termos da Portaria PGF nº 200, de 25 de fevereiro de 2008, resolve:

Art. 1º Atribuir à Procuradoria Regional Federal da 5ª Região, observada a sua competência territorial:

I - a representação judicial e as atividades de consultoria jurídica da Superintendência do Desenvolvimento do Nordeste - SUDENE, a partir de 3 de agosto de 2009;

II - a representação judicial do Departamento Nacional de Infraestrutura de Transportes - DNIT e da Universidade Federal de Pernambuco - UFPE, a partir de 10 de agosto de 2009.

Art. 2º A Procuradoria Federal junto à Superintendência do Desenvolvimento do Nordeste - SUDENE permanecerá responsável pelas atividades de assessoramento jurídico da autarquia.

Art. 3º A Procuradoria Regional Federal da 5ª Região e a Procuradoria Federal junto à Superintendência do Desenvolvimento do Nordeste - SUDENE prestarão colaboração mútua, sob a coordenação do titular da primeira.

Art. 4º Esta Portaria entra em vigor na data de sua publicação, convalidando-se os atos anteriormente praticados.

MARCELO DA SILVA FREITAS

CONSELHO DE DEFESA NACIONAL
SECRETARIA EXECUTIVA

PORTARIA Nº 34, DE 5 DE AGOSTO DE 2009

Institui Grupo de Trabalho de Segurança das Infraestruturas Críticas da Informação, no âmbito do Comitê Gestor de Segurança da Informação - CGSI.

O MINISTRO DE ESTADO CHEFE DO GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA, na condição de **SECRETÁRIO-EXECUTIVO DO CONSELHO DE DEFESA NACIONAL**, no uso de suas atribuições, tendo em vista o disposto no art. 4º do Decreto nº 3.505, de 13 de junho de 2000, e **CONSIDERANDO**:

as Infraestruturas Críticas como sendo as instalações, serviços, bens e sistemas que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade;

a necessidade de assegurar dentro do espaço cibernético ações de segurança da informação como fundamentais para garantir disponibilidade, integridade, confidencialidade e autenticidade da informação e comunicações no âmbito da Administração Pública Federal, direta e indireta;

a possibilidade real de uso dos meios computacionais para ações ofensivas através da penetração nas redes de computadores de alvos estratégicos; e

o ataque cibernético como sendo uma das maiores ameaças mundiais na atualidade,

RESOLVE:

Art. 1º Instituir, no âmbito do Comitê Gestor de Segurança da Informação - CGSI, um Grupo de Trabalho para estudo e análise de matérias relacionadas à Segurança de Infraestruturas Críticas da Informação.

Art. 2º Para fins desta Portaria consideram-se Infraestruturas Críticas da Informação o subconjunto de ativos de informação que afetam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade.

Parágrafo único. Consideram-se ativos de informação os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.

Art. 3º O Grupo de Trabalho será integrado por representantes, titular e suplente, de cada um dos seguintes órgãos:

I- Gabinete de Segurança Institucional da Presidência da República, que o coordenará por intermédio do Departamento de Segurança da Informação e Comunicações;

II- Casa Civil da Presidência da República;

III- Ministério da Defesa;

IV- Ministério da Saúde;

V- Ministério da Ciência e Tecnologia;

VI- Ministério do Planejamento, Orçamento e Gestão;

VII- Ministério das Relações Exteriores;

VIII- Banco Central do Brasil;

IX- Banco do Brasil;

X- Caixa Econômica Federal;

XI- SERPRO;

XII- PETROBRAS; e

XIII- DATAPREV.

Parágrafo único. O Comitê Gestor de Segurança da Informação indicará, dentre os seus integrantes, o relator do Grupo de Trabalho.

Art. 4º Os integrantes do Grupo de Trabalho serão indicados pelos dirigentes máximos dos órgãos referidos no artigo 3º, no prazo de até trinta dias, a partir da data de publicação desta Portaria.

Parágrafo único. A indicação dos representantes de que trata o ***caput*** deverá atender o perfil técnico necessário.

Art. 5º O Grupo de Trabalho será instalado no prazo de até quinze dias após a indicação de seus integrantes.

Art. 6º São atribuições do Grupo de Trabalho, além de outras julgadas relevantes e pertinentes:

I - levantar e avaliar as potenciais vulnerabilidades e riscos que possam afetar a Segurança de Infraestruturas Críticas da Informação, identificada a sua interdependência;

II - propor, articular e acompanhar medidas necessárias à Segurança de Infraestruturas Críticas da Informação;

III - estudar, propor e acompanhar a implementação de um sistema de informações que conterá dados atualizados de Infraestruturas Críticas da Informação, para apoio a decisões; e

IV - pesquisar e propor um método de identificação de alertas e ameaças da Segurança de Infraestruturas Críticas da Informação.

Art. 7º O Grupo de Trabalho reunir-se-á de forma ordinária uma vez por mês e, extraordinariamente, quando convocado por seu Coordenador.

Art. 8º O Grupo de Trabalho poderá interagir com outros órgãos para consulta e adoção de providências necessárias à complementação das atividades atribuídas por esta Portaria.

Art. 9º Poderão ser convidados a participar do Grupo de Trabalho, a juízo de sua coordenação ou por representantes por ela indicados, técnicos e especialistas dos demais órgãos e entidades integrantes da Administração Pública Federal, direta e indireta, bem como da academia e da iniciativa privada.

Art. 10. O Grupo de Trabalho poderá, submetida à aprovação do Comitê Gestor de Segurança da Informação - CGSI, criar subgrupos de trabalho para deliberar sobre assuntos específicos.

Art. 11. As medidas e ações necessárias serão relatadas ao Comitê Gestor de Segurança da Informação - CGSI, por intermédio do Coordenador do Grupo de Trabalho.

Art. 12. A participação no Grupo de Trabalho de que trata esta Portaria será considerada de relevante interesse público e não remunerada.

Art. 13. Caberá ao Gabinete de Segurança Institucional da Presidência da República, por intermédio do Departamento de Segurança da Informação e Comunicações, prover o apoio administrativo e os meios necessários para o cumprimento desta Portaria.

Art. 14. Esta Portaria entra em vigor na data de sua publicação.

JORGE ARMANDO FELIX

APÊNDICE 02 - Portaria 59 do Conselho de Defesa Nacional

SECRETARIA EXECUTIVA

PORTARIA Nº 283, DE 10 DE NOVEMBRO DE 2009

O SECRETÁRIO-EXECUTIVO DO GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA, no uso da subdelegação de competência que lhe foi conferida pelo art. 1º da Portaria nº 9 - GSIPR/CH, de 13 de fevereiro de 2009, resolve

DISPENSAR

o ST BMDF JOSÉ NASCIMENTO SOARES de exercer a função de ASSISTENTE - GR.IV no Departamento de Segurança da Secretaria-Executiva do Gabinete de Segurança Institucional da Presidência da República, a partir de 09 de novembro de 2009.

JOÃO ROBERTO DE OLIVEIRA

ADVOCACIA-GERAL DA UNIÃO

PORTARIA Nº 1.620, DE 10 DE NOVEMBRO DE 2009

O **ADVOGADO-GERAL DA UNIÃO**, no uso das atribuições que lhe conferem os incisos I e XVIII do art. 4º da Lei Complementar nº 73, de 10 de fevereiro de 1993, resolve

NOMEAR

DÉBORA CRISTINA DE CARVALHO RODRIGUES para exercer o cargo em comissão de Chefe de Serviço, código DAS 101.1, da Coordenação-Geral de Recursos Humanos da Diretoria de Recursos Humanos e Tecnologia da Informação, da Secretaria-Geral da Advocacia-Geral da União.

LUÍS INÁCIO LUCENA ADAMS

PROCURADORIA-GERAL FEDERAL

PORTARIA CONJUNTA Nº 184, DE 9 DE NOVEMBRO DE 2009

O **PROCURADOR-GERAL FEDERAL** e o **PRESIDENTE DO INSTITUTO BRASILEIRO DO MEIO AMBIENTE E DOS RECURSOS NATURAIS RENOVÁVEIS - IBAMA,** no uso da competência de que trata o inciso VI do § 2º do art. 11 da Lei nº 10.480, de 2 de julho de 2002, e o disposto no art. 143 da Lei nº 8.112, de 11 de dezembro de 1990, resolvem:

Art. 1º Reconduzir a comissão Processante designada pela Portaria Conjunta nº 8, de 29 de janeiro de 2009, publicada no Diário Oficial da União de 30 de janeiro de 2009, prorrogada pela Portaria Conjunta nº 52, de 28 de abril de 2009, publicada no Diário Oficial da União de 4 de maio de 2009, reconduzida pela Portaria Conjunta nº 93, de 30 de julho de 2009, publicada no Diário Oficial da União de 3 de agosto de 2009, reconduzida pela Portaria Conjunta nº 109, de 1 de setembro de 2009, publicada no Diário Oficial da União de 3 de setembro de 2009, e designar o servidor AURO NEUBAUER, Matrícula SIAPE nº 1365424, para, em substituição ao servidor WILLIS GOMES DE ALARCÃO, Matrícula SIAPE nº 0679704 integrar a Comissão de Processo Administrativo Disciplinar, visando a prosseguir na apuração dos fatos apontados nos autos do Processo Administrativo nº 00407.003988/2008-51 e seus apensos, bem como os fatos conexos.

Art. 2º A Comissão terá o prazo de 60 (sessenta) dias para ultimar os trabalhos apuratórios.

Art. 3º Esta Portaria entra em vigor na data de sua publicação, convalidando-se os atos praticados posteriormente ao término da vigência da Portaria Conjunta nº 109, de 1 de setembro de 2009.

MARCELO DE SIQUEIRA FREITAS
Procurador-Geral Federal

ROBERTO MESSIAS FRANCO
Presidente do IBAMA

SECRETARIA-GERAL

PORTARIA Nº 340, DE 3 DE NOVEMBRO DE 2009

O **SECRETÁRIO-GERAL DA ADVOCACIA-GERAL DA UNIÃO**, no uso da competência que lhe foi delegada pela Portaria nº 611, de 16 de agosto de 2002, do Advogado-Geral da União, e tendo em vista o que consta do Processo nº 00460.004266/2009-51, resolve

Conceder aposentadoria voluntária a RAIMUNDO NONATO SANTOS PEREIRA, matrícula SIAPE nº 6174751, ocupante do cargo de Agente Administrativo, Classe S, Padrão III, código da vaga 75543, do Quadro de Pessoal da Advocacia-Geral da União, com fundamento no art. 3º, incisos I, II e III, parágrafo único, da Emenda Constitucional nº 47, de 5 de julho de 2005, combinado com o § 1º do art. 40 da Constituição Federal, com paridade e proventos integrais correspondentes ao vencimento básico do cargo efetivo, acrescido dos anuênios, de acordo com o art. 67 da Lei nº 8.112, de 11 de dezembro de 1990, combinado com art. 15 da Medida Provisória nº 2.225-45, de 4 de setembro de 2001, e Ofício Circular nº 36/SRH/MP 2001, das Gratificações de Desempenho de Atividade de Apoio Técnico-Administrativo, Lei nº 10.480, de 2 de julho de 2002, da Específica de Apoio Técnico Administrativo, Lei nº 10.907, 15 de julho de 2004, e da vantagem prevista no art. 3º da Lei nº 8.911, de 11 de julho de 1994, assegurada pelo art. 15, § 2º da Lei nº 9.527, de 10 de dezembro de 1997, declarando, em decorrência, a vacância do cargo acima mencionado.

ROMEU COSTA RIBEIRO BASTOS

CONTROLADORIA-GERAL DA UNIÃO
SECRETARIA EXECUTIVA
DIRETORIA DE GESTÃO INTERNA

PORTARIAS DE 10 DE NOVEMBRO DE 2009

O **DIRETOR DE GESTÃO INTERNA DA CONTROLADORIA-GERAL DA UNIÃO**, no uso da competência que lhe foi subdelegada pela Portaria CGU n.º 1.566, de 25 de outubro de 2007, publicada no DOU do dia 26 subsequente, e com o disposto no Processo n.º 00190.058120/2009-36, resolve:

Nº 2.317 - Declarar vago o cargo de Analista de Finanças e Controle ocupado pelo servidor ANDRÉ NASCIMENTO BARBOSA, matrícula SIAPE n.º 1658278, Classe A, Padrão I, a contar de 28 de outubro de 2009, em virtude de posse em outro cargo inacumulável no Senado Federal.

O **DIRETOR DE GESTÃO INTERNA DA CONTROLADORIA-GERAL DA UNIÃO**, no uso da competência que lhe foi subdelegada pela Portaria CGU nº 1.566, de 25 de outubro de 2007, publicada no DOU de 26 subsequente e tendo em vista o que consta no Processo nº 00206.000868/2009-40, resolve:

Nº 2.318 - Conceder, Pensão Civil vitalícia à ROSILANDE DE SOUZA SANTOS OLIVEIRA, e temporária a JENNIFER DE SOUZA SANTOS, PEDRO ALVES DE SOUSA JÚNIOR, ROSIMEIRE DOS SANTOS ALVES, PATRÍCIA DOS SANTOS ALVES e CARLOS JOHNNY DE SOUZA SANTOS, respectivamente viúva e enteados do ex-servidor ROGÉRIO FIRMINO DE OLIVEIRA, ex-ocupante do cargo de Técnico de Finanças e Controle, Classe S, Padrão IV, matrícula SIAPE nº 0117357, do quadro de pessoal permanente da Controladoria-Geral da União, com fundamento no art. 40, § 7º, inciso II, da Constituição Federal, com a redação dada pela Emenda Constitucional nº 41, de 19.12.2003, publicada no Diário Oficial da União de 31.12.2003, c/c art. 2º, inciso II, da Lei nº 10.887, de 18.06.2004 e com os artigos 216 e 217, inciso I, alínea "a", e inciso II, alínea "a" da Lei nº 8.112/90, com vigência a partir de 18 de setembro de 2009, data do óbito do instituidor.

Declarar vago o referido cargo.

O **DIRETOR DE GESTÃO INTERNA DA CONTROLADORIA-GERAL DA UNIÃO**, no uso da competência que lhe foi delegada pela Portaria CGU nº 1.566, de 25 de outubro de 2007, e tendo em vista o que consta no Processo nº 00190.038011/2009-19, resolve:

Nº 2.319 - Conceder aposentadoria voluntária com proventos integrais ao servidor AHIRTON PONTES VIEIRA, matrícula SIAPE nº 0093068, ocupante do cargo de Técnico de Finanças e Controle, Classe S, Padrão IV, do Quadro de Pessoal desta Controladoria-Geral da União, com fundamento no artigo 3º da Emenda Constitucional nº 47/2005.

Declarar vago o referido cargo.

O **DIRETOR DE GESTÃO INTERNA DA CONTROLADORIA-GERAL DA UNIÃO**, no uso da competência que lhe foi subdelegada pela Portaria CGU nº 1.566, de 25 de outubro de 2007, e tendo em vista o que consta no Processo nº 00217.000123/2008-71, resolve:

Nº 2.320 - Aposentar, por invalidez permanente, o servidor CARLOS FERNANDO ANZOATEGUI, ocupante do cargo efetivo de Analista de Finanças e Controle, matrícula SIAPE nº 1055908, Classe S, Padrão IV, do Quadro de Pessoal da Controladoria-Geral da União, com fundamento no artigo 40, § 1º, inciso I da Constituição Federal/1988, com redação dada pela Emenda Constitucional nº 41, de 19 de dezembro de 2003, publicada no Diário Oficial da União de 31 de dezembro de 2003 e no artigo 186, § 1º da Lei nº 8.112, de 11 de dezembro de 1990.

Declarar vago o referido cargo.

O **DIRETOR DE GESTÃO INTERNA DA CONTROLADORIA-GERAL DA UNIÃO**, no uso da competência que lhe foi delegada pela Portaria CGU nº 1.566, de 25 de outubro de 2007, e tendo em vista o que consta no Processo nº 00224.000106/2008-44, resolve:

Nº 2.321 - Conceder aposentadoria voluntária com proventos integrais ao servidor JORGE MOTA CÂMARA, matrícula SIAPE nº 0093431, ocupante do cargo de Técnico de Finanças e Controle, Classe S, Padrão IV, do Quadro de Pessoal desta Controladoria-Geral da União, com fundamento no artigo 3º da Emenda Constitucional nº 47/2005.

Declarar vago o referido cargo.

CLÁUDIO TORQUATO DA SILVA

CONSELHO DE DEFESA NACIONAL
SECRETARIA EXECUTIVA

PORTARIAS DE 10 DE NOVEMBRO DE 2009

O **MINISTRO DE ESTADO CHEFE DO GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA**, na condição de **SECRETÁRIO-EXECUTIVO DO CONSELHO DE DEFESA NACIONAL**, no uso de suas atribuições, tendo em vista o disposto no art. 6º e no art. 7º do Decreto Nº 3.505, de 13 de junho de 2000, resolve:

Nº 58 - Art. 1º Designar os membros do Grupo de Trabalho de Criptografia, instituído pela Portaria nº 35, publicada no DOU Nº 150 - Seção 1, de 7 de agosto de 2009, integrado por representantes dos seguintes órgãos:

ÓRGÃO	REPRESENTANTES
GSIPR/DSIC	Raphael Mandarino Junior (titular) Gerson Charbel Costa (suplente)
GSIPR/ABIN	Ricardo Moxor Gonçalves de Morais (titular) José Antônio Carnaz Barbosa (suplente)
Casa Civil da Presidência da República/ITI	Renato da Silveira Martini (titular) André Machado Cancelli (suplente)
Ministério da Defesa	Coronel Inf Aer Inneu José de Oliveira (FAB) (titular) Major-Aviador Cláudio Ramos da Cruz (FAB) (suplente) Capitão-de-Fragata Valter Monteiro Junior (MD) (suplente) Coronel R1 Rily Mello (EB) (suplente) Major Fernando César Castaño Mantilo (EB) (suplente)
Ministério da Justiça	Jonilson da Silva Rodrigues (titular) Marconi Mizuno (suplente)
Ministério das Relações Exteriores	Celso Ricardo Hotturn (titular) Filipe Carneiro Guimarães (suplente)
Ministério das Comunicações	César de Souza Ribeiro (titular) Wagner Santilli (suplente)
Ministério do Desenvolvimento, Indústria e Comércio Exterior	Eduardo Roberto de Souza Trindade (titular) José Luiz de Carvalho (suplente)
Ministério da Ciência e Tecnologia	Eduardo Viola (titular) Suzana de Queiroz Ramos Teixeira (suplente)
Ministério da Fazenda	Odilon Neves Junior (titular) Josenilson Torres Veras (suplente)
Advocacia Geral da União	Paulo Fernando Aires de Albuquerque Filho (titular) Mônica Costa Tkaczyk Marinaj (suplente)
Agência Nacional de Telecomunicações	Túlio Márcio Peres Barbosa (titular) Fausto Luiz Jorge Pádua (suplente)

Art. 2º Os trabalhos do Grupo serão coordenados pelo representante do Gabinete de Segurança Institucional.

Art. 3º Esta Portaria entra em vigor na data de sua publicação.

O **MINISTRO DE ESTADO CHEFE DO GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA**, na condição de **SECRETÁRIO-EXECUTIVO DO CONSELHO DE DEFESA NACIONAL**, no uso de suas atribuições, tendo em vista o disposto no art. 6º e no art. 7º do Decreto Nº 05, de 13 de junho de 2000, resolve:

Nº 59 - Art. 1º Designar os membros do Grupo de Trabalho de Segurança das Infraestruturas Críticas da Informação, instituído pela Portaria nº 34, publicada no DOU Nº 149 - Seção 1, de 6 de agosto de 2009, integrado por representantes dos seguintes órgãos:

ÓRGÃO	REPRESENTANTES
GSIPR/DSIC	Raphael Mandarino Junior (titular) Claudia Lyra Canongia (suplente)
Casa Civil da Presidência da República	Renato da Silveira Martini (titular) Pedro Paulo Lemos de Machado (suplente)
Ministério da Defesa	Capitão-de-Fragata (FN) Alexandre Mariano Feitosa (titular) Capitão-de-Fragata Ricardo Brigatto Salvatore (MB) (suplente) Major Rodolfo Tristão Pina (EB) (suplente) Ten Cel Eduardo Rebouças dos Anjos (EB) (suplente) 1º Tenente Eng. André Luiz Corrêa (FAB) (suplente)
Ministério das Relações Exteriores	Filipe Carneiro Guimarães (titular) Celso Ricardo Hotturn (suplente)
Ministério da Saúde	Milson Henriques de Oliveira (titular) Adelino Fernando de Souza Correia (suplente)
Ministério do Planejamento, Orçamento e Gestão	Rogério Santanna dos Santos (titular) Antônio Carlos Alff (suplente)
Ministério da Ciência e Tecnologia	Eduardo Viola (titular) Suzana de Queiroz Ramos Teixeira (suplente)
Banco Central do Brasil	Paulo Roberto Alves de Carvalho (titular) Amilcar Francisco Faria (suplente)
Banco do Brasil	Mônica Luciana Martins de Oliveira (titular) Francisco Diey Brito (suplente)
Caixa Econômica Federal	Alexandre Costa Guindani (titular) Argemiro Soares de Souza Júnior (suplente)
SERPRO	Gleyner Martins Novaes (titular) Marcos Allemand Lopes (suplente)
PETROBRAS	Bernadete Soares da Cunha de Castilho (titular) Murilo Sergio de Farias Felix (suplente)
DATAPREV	Humberto Degrazia Campedelli (titular) Joel Jurandir Ferreira Correa (suplente)

Art. 2º Os trabalhos do Grupo serão coordenados pelo representante do Gabinete de Segurança Institucional.

Art. 3º Esta Portaria entra em vigor na data de sua publicação.

JORGE ARMANDO FELIX

SECRETARIA DE COMUNICAÇÃO SOCIAL

PORTARIA Nº 103, DE 10 DE NOVEMBRO DE 2009

O **MINISTRO DE ESTADO CHEFE DA SECRETARIA DE COMUNICAÇÃO SOCIAL DA PRESIDÊNCIA DA REPÚBLICA,** interino, no uso da competência que lhe foi delegada pelo Decreto nº 6.216, de 4 de outubro de 2007 e tendo em vista a Portaria nº 1.056, de 11 de junho de 2003, do Ministro de Estado Chefe da Casa Civil da Presidência da República, resolve

NOMEAR

MÁRCIO SOUZA DATTOLI, para exercer o cargo de Assistente no Departamento de Mídia da Secretaria de Comunicação Integrada desta Secretaria, código DAS 102.2.

OTTONI FERNANDES JR.

EMPRESA BRASIL DE COMUNICAÇÃO S.A.

DESPACHOS DA DIRETORA-PRESIDENTE
Em 5 de novembro de 2009

A **DIRETORA-PRESIDENTE DA EMPRESA BRASIL DE COMUNICAÇÃO S.A. - EBC**, no uso da competência que lhe foi delegada pela Portaria Ministerial SECOM/PR nº 40, de 30 de abril de 2009, resolve autorizar o afastamento do país dos empregados da Empresa Brasil de Comunicação S.A. - EBC abaixo, para os fins que especifica:

DELORGEL VALDIR KAISER, Gerente Executivo da Diretoria de Serviços, para a cidade de Buenos Aires/Argentina, no período de 09 a 11 de novembro de 2009, que realizará viagem a serviço da empresa para participar do Seminário de TV Educativa e Convergência Digital, Programação Integral do X Encontro Internacional Virtual Educa Argentina 2009, incluído o trânsito, com ônus. (Processo nº 2911/2009).

JOSÉ DONIZETE DE LIMA, Repórter, FÁBIO RODRIGUES GONÇALVES DAMASCENO, Repórter Cinematográfico, para a cidade de Tegucigalpa/Honduras, no período de 09 a 23 de novembro de 2009, que realizará cobertura jornalística do retorno a Honduras, do Presidente deposto Sr. José Manuel Zelaya Rosales, naquele país, incluído o trânsito, com ônus. (Processo nº 2913/2009).

ROGÉRIO ALVES DA SILVA, Técnico de Televisão, MAURÍCIO ERNANY AGUIAR, Técnico de Agência/Rádio, RONAN CÂNDIDO GOMES, Auxiliar do Cinegrafista Oficial, LUCIANA COLLARES HOLANDA, Repórter de Televisão, no período de 11 a 16 de novembro de 2009; ERICARLOS DE JESUS BARBOSA FRANCISCO, Cinegrafista Oficial, no período de 14 a 16 de novembro de 2009; AMANDA MACHADO CIEGLINSKI, Repórter da Agência Brasil, GILVAN ALVES DA ROCHA, Cinegrafista da TV Brasil, no período de 13 a 18 de novembro de 2009, todos para a cidade de Roma/Itália, que realizarão viagem à cobertura jornalística da viagem oficial do Exmo. Senhor Presidente da República, LUIZ INÁCIO LULA DA SILVA, onde participará da reunião da III Cimeira Mundial de Chefes de Estado e de Governo sobre a Segurança Alimentar da FAO, incluído o trânsito, com ônus. (Processo nº 2914/2009).

MARIA TEREZA CRUVINEL

SECRETARIA ESPECIAL DE PORTOS
COMPANHIA DOCAS DO PARÁ

RESOLUÇÃO Nº 246, DE 10 DE NOVEMBRO DE 2009

O **DIRETOR PRESIDENTE DA COMPANHIA DOCAS DO PARÁ (CDP)**, no uso de suas atribuições legais, e CONSIDERANDO a necessidade da aplicação de Licitação, na modalidade Pregão Eletrônico, Pregão Eletrônico para Registro de Preço no módulo SIASG, bem como, homologação de cotação eletrônica e dos procedimentos licitatórios no módulo SIASGNET, conforme o disposto na Lei nº 10.520/2002, de 17.07.2002, regulamentada pelo Decreto nº 5.450, de 31.05.2005 e demais vigentes, RESOLVE: 1- designar o empregado relacionado abaixo, como agente responsável pelo Pregão Eletrônico, Pregão Eletrônico para Registro de Preço no módulo SIASG, procedimentos licitatórios no módulo SIASGNET e demais meios disponíveis no COMPRASNET, na figura de AUTORIDADE HOMOLOGADORA, conforme identificação no sistema: Código da UASG: 399005/Secretaria Especial de Portos - SEP/ Companhia Docas do Pará - CDP, para o período de 01 (um) ano.

- Autoridade Homologadora:

- OLIVIO ANTONIO PALHETA GOMES
CPF/MF: 259.413.132 - 68

CLYTHIO VAN BUGGENHOUT

Ministério da Agricultura, Pecuária e Abastecimento

GABINETE DO MINISTRO

PORTARIAS DE 10 DE NOVEMBRO DE 2009

O MINISTRO DE ESTADO DA AGRICULTURA, PECUÁRIA E ABASTECIMENTO, no uso da competência que lhe foi subdelegada pelo art. 1º, inciso I, da Portaria nº 1.056, de 11 de junho de 2003, do Ministro de Estado Chefe da Casa Civil da Presidência da República, resolve:

Nº 924 - Nomear MARICÉLIA NUNES GOMES, matrícula SIAPE nº 6027661, ocupante do cargo de Agente Administrativo, classe S, padrão III, do Quadro de Pessoal deste Ministério, para exercer o cargo em comissão de Chefe do Serviço de Administração de Almoxarifado, código DAS 101.1, da Coordenação de Administração de Material e Patrimônio, da Coordenação-Geral de Logística e Serviços Gerais, da Subsecretaria de Planejamento, Orçamento e Administração, da Secretaria-Executiva, de que tratam os Decretos nºs 5.351, de 21 de janeiro de 2005, e 6.348, de 8 de janeiro de 2008, ficando dispensada da função que atualmente ocupa.

O MINISTRO DE ESTADO DA AGRICULTURA, PECUÁRIA E ABASTECIMENTO, no uso da competência que lhe foi subdelegada pelo art. 1º, inciso I, da Portaria nº 1.056, de 11 de junho de 2003, do Ministro de Estado Chefe da Casa Civil da Presidência da República, e tendo em vista o disposto no art. 38 da Lei nº 8.112, de 11 de dezembro de 1990, com a redação dada pela Lei nº 9.527, de 10 de dezembro de 1997, resolve

Nº 925 - Dispensar, a partir de 10 de novembro de 2009, ISABEL REGINA FLORES CARNEIRO ROXO, matrícula SIAPE nº 127476, ocupante do cargo de Assistente Administrativo, classe C, padrão 001, da Tabela Celetista deste Ministério, do encargo de Substituta do Chefe do Serviço de Acompanhamento Setorial, código DAS 101.1, da Coordenação-Geral de Planejamento e Estratégias, do Departamento do Café, da Secretaria de Produção e Agroenergia, de que tratam os Decretos nºs 5.351, de 21 de janeiro de 2005, e 6.348, de 8 de janeiro de 2008.

O MINISTRO DE ESTADO DA AGRICULTURA, PECUÁRIA E ABASTECIMENTO, no uso da competência que lhe foi delegada pelo artigo 7º, do Decreto nº 4.941, de 29 de dezembro de 2003, resolve:

Nº 926 - Dispensar SELMA DE FARIA GONÇALVES, matrícula SIAPE nº 4865, do Quadro de Pessoal deste Ministério, da Função Comissionada Técnica de Técnico em Gestão Administrativa IV, código FCT-15, da Superintendência Federal de Agricultura, Pecuária e Abastecimento no Estado de Goiás.

Nº 927 - Designar ALEXANDRE REIS COUTINHO, matrícula SIAPE nº 6004894, do Quadro de Pessoal deste Ministério, para exercer a Função Comissionada Técnica de Técnico em Gestão Administrativa IV, código FCT-15, da Superintendência Federal de Agricultura, Pecuária e Abastecimento no Estado de Goiás.

REINHOLD STEPHANES

DESPACHOS DO MINISTRO
Em 10 de novembro de 2009

O MINISTRO DE ESTADO DA AGRICULTURA, PECUÁRIA E ABASTECIMENTO, no uso da competência que lhe foi delegada pelo Decreto nº 1.367, de 7 de fevereiro de 1995, autoriza o(a) Fiscal Federal Agropecuário MARIANA DE SOUZA E SILVA DA COSTA TEIXEIRA, do Quadro Permanente deste Ministério, lotado no(a) Secretaria de Defesa Agropecuária - SDA, a afastar-se do País, na forma do disposto no Art. 1º, inciso IV, do citado Decreto, com o objetivo de participar da VII Reunião do Grupo Ad Hoc para Assuntos de Quarentena do COSAVE, em Montevidéu, República Oriental do Uruguai, no período de 8 a 14.11.2009, com ônus para o(a) PI-VICHPITO 1. (Processo nº 21000.009603/2009-93)

Autoriza o(a) Fiscal Federal Agropecuário MARCUS VINÍCIUS SEGURADO COELHO, do Quadro Permanente deste Ministério, lotado no(a) Secretaria de Defesa Agropecuária (SDA), a afastar-se do País, na forma do disposto no Art. 1º, inciso IV, do citado Decreto, com o objetivo de participar de reunião sobre identificação e documentação de organismos vivos geneticamente modificados em movimentos transfronteiriço promovido pelo Secretariado do CDB, na Cidade do México, Estados Unidos Mexicanos, no período de 22 a 28.11.2009, com ônus limitado. (Processo nº 21000.009602/2009-49)

Autoriza o(a) Engenheiro Agrônomo ARISTOTELES PIRES DE MATOS, contratado(a) pela EMBRAPA, sob o regime de CLT, lotado no(a) Mandioca e Fruticultura Tropical, a afastar-se do País, na forma do disposto no Art. 1º, inciso V, do citado Decreto, com o objetivo de participar de Missão do Ministério das Relações Exteriores-MRE/ABC, para realizar um diagnóstico das condições locais dos sistemas de produção de mandioca no Haiti, em Porto Príncipe, República do Haiti, no período de 21 a 29.11.2009, com ônus para o(a) MRE/ABC. (Processo nº 21000.009647/2009-13)

Autoriza o(a) Economista ANTONIO LUIZ MACHADO DE MORAES, Pesquisador da EMBRAPA, à disposição deste Ministério, lotado no(a) Secretaria de Política Agrícola (SPA), a afastar-se do País, na forma do disposto no Art. 1º, inciso IV, do citado Decreto, com o objetivo de participar das reuniões do Comitê de Agricultura da Organização para a Cooperação e Desenvolvimento Econômico (OCDE), em Paris, República Francesa, no período de 22 a 28.11.2009, com ônus para o(a) SPA. (Processo nº 21000.009646/2009-79)

Autoriza o(a) Fiscal Federal Agropecuário MARCO ANTÔNIO ARAÚJO DE ALENCAR, do Quadro Permanente deste Ministério, lotado no(a) Secretaria de Relações Internacionais do Agronegócio-SRI, a afastar-se do País, na forma do disposto no Art. 1º, inciso V, do citado Decreto, com o objetivo de participar da Reunião do Comitê de Normas da Comissão de Medidas Fitossanitárias da Convenção Internacional para a Proteção dos Vegetais - CIPV/FAO, em Roma, República Italiana, no período de 7 a 13.11.2009, com ônus para o(a) SRI-PI.MISSÕES 2. (Processo nº 21000. 009645/09-24)

Autoriza o(a) Fiscal Federal Agropecuário MARCO ANTÔNIO ARAÚJO DE ALENCAR, do Quadro Permanente deste Ministério, lotado no(a) Secretaria de Relações Internacionais do Agronegócio (SRI), a afastar-se do País, na forma do disposto no Art. 1º, inciso IV, do citado Decreto, com o objetivo de participar do XIX Curso Internacional teórico-prático sobre detecção e identificação de virus, viróides e fitoplasmas, em Madrid, Reino da Espanha, no período de 14 a 28.11.2009, com ônus limitado. (Processo nº 21000.008348/2009-61)

Autoriza o(a) Médico Veterinário LUIZ SÉRGIO DE ALMEIDA CAMARGO, contratado(a) pela EMBRAPA, sob o regime da CLT, lotado no(a) Gado de Leite, a afastar-se do País, na forma do disposto no Art. 1º, inciso V, do citado Decreto, com o objetivo de participar do curso Biotecnologia embrionaria aplicada al mejoramiento animal, al de desarrollo de fármacos y de células madres como palestrante na Universidade de Buenos Aires, em Buenos Aires, República da Argentina, no período de 10 a 14.11.2009, com ônus limitado. (Processo nº 21000.009586/2009-94)

Autoriza o(a) Engenheiro Agrônomo PEDRO ANTÔNIO ARRAES PEREIRA, Diretor-Presidente da EMBRAPA, Empresa Brasileira de Pesquisa Agropecuária, a afastar-se do País, na forma do disposto no Art. 1º, inciso V, do citado Decreto, com o objetivo de participar do Fórum de Prospecção 2009: Cenários de Inovação para o Desenvolvimento e para a reserva alimentar, em Montevidéu, República Oriental do Uruguai, no período de 23 a 25.11.2009, com ônus para o(a) EMBRAPA (Projeto Agrofuturo). (Processo nº 21000.009587/2009-39)

APÊNDICE 03 - Council Framework Decisions on attacks against information systems

(Actos adoptados em aplicação do título VI do Tratado da União Europeia)

DECISÃO-QUADRO 2005/222/JAI DO CONSELHO

de 24 de Fevereiro de 2005

relativa a ataques contra os sistemas de informação

O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado da União Europeia, nomeadamente o artigo 29.º, a alínea a) do n.º 1 do artigo 30.º, a alínea e) do n.º 1 do artigo 31.º e a alínea b) do n.º 2 do artigo 34.º,

Tendo em conta a proposta da Comissão,

Tendo em conta o parecer do Parlamento Europeu [1],

Considerando o seguinte:

(1) A presente decisão-quadro tem por objectivo reforçar a cooperação entre as autoridades judiciárias e outras autoridades competentes, nomeadamente as autoridades policiais e outros serviços especializados responsáveis pela aplicação da lei nos Estados-Membros, mediante uma aproximação das suas disposições de direito penal em matéria dos ataques contra os sistemas de informação.

(2) Há provas de ataques contra os sistemas de informação, nomeadamente devido à ameaça que representa a criminalidade organizada, existindo uma crescente inquietação perante a eventualidade de ataques terroristas contra os sistemas de informação que constituem a infra-estrutura vital dos Estados-Membros. Esta ameaça poderá comprometer a instauração de uma sociedade da informação mais segura e de um espaço de liberdade, de segurança e de justiça, exigindo, portanto, uma resposta ao nível da União Europeia.

(3) Uma resposta eficaz a essas ameaças pressupõe uma abordagem global em matéria de segurança das redes e da informação, como foi sublinhado no Plano de Acção «eEurope», na Comunicação da Comissão intitulada «Segurança das redes e da informação: proposta de abordagem de uma política europeia» e na Resolução do Conselho de 28 de Janeiro de 2002, sobre uma abordagem comum e acções específicas no domínio da segurança das redes e da informação [2].

(4) A necessidade de reforçar a sensibilização para os problemas associados à segurança da informação e de fornecer assistência prática foi igualmente sublinhada pela Resolução do Parlamento Europeu de 5 de Setembro de 2001.

(5) As consideráveis lacunas e diferenças entre as legislações dos Estados-Membros neste domínio podem entravar a luta contra a criminalidade organizada e o terrorismo e podem dificultar uma cooperação policial e judiciária eficaz no âmbito de ataques contra os sistemas de informação. A natureza transnacional e sem fronteiras dos modernos sistemas de informação implica que os ataques contra esses sistemas têm frequentemente uma dimensão transfronteiriça, evidenciando assim a necessidade urgente de prosseguir a harmonização das legislações penais neste domínio.

(6) O Plano de Acção do Conselho e da Comissão sobre a melhor forma de aplicar as disposições do Tratado de Amesterdão relativas à criação de um espaço de liberdade, de segurança e de justiça [3], o Conselho Europeu de Tampere, de 15 e 16 de Outubro de 1999, o Conselho Europeu de Santa Maria da Feira, de 19 e 20 de Junho de 2000, o Painel de Avaliação da Comissão e a Resolução do Parlamento Europeu de 19 de Maio de 2000 mencionam ou requerem medidas legislativas contra a criminalidade de alta tecnologia, nomeadamente definições, incriminação e sanções comuns.

(7) É necessário completar o trabalho realizado pelas organizações internacionais, especialmente ao nível do Conselho da Europa, no domínio da aproximação do direito penal e os trabalhos do G8 sobre cooperação transnacional no âmbito da criminalidade de alta tecnologia, propondo uma abordagem comum neste domínio ao nível da União Europeia. Este pedido foi desenvolvido na Comunicação que a Comissão dirigiu ao Conselho, ao Parlamento Europeu, ao Comité Económico reforçando a segurança das infra-estruturas da informação e lutando contra a cibercriminalidade.

(8) As disposições de direito penal em matéria de ataques contra os sistemas de informação devem ser harmonizadas, a fim de assegurar a melhor cooperação policial e judiciária possível no que diz respeito às infracções penais associadas a este tipo de ataques e contribuir para a luta contra a criminalidade organizada e o terrorismo.

[1] JO C 300 E de 11.12.2003, p. 26.
[2] JO C 43 de 16.2.2002, p. 2.
[3] JO C 19 de 23.1.1999, p. 1.

(9) Todos os Estados-Membros ratificaram a Convenção do Conselho da Europa, de 28 de Janeiro de 1981, para a Protecção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal. Os dados de carácter pessoal, tratados no contexto da aplicação da presente decisão-quadro, serão protegidos em conformidade com os princípios estabelecidos na referida Convenção.

(10) É importante estabelecer definições comuns neste domínio, especialmente em relação aos sistemas de informação e aos dados informáticos, a fim de assegurar uma abordagem coerente da aplicação da presente decisão-quadro nos Estados-Membros.

(11) É necessário adoptar uma abordagem comum para os elementos constitutivos das infracções penais, prevendo infracções comuns por acesso ilegal a determinado sistema de informação, por interferência ilegal no sistema e por interferência ilegal nos dados.

(12) No interesse do combate à criminalidade informática, cada Estado-Membro deverá assegurar uma cooperação judiciária eficaz no que diz respeito às infracções baseadas nos tipos de comportamento a que se referem os artigos 2.º, 3.º, 4.º e 5.º

(13) É necessário evitar uma incriminação exorbitante, nomeadamente de casos insignificantes, bem como a incriminação de titulares de direitos e de pessoas autorizadas.

(14) É necessário que os Estados-Membros estabeleçam sanções para combater os ataques contra os sistemas de informação. Essas sanções deverão ser efectivas, proporcionadas e dissuasivas.

(15) É adequado prever penas mais severas nos casos em que um ataque contra determinado sistema de informação tenha sido praticado no âmbito de uma organização criminosa, tal como definida na Acção Comum 98/733/JAI do Conselho, de 21 de Dezembro de 1998, relativa à incriminação da participação numa organização criminosa nos Estados-Membros da União Europeia [1]. É igualmente adequado prever penas mais severas quando um tal ataque tiver causado danos graves ou lesado interesses essenciais.

(16) Deverão ser igualmente adoptadas medidas de cooperação entre os Estados-Membros, a fim de assegurar uma acção eficaz contra os ataques que visem os sistemas de informação. Os Estados-Membros devem, pois, recorrer à actual rede de pontos de contacto operacionais referida na Recomendação do Conselho, de 25 de Junho de 2001, relativa a um serviço de 24 horas por dia de combate ao crime de alta tecnologia [2], para efeitos de troca de informações.

(17) Atendendo a que os objectivos da presente decisão-quadro, a saber, garantir que os ataques contra os sistemas de informação sejam puníveis em todos os Estados-Membros com sanções penais efectivas, proporcionadas e dissuasivas, bem como melhorar e favorecer a cooperação judiciária, suprimindo potenciais dificuldades, não podem ser suficientemente realizados pelos Estados-Membros, já que as normas devem ser comuns e compatíveis, e podem, pois, ser melhor alcançados ao nível da União, esta pode tomar medidas em conformidade com o princípio da subsidiariedade consagrado no artigo 5.º do Tratado CE. Em conformidade com o princípio da proporcionalidade consagrado neste mesmo artigo, a presente decisão-quadro não excede o necessário para alcançar aqueles objectivos.

(18) A presente decisão-quadro respeita os direitos fundamentais e os princípios reconhecidos pelo artigo 6.º do Tratado União Europeia e reflectidos na Carta dos Direitos Fundamentais da União Europeia, designadamente nos capítulos II e VI,

ADOPTOU A PRESENTE DECISÃO-QUADRO:

Artigo 1.º

Definições

Para efeitos da presente decisão-quadro, entende-se por:

a) «Sistema de informação», qualquer dispositivo ou qualquer grupo de dispositivos interligados ou associados, um ou vários dos quais executem, graças a um programa, o tratamento automático de dados informáticos, bem como dados informáticos por eles armazenados, tratados, recuperados ou transmitidos, tendo em vista o seu funcionamento, utilização, protecção e manutenção;

b) «Dados informáticos», qualquer representação de factos, informações ou conceitos, de forma a serem processados num sistema de informação, nomeadamente um programa capaz de permitir que um sistema de informação execute uma dada função;

c) «Pessoa colectiva», qualquer entidade que beneficie desse estatuto por força do direito aplicável, com excepção do Estado ou de outras entidades de direito público no exercício das suas prerrogativas de autoridade pública e das organizações internacionais de direito público;

[1] JO L 351 de 29.12.1998, p. 1.

[2] JO C 187 de 3.7.2001, p. 5.

d) «Não autorizado», acesso ou interferência não consentidos pelo proprietário, por outro titular do direito do sistema ou de parte dele, ou não permitidos nos termos do direito nacional.

Artigo 2.º

Acesso ilegal aos sistemas de informação

1. Os Estados-Membros devem tomar as medidas necessárias para assegurar que o acesso intencional, não autorizado, à totalidade ou a parte de um sistema de informação seja punível como infracção penal, pelo menos nos casos que não sejam de menor gravidade.

2. Os Estados-Membros podem decidir que os comportamentos referidos no n.º 1 são puníveis apenas quando a infracção tiver sido cometida em violação de uma medida de segurança.

Artigo 3.º

Interferência ilegal no sistema

Cada Estado-Membro deve tomar as medidas necessárias para assegurar que o acto intencional e não autorizado de impedir ou interromper gravemente o funcionamento de um sistema de informação, introduzindo, transmitindo, danificando, apagando, deteriorando, alterando, suprimindo ou tornando inacessíveis os dados informáticos, seja punível como infracção penal, pelo menos nos casos que não sejam de menor gravidade.

Artigo 4.º

Interferência ilegal nos dados

Cada Estado-Membro deve tomar as medidas necessárias para assegurar que o acto intencional e não autorizado de apagar, danificar, deteriorar, alterar, suprimir ou tornar inacessíveis os dados informáticos de um sistema de informação seja punível como infracção penal, pelo menos nos casos que não sejam de menor gravidade.

Artigo 5.º

Instigação, auxílio, cumplicidade e tentativa

1. Cada Estado-Membro deve assegurar que a instigação, o auxílio e a cumplicidade na prática de alguma das infracções referidas nos artigos 2.º, 3.º e 4.º sejam puníveis como infracção penal.

2. Cada Estado-Membro deve assegurar que a tentativa de prática das infracções referidas nos artigos 2.º, 3.º e 4.º seja punível como infracção penal.

3. Cada Estado-Membro pode decidir não aplicar o n.º 2 relativamente às infracções referidas no artigo 2.º

Artigo 6.º

Sanções

1. Cada Estado-Membro deve tomar as medidas necessárias para assegurar que as infracções referidas nos artigos 2.º, 3.º, 4.º e 5.º sejam passíveis de sanções penais efectivas, proporcionadas e dissuasivas.

2. Cada Estado-Membro deve tomar as medidas necessárias para assegurar que as infracções referidas nos artigos 3.º e 4.º sejam passíveis de pena privativa de liberdade com duração máxima de, pelo menos, um a três anos.

Artigo 7.º

Circunstâncias agravantes

1. Cada Estado-Membro deve tomar as medidas necessárias para assegurar que a infracção referida no n.º 2 do artigo 2.º e as referidas nos artigos 3.º e 4.º sejam passíveis de pena privativa de liberdade com duração máxima de, pelo menos, dois a cinco anos quando forem praticadas no âmbito de uma organização criminosa, tal como definida na Acção Comum 98/733/JAI, independentemente do nível da pena nesta referido.

2. Um Estado-Membro pode também tomar as medidas a que se refere o n.º 1 nos casos em que a infracção em causa tenha causado danos graves ou lesado interesses essenciais.

Artigo 8.º

Responsabilidade das pessoas colectivas

1. Cada Estado-Membro deve tomar as medidas necessárias para assegurar que as pessoas colectivas possam ser consideradas responsáveis pelas infracções referidas nos artigos 2.º, 3.º, 4.º e 5.º, praticadas em seu benefício por qualquer pessoa, agindo individualmente ou enquanto integrando um órgão da pessoa colectiva, que nela ocupe uma posição dominante baseada:

a) Nos seus poderes de representação da pessoa colectiva; ou

b) No seu poder para tomar decisões em nome da pessoa colectiva; ou

c) Na sua autoridade para exercer controlo dentro da pessoa colectiva.

2. Para além dos casos previstos no n.º 1, os Estados-Membros devem assegurar que uma pessoa colectiva possa ser considerada responsável sempre que a falta de vigilância ou de controlo por parte de uma pessoa referida no n.º 1 tenha tornado possível a prática, por uma pessoa que lhe esteja subordinada, das infracções referidas nos artigos 2.º, 3.º, 4.º e 5.º, em benefício dessa pessoa colectiva.

3. A responsabilidade de uma pessoa colectiva nos termos dos n.os 1 e 2 não exclui a instauração de procedimento penal contra as pessoas singulares envolvidas na qualidade de autoras, instigadoras ou cúmplices nas infracções referidas nos artigos 2.º, 3.º, 4.º e 5.º

Artigo 9.º

Sanções aplicáveis às pessoas colectivas

1. Cada Estado-Membro deve tomar as medidas necessárias para assegurar que uma pessoa colectiva considerada responsável nos termos do n.º 1 do artigo 8.º seja passível de sanções efectivas, proporcionadas e dissuasivas, incluindo multas ou coimas e eventualmente outras sanções, designadamente:

a) Exclusão do benefício de vantagens ou auxílios públicos;

b) Interdição temporária ou permanente de exercer actividade comercial;

c) Colocação sob vigilância judicial;

d) Dissolução por via judicial.

2. Cada Estado-Membro deve tomar as medidas necessárias para assegurar que uma pessoa colectiva considerada responsável nos termos do n.º 2 do artigo 8.º seja passível de sanções ou medidas efectivas, proporcionadas e dissuasivas.

Artigo 10.º

Competência

1. Cada Estado-Membro deve definir a sua competência relativamente às infracções referidas nos artigos 2.º, 3.º, 4.º e 5.º, sempre que a infracção tiver sido praticada:

a) Total ou parcialmente no seu território; ou

b) Por um nacional seu; ou

c) Em benefício de uma pessoa colectiva com sede no seu território.

2. Ao definir a sua competência em conformidade com a alínea a) do n.º 1, cada Estado-Membro deve assegurar que sejam incluídos os casos em que:

a) O autor praticou a infracção quando se encontrava fisicamente presente no território desse Estado-Membro, independentemente de a infracção visar ou não um sistema de informação situado no seu território; ou

b) A infracção foi praticada contra um sistema de informação situado no território desse Estado-Membro, independentemente de o autor da infracção se encontrar ou não fisicamente presente no seu território.

3. Qualquer Estado-Membro que, nos termos do seu direito, ainda não extradite ou entregue os seus nacionais, deve tomar as medidas necessárias para definir a sua competência e, eventualmente, para instaurar procedimento penal relativamente às infracções referidas nos artigos 2.º, 3.º, 4.º e 5.º, quando praticadas por um dos seus nacionais fora do seu território.

4. Sempre que uma infracção seja da competência de mais do que um Estado-Membro e qualquer um deles possa validamente instaurar procedimento penal com base nos mesmos factos, os Estados-Membros em causa devem cooperar para decidir qual deles moverá o procedimento contra os autores da infracção, tendo em vista centralizá-lo, se possível, num único Estado-Membro. Para o efeito, os Estados-Membros podem recorrer a qualquer órgão ou mecanismo instituído no seio da União Europeia para facilitar a cooperação entre as suas autoridades judiciais e a coordenação das respectivas acções. Serão tidos em conta, sucessivamente, os seguintes elementos:

— o Estado-Membro ser aquele em cujo território foram praticadas as infracções, nos termos da alínea a) do n.º 1 e do n.º 2,

— o Estado-Membro ser o da nacionalidade do autor,

— o Estado-Membro ser aquele em cujo território o autor foi encontrado.

5. Qualquer Estado-Membro pode decidir que não aplicará ou que só aplicará em casos ou condições específicos, as regras de competência estabelecidas nas alíneas b) e c) do n.º 1.

6. Sempre que decidirem aplicar o n.º 5, os Estados-Membros devem informar desse facto o Secretariado-Geral do Conselho e a Comissão, indicando, se necessário, os casos ou condições especiais em que a decisão se aplica.

Artigo 11.º

Intercâmbio de informações

1. Para efeitos da troca de informações relativa às infracções referidas nos artigos 2.º, 3.º, 4.º. e 5.º e de acordo com as normas em matéria de protecção de dados, os Estados-Membros devem recorrer à rede existente de pontos de contacto operacionais, disponíveis 24 horas por dia e sete dias por semana.

2. Cada Estado-Membro deve notificar ao Secretariado-Geral do Conselho e à Comissão o ponto de contacto designado para efeitos de troca de informações sobre infracções relacionadas com ataques contra sistemas de informação. O Secretariado-Geral transmite essa informação aos restantes Estados-Membros.

Artigo 12.º

Transposição

1. Os Estados-Membros devem tomar as medidas necessárias para dar cumprimento às disposições da presente decisão-quadro até 16 de Março de 2007.

2. Os Estados-Membros devem transmitir ao Secretariado-Geral do Conselho e à Comissão, até 16 de Março de 2007, o texto das disposições que transpõem para o respectivo direito nacional as obrigações resultantes da presente decisão-quadro. Até 16 de Setembro de 2007, com base num relatório elaborado a partir daquelas informações e num relatório escrito apresentado pela Comissão, o Conselho verifica em que medida os Estados-Membros tomaram as medidas necessárias para dar cumprimento à presente decisão-quadro.

Artigo 13.º

Entrada em vigor

A presente decisão-quadro entra em vigor na data da sua publicação no *Jornal Oficial da União Europeia*.

Feito em Bruxelas, em 24 de Fevereiro de 2005.

Pelo Conselho

O Presidente

N. SCHMIT

APÊNDICE 04 - Towards a general policy on the fight against cybercrime

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 22.5.2007
COM(2007) 267 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL AND THE COMMITTEE OF THE REGIONS

Towards a general policy on the fight against cyber crime

{SEC(2007) 641}
{SEC(2007) 642}

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL AND THE COMMITTEE OF THE REGIONS

Towards a general policy on the fight against cyber crime

1. INTRODUCTION

1.1. What is cyber crime?

The security of the increasingly important information systems in our societies covers many aspects, of which the fight against cyber crime is a core element. Without an agreed definition of cyber crime, the terms "cyber crime", "computer crime", "computer-related crime" or "high-tech crime" are often used interchangeably. For the purpose of this Communication, 'cyber crime' is understood as "criminal acts committed using electronic communications networks and information systems or against such networks and systems".

In practice, the term cyber crime is applied to three categories of criminal activities. The first covers **traditional forms of crime** such as fraud or forgery, though in a cyber crime context relates specifically to crimes committed over electronic communication networks and information systems (hereafter: electronic networks). The second concerns the publication of **illegal content** over electronic media (i.a. child sexual abuse material or incitement to racial hatred). The third includes **crimes unique to electronic networks**, i.e. attacks against information systems, denial of service and hacking. These types of attacks can also be directed against the crucial critical infrastructures in Europe and affect existing rapid alert systems in many areas, with potentially disastrous consequences for the whole society. Common to each category of crime is that they may be committed on a mass-scale and with a great geographical distance between the criminal act and its effects. Consequently the technical aspects of applied investigative methods are often the same. These commonalities will form the focus of this Communication.

1.2. Latest developments in cyber crime

1.2.1. In general

The combination of constantly evolving criminal activities and a lack of reliable information makes it difficult to obtain an exact picture of the current situation. Nevertheless, some general trends can be discerned:

- The number of cyber crimes is growing and criminal activities are becoming increasingly sophisticated and internationalised[1]
- Clear indications point to a growing involvement of organised crime groups in cyber crime

[1] The majority of this Communication's statements on current trends have been taken from the Study to assess the impact of a communication on cyber crime, ordered by the Commission in 2006 (Contract No JLS/2006/A1/003).

- However, the number of European prosecutions on the basis of cross-border law enforcement cooperation do not increase

1.2.2. Traditional crime on electronic networks

Most crimes can be committed with the use of electronic networks, and different types of fraud and attempted fraud are particularly common and growing forms of crime on electronic networks. Instruments such as identity theft, phishing[2], spams and malicious codes may be used to commit large scale fraud. Illegal national and international Internet-based trade has also emerged as a growing problem. This includes trade in drugs, endangered species and arms.

1.2.3. Illegal content

A growing number of illegal content sites are accessible in Europe, covering child sexual abuse material, incitement to terrorist acts, illegal glorification of violence, terrorism, racism and xenophobia. Law enforcement action against such sites is extremely difficult, as site owners and administrators are often situated in countries other than the target country, and often outside the EU. The sites can be moved very quickly, also outside the territory of the EU, and the definition of illegality varies considerably from one state to another.

1.2.4. Crimes unique to electronic networks

Large scale attacks against information systems or organisations and individuals (often through so called botnets[3]) appear to have become increasingly prevalent. Also, incidents with systematic, well co-ordinated and large-scale direct attacks against the critical information infrastructure of a state have recently been observed. This has been compounded by the merging technologies and accelerated interlinking of information systems, which rendered those systems more vulnerable. Attacks are often well organised and used for purposes of extortion. It can be assumed that the extent of reporting is minimised, in part due to the business disadvantages which may be the result if security problems were to become public.

1.3. Objectives

In the light of this changing environment, there is an urgent need to take action – at national as well as European level – against all forms of cyber crime, which are increasingly significant threats to critical infrastructures, society, business and citizens. Protection of individuals against cyber crime is often exacerbated by issues related to the determination of the competent jurisdiction, applicable law, cross-border enforcement or the recognition and use of electronic evidence. The essentially cross-border dimension of cyber crime highlights such difficulties. In addressing these threats, the Commission is launching a general policy initiative to improve European and international level coordination in the fight against cyber crime.

The objective is to strengthen the fight against cyber crime at national, European and international level. Further development of a specific EU policy, in particular, has long been recognised as a priority by the Member States and the Commission. The focus of the initiative

---

2 Phishing describes attempts to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person in an electronic communication.

3 Botnet refers to a collection of compromised machines running programs under a common command.

will be on the law enforcement and criminal law dimensions of this fight and the policy will complement other EU actions to improve security in cyber space in general. The policy will eventually include: improved operational law enforcement cooperation; better political cooperation and coordination between Member States; political and legal cooperation with third countries; awareness raising; training; research; a reinforced dialogue with industry and possible legislative action.

The policy on the fight and prosecution of cyber crime will be defined and implemented in a manner fully respecting fundamental rights, in particular those of freedom of expression, respect for private and family life and the protection of personal data. Any legislative action taken in the context of this policy will be first scrutinised for compatibility with such rights, in particular the EU Charter of Fundamental Rights. It should also be noted that all such policy initiatives will be carried out in full consideration of Articles 12 to 15 of the so called e-commerce Directive[4], where this legal instrument applies.

The objective of this Communication can be divided into three main operational strands, which can be summarised as follows:

- To improve and facilitate coordination and cooperation between cyber crime units, other relevant authorities and other experts in the European Union
- To develop, in coordination with Member States, relevant EU and international organisations and other stakeholders, a coherent EU Policy framework on the fight against cyber crime
- To raise awareness of costs and dangers posed by cyber crime

2. EXISTING LEGAL INSTRUMENTS IN THE FIGHT AGAINST CYBER CRIME

2.1. Existing instruments and actions at EU level

The present Communication on cyber crime policy consolidates and develops the 2001 Communication on Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime[5] (hereafter: the 2001 Communication). The 2001 Communication proposed appropriate substantive and procedural legislative provisions to deal with both domestic and trans-national criminal activities. From this, several important proposals followed. In particular, these include the proposal leading to the Framework Decision 2005/222/JHA on attacks against information systems[6]. In this context, it should also be noted that other, more general, legislation covering also aspects of the fight against cyber crime has been adopted, such as the Framework Decision 2001/413/JHA on combating fraud and counterfeiting of non-cash means of payment[7].

---

4 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (OJ L 178, 17.7.2000, p. 1).

5 COM(2000) 890, 26.1.2001.

6 OJ L 69, 16.3.2005, p. 67.

7 OJ L 149, 2.6.2001, p. 1.

The Framework Decision 2004/68/JHA on sexual exploitation of children[8] is a good example of the particular focus put by the Commission on the **protection of children**, especially in relation to the fight against all forms of child sexual abuse material illegally published using information systems, a horizontal priority which will be kept in the future.

To tackle security challenges for the information society, the European Community has developed a three-pronged approach for network and information security: specific network and information security measures, the regulatory framework for electronic communications and the fight against cyber crime. Although these three aspects can, to a certain extent, be developed separately, the numerous interdependencies call for tight coordination. In the related field of Network and Information security, a 2001 Commission Communication on Network and Information Security: A proposal for an EU policy approach[9], was adopted in parallel to the 2001 communication on cyber crime. The ePrivacy directive 2002/58/EC lays down an obligation for providers of publicly available electronic communication services to safeguard the security of their services. Provisions against spam and spyware are also laid down there. The Network and Information security policy has since been developed through a number of actions, most recently in Communications on a Strategy for a secure Information society[10] that sets out the revitalized strategy and provides the framework to carry forward and refine a coherent approach to Network and Information security, and on Fighting spam, spyware and malicious software[11], and in the 2004 creation of ENISA[12]. The main objective of ENISA is to develop expertise to stimulate cooperation between the public and private sectors, and provide assistance to the Commission and Member States. **Research results** in the area of technologies to secure information systems will also play an important role in the fight against cyber crime. Accordingly, Information and Communication Technologies as well as Security are all mentioned as objectives in the EU Seventh Research Framework Programme (FP 7), which will be operational during the period 2007-2013[13]. The review of the regulatory framework for electronic communications might result in amendments to to enhance the effectiveness of the security-related provisions of the ePrivacy Directive and the Universal Service Directive 2002/22/EC[14].

2.2. Existing international instruments

Due to the global nature of information networks, no policy on cyber crime can be effective if efforts are confined within the EU. Criminals can not only attack information systems or commit crimes from one Member State to another, but can easily do so from outside the EU's jurisdiction. Accordingly, the Commission has actively participated in international discussions and cooperation structures, i.a. the G 8 Lyon-Roma High-Tech Crime Group and Interpol-administered projects. The Commission is in particular closely following the work of the network for 24-hour contacts for International High-Tech Crime (the 24/7 network)[15], of which a considerable number of states worldwide, including most EU Member States, are

---

8 OJ L 13, 20.1.2004, p. 44.
9 COM(2001) 298.
10 COM(2006) 251.
11 COM(2006) 688.
12 Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency (OJ L 77, 13.3.2004, p. 1).
13 The European Union has already under the 6th Framework Programme for Research and and Technological development supported a number of relevant, and successful, research projects.
14 COM(2006) 334, SEC(2006)816, SEC(2006) 817.
15 See Article 35 in the Council of Europe Convention on cyber crime.

members. The G8 network constitutes a mechanism to expedite contacts between participating states, with 24-hour points of contact for cases involving electronic evidence, and those requiring urgent assistance from foreign law enforcement authorities.

Arguably, the predominant European and international instrument in this field is the Council of Europe's 2001 Convention on cyber crime[16]. The Convention, which was adopted and entered into force in 2004, contains common definitions of different types of cyber crime and lays the foundation for a functioning judicial cooperation between contracting states. It has been signed by many states, including the United States of America and other non-European states, and by all Member States. A number of Member States have however not yet ratified the Convention or the additional protocol to the Convention dealing with acts of racist and xenophobic nature committed through computer systems. Considering the agreed importance of the Convention, the Commission will encourage Member States and relevant third countries to ratify the Convention and consider the possibility for the European Community to become a party to the Convention.

3. FURTHER DEVELOPMENT OF SPECIFIC INSTRUMENTS IN THE FIGHT AGAINST CYBER CRIME

3.1. Strengthening operational law enforcement cooperation and EU-level training efforts

The lack, or underutilisation, of immediate structures for **cross-border operational cooperation** remains a major weakness in the area of Justice, Freedom and Security. Traditional mutual assistance when confronted with urgent cyber crime cases has proven slow and ineffective, and new cooperation structures have not yet been sufficiently developed. While national judicial and law enforcement authorities in Europe cooperate closely via Europol, Eurojust and other structures, there remains an obvious need to strengthen and clarify responsibilities. Consultations undertaken by the Commission indicate that these crucial channels are not used in an optimal way. A more coordinated European approach must be both operational and strategic and also cover the exchange of information and best practices.

The Commission will in the near future lay particular emphasis on **training** needs. It is an established fact that the technological developments produce a need for continuous training on cyber crime issues for law enforcement and judicial authorities. A reinforced and better coordinated financial support from the EU to multinational training programs is therefore envisaged. The Commission will also, in close cooperation with Member States and other competent organs such as Europol, Eurojust, the European Police College (CEPOL) and the European Judicial Training Network (EJNT), work to achieve an EU level coordination and interlinking of all relevant training programmes.

The Commission will organise a **meeting** of law enforcement experts from Member States, as well as from Europol, CEPOL and the EJTN, to discuss how to improve strategic and operational cooperation as well as cyber crime training in Europe in 2007. Among other things, the creation of both a permanent EU contact point for information exchange and an

---

[16] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

EU cyber crime training platform will be considered. The 2007 meeting will be the first in a series of meetings planned for the near future.

3.2. Strengthen the dialogue with industry

Both private and public sectors have an interest in jointly developing methods to identify and prevent harm resulting from the activities of crime. Shared private and public sector participation, based on mutual trust and a common objective of harm reduction, promises to be an effective way of enhancing security, also in the fight against cyber crime. The public-private aspects of the Commission's cyber crime policy will in time be part of a planned global EU policy on dialogue between the public and the private sector, covering the whole area of European security. This policy will in particular be taken forward by the European Security Research and Innovation Forum, which the Commission plans to create shortly and which will regroup relevant stakeholders from the public and the private sector.

The development of modern information technologies and electronic communication systems is largely controlled by private operators. Private companies carry out threat assessments, establish programmes for the fight against crime and develop technical solutions to prevent crime. Industry has displayed a very positive attitude to assisting public authorities in the fight against cyber crime, especially in efforts to counter child pornography[17] and other types of illegal content on the Internet.

Another issue concerns the apparent lack of exchange of information, expertise and best practices between the public and the private sector. Private sector operators are often, in order to protect business models and secrets, reluctant, or are under no clear legal obligation, to report or share relevant information on crime incidences with law enforcement authorities. However, such information may be needed if public authorities are to formulate an efficient and appropriate anti-crime policy. The possibilities to improve cross-sector information exchange will be considered also in the light of existing rules on protection of personal data.

The Commission already plays an important role in various public-private structures dealing with cyber crime, such as the Fraud Prevention Expert Group[18]. The Commission is convinced that an effective general policy for the fight against cyber crime must also include a strategy for cooperation between the public sector and private sector operators, including civil society organisations.

To achieve broader public-private cooperation in this field, the Commission will in 2007 organise a conference for law enforcement experts and private sector representatives, especially Internet Service Providers, to discuss how to improve public-private operational cooperation in Europe[19]. The conference will touch upon all subjects deemed to add value for both sectors, but especially:

---

17 One recent example of cooperation in this field is the cooperation between law enforcement and credit-card companies, through which the latter have assisted the police in tracking down purchasers of online child pornography.

18 See http://ec.europa.eu/internal_market/payments/fraud/index_en.htm

19 The Conference could be regarded as the continuation of the EU Forum presented in Section 6.4 in the computer-crime communication.

- Improving operational cooperation in the fight against illegal activities and content on the Internet, specifically in the areas of terrorism, child sexual abuse material and other illegal activities particularly sensitive from a child protection perspective

- Initiating public-private agreements aiming at the EU-wide blocking of sites containing illegal content, especially child sexual abuse material

- Devising a European model for the sharing of necessary and relevant information across the private and public sectors, one consideration being to cultivate an atmosphere of mutual confidence and take the interests of all parties into account

- Establishing a network of law enforcement contact points in both private and public sectors

3.3. Legislation

General harmonisation of crime definitions and national penal laws in the field of cyber crime, is not yet appropriate, due to the variety of the types of offences covered by this notion. Since effective cooperation between law enforcement authorities often depends on having at least partly harmonised crime definitions, it remains a long-term objective to continue harmonising Member States' legislation[20]. With regard to certain key crime definitions, an important step has already been taken with the Framework Decision on attacks against information systems. As described above, new threats have subsequently appeared and the Commission is closely following this evolution given the importance of continuously assessing the need for additional legislation. The monitoring of the evolving threats is closely coordinated with the European Programme for Critical Infrastructure Protection.

Targeted legislation against cyber crime should however also be considered now. A particular issue which may require legislation relates to a situation where cyber crime is committed in conjunction with **identity theft**. Generally, "identity theft" is understood as the use of personal identifying information, e.g. a credit card number, as an instrument to commit other crimes. In most Member States, a criminal would most likely be prosecuted for the fraud, or another potential crime, rather than for the identity theft; the former being considered a more serious crime. Identity theft as such is not criminalised across all Member States. It is often easier to prove the crime of identity theft than that of fraud, so that EU law enforcement cooperation would be better served were identity theft criminalised in all Member States. The Commission will in 2007 commence consultations to assess if legislation is appropriate.

3.4. Development of statistical data

It is generally agreed that the current state of information concerning the prevalence of crime is largely inadequate, and in particular that much improvement is needed to compare data between Member States. An ambitious five-year plan to tackle this problem was set out in the Communication from the Commission on *Developing a comprehensive and coherent EU strategy to measure crime and criminal justice: An EU Action Plan 2006 – 2010*[21]. The Expert Group set up under this Action Plan would provide a suitable forum for developing relevant indicators for measuring the extent of cyber crime.

---

[20] This longer-term objective has already been mentioned on page 3 of the 2001 Communication.

[21] COM(2006) 437, 7.8.2006.

4. THE WAY FORWARD

The Commission will now take the general policy for the fight against cyber crime forward. Due to the limited powers of the Commission in the field of criminal law, this policy can only be a complement to the actions undertaken by Member States and other bodies. The most important actions – each of which will imply the use of one, several or all of the instruments presented in Chapter 3 – will also be supported through the Financial Programme "Prevention of and Fight against Crime":

4.1. The fight against cyber crime in general

- Establish a strengthened operational cooperation between Member States' law enforcement and judicial authorities, an action which will begin with the organisation of a dedicated expert meeting in 2007 and which may include the setting up of a central EU cyber crime contact point

- Increase financial support to initiatives for improved training of law enforcement and judicial authorities vis-à-vis the handling of cyber crime cases and take action to coordinate all multinational training efforts in this field by the setting up of an EU training platform

- Promote a stronger commitment from Member States and all public authorities to take effective measures against cyber crime and to allocate sufficient resources to combat such crimes

- Support research beneficial to the fight against cyber crime

- Organise at least one major conference (in 2007) with law enforcement authorities and private operators, especially to initiate cooperation in the fight against illegal Internet activities in and against electronic networks and to promote a more effective non-personal information exchange, and to follow-up on the conclusions from this 2007 conference with concrete public-private cooperation projects

- Take the initiative for and participate in public-private actions aimed at raising awareness, especially among consumers, of the cost of and dangers posed by cyber crime, while avoiding the undermining of the trust and confidence of consumers and users by focusing only on negative aspects of security

- Actively participate in and promote global international cooperation in the fight against cyber crime

- Initiate, contribute to and support international projects which are in line with the Commission policy in this field, e.g. projects run by the G 8 and consistent with the Country and Regional Strategy Papers (regarding cooperation with third countries)

- Take concrete action to encourage all Member States and relevant third countries to ratify the Council of Europe's Cyber Crime Convention and its additional protocol and consider the possibility for the Community to become a party to the Convention

- Examine, together with the Member States, the phenomenon of co-ordinated and large scale attacks against the information infrastructure of member states in view of preventing

and combating these, including co-ordinating responses, and sharing information and best practices

4.2. Fight against traditional crime in electronic networks

- Initiate an in-depth analysis with a view to preparing a proposal for specific EU legislation against identity theft
- Promote the development of technical methods and procedures to fight fraud and illegal trade on the Internet, also through public-private cooperation projects
- Continue and develop work in specific targeted areas, such as in the Fraud Prevention Expert Group on the fight against fraud with non-cash means of payment in electronic networks

4.3. Illegal content

- Continue to develop actions against specific illegal content, especially regarding child sexual abuse material and incitement to terrorism and notably through the follow-up of the implementation of the Framework Decision on sexual exploitation of children
- Invite the Member States to allocate sufficient financial resources to strengthen the work of law enforcement agencies with special attention to identifying the victims of sexual abuse material which is distributed online
- Initiate and support actions against illegal content that may incite minors to violent and other serious illegal behaviour, i.a. certain types of extremely violent on-line video games
- Initiate and promote dialogue between Member States and with third countries on technical methods to fight illegal content as well as on procedures to shut down illegal websites, also with a view to the possible development of formal agreements with neighbouring and other countries on this issue
- Develop EU-level voluntary agreements and conventions between public authorities and private operators, especially Internet service providers, regarding procedures to block and close down illegal Internet sites

4.4. Follow-up

In this Communication, a number of actions aimed at improving cooperation structures in the EU have been outlined as next steps. The Commission will take these actions forward, assess progress on the implementation of the activities, and report to the Council and Parliament.

APÊNDICE 05 - NGO Report - 12º Congresso das Nações Unidas para Prevenção e Justiça Criminal

ISPAC

International Scientific and Professional Advisory Council of the United Nations Crime Prevention and - Criminal Justice Programme (ISPAC)

TWELFTH UNITED NATIONS CONGRESS
on
CRIME PREVENTION AND CRIMINAL JUSTICE

Salvador, Brazil – 12 to 19 April 2010

Report on the Activities of the Non-governmental Organizations (NGOs) and the Ancillary Meetings

Support for the work of the NGOs has been provided by:
Department of Justice, Government of Canada
Associaçao Contas Abertas (through UNODC's "Looking Beyond" Project)
Microsoft Corporation
ISPAC
Contact Center, Inc.
CEGA Services, Inc.

For Information, contact:
Gary Hill - Email: Garyhill@cega.com
P.O. Box 81826
Lincoln, Nebraska 68501-1826
USA
Phone: 402 420-0602
Fax: 402 420-0604
Web site: www.ispac-italy.org

prison model. In economic terms the government would spend three million dollars to build houses for 1000 people while it would cost fifty million dollars to build a traditional prison.

69 - Cancelled

70 – Cancelled

71-Challenges posed by the globalization of criminal justice
Session Coordinator: Giovanni Pasqua (Giovanni.pasqua@isisc.org) - Association Internationale de Droit Penal (AIDP-IAPL) and Istituto Supreiore Internazionale di Socienze Criminal (ISISC)
Time and location of the event: 15 April, 16.30-18.00, Kariri
Rapporteur: Carlos Cerqueira Jr.
Speakers:

- José Luis de la Cuesta, Association Internationale de Droit Pénal (AIDP-IAPL)
- Istituto Superiore Internazionale di Scienze Criminali
- Open Society Justice Initiative
- Penal Reform International
- ICPS
- OSI Special Initiatives Fund,
- Northwestern University.

Number of people in the audience: 32
Summary:
The issue of globalization and its impact on criminal law has been an issue of concern for the Association Internationale de Droit Pénal (AIDP) during recent years, which is why it has been involved in surveys that seek to analyse the capacity of an international criminal justice system to perfom as a unit in real time and worldwide.
The most prominent themes in the criminal context, on which international organizations develop studies in the search for effective solutions, are: terrorism, organized crime, corruption and cybercrime.
The issue of terrorism was included on the agenda of the first world conference on criminal law, which was held in November 2007 in Guadalajara, Mexico. Later, in 2009, in Istanbul, Turkey, the universal jurisdiction, the financing of terrorism, special procedural measures and observance of human rights, and the expansion of forms of punishment were discussed. Corruption was discussed at a congress in Beijing in 2004, where it was defined as a "deadly disease of democracies".
AIDP works through the Higher Institute of International Criminal Science (in Siracusa, Italy), international congresses, national groups and research activities. In 1999, at a congress held in Budapest, Hungary, the following resolutions were adopted: the need to properly organize the criminal justice intervention in order to cope with specific characteristics, the need to strengthen the effectiveness of international cooperation in criminal matters while adhering to principles of criminal law and fundamental human rights like proportionality and legality.
It was noted that the work of criminologists, lawyers and victimologists was necessary for the development of a culture of human rights (i.e., civilize globalization, build a criminal justice system that respects traditions but with democratic profiles in the service of people, social justice and peace).
It was argued that international judicial cooperation (e.g. on civil, administrative or penal issues), as well as administrative cooperation (e.g. police, intelligence services) are vital to the effectiveness of actions against the financing of terrorism. It is necessary to strengthen States' common actions. In all cases, respect for human rights must remain a priority.

72-Addressing the challenge of cybercrime: past, present and future
Session Coordinator: Marco Gercke (Gercke@cybercrime-institute.com) – UNODC/Microsoft
Time and location of the event: 15 April, 16.30-18.00, Juma
Rapporteurs: Bruno Stolze Lyrio and Giovanna Maria Sgaria de Morais
Speakers:

- T.J. Campana, Microsoft
- Marco Gercke, Cybercrime Research Institute
- Demostenes Chryssikos, United Nations Office on Drugs and Crimes
- Alexander Seger, Council of Europe
- Gilberto Martins de Almeida, Martins de Almeida Advogados

- Jan Neutze, Counter-Terrorism Implementation Task Force
- Gillian Murrary, United Nations Office on Drugs and Crimes
- Vashti Maharaj, Ministry of Public Administration of Trinidad Tobago

Number of people in the audience: around 25

Summary

Cybercrime can come in many forms and include crimes against the integrity of functional systems, damage against databases (in the case of fraud), intellectual piracy, pornography or many other practices. The lack of an international convention specifically against cybercrime is not a barrier for the application of sanction for the perpetrators. Regionally, the Council of Europe was promoting the Budapest Convention on Cybercrime.

At first, only European countries signed the Convention, but now the number of signatory States is increasing and expanding. The Convention covers procedural tools, measures for international cooperation and the criminalization of practices like illegal access, illegal interception, data interference, system interference, fraud and forgery, child pornography and IP-related offenses. Once ratified, the Convention works like a standard and, for that reason, States must make an effort to implement it. It is also important to know that the principles contained in the Convention can and should be supplemented by national instruments designed to combat cybercrime.

The Internet can also be used to commit acts of terrorism. If law enforcement officers can discover information about any preparation being done over the Internet, then a larger attack will probably not happen. There are new threats in the Internet, for that reason it is important to pay attention to these criminals acts, by combining know-how (technique) and legislation.

All over the world, there are cases of wrong use of the Internet. This has affected not only the security of information in developed countries but also in developing countries. There are only few studies about this practice in developing countries, where the response from Government has largely been weak.

Vashti Maharaj reminded listeners that developing countries are dealing with more challenges. In addition, victims of cybercrime do not look for help, it is difficult to get information and many countries simply do not have the skills and technologies to deal with cybercrime. State sovereignty can be a barrier to investigation because it leads authorities to not share the necessary information about any perpetrators located in their country.

Another problem lies in the fact that although many tools and instruments against cybercrime are already available (others are being developed), they are not necessarily implemented for lack of resources, capacity and commitment. This is why States must cooperate with civil society, to mobilize the population, to provide training to law enforcement and to work together with non-governmental experts.

Gilberto Martins de Almeida noted that cybercrime legislation requires a clear institutional and specialized legal and technical drafting. He also agreed that already existing laws regulating cybercrime and normative texts should be used as guidelines.

It is important to understand that the existence of norms at the international level is substantially similar and, for that reason, regional agendas shall be considered. Each country has its own principles and needs, which is why it is a cross-cultural challenge to have legislation that can be applied successfully.

There are some keys role to try to prevent this kind of practice, culture (good practices), education (doctrine), training (how to comply with) and inhibition (power of state to impose penalties). In addition, strengthening of legislation, training, high-tech crime units, international cooperation, protection of children, rule of law and human rights and political commitment

Finally, the representative of Microsoft remembered that cybercrime is a global problem and one way to fight against it is was to enter into public-private partnerships, as Microsoft does. Dialoguing within these partnerships is very important because just knowing what the problem is makes it possible to solve it.

73-Child online protection

Session Coordinator: Marco Gercke (gercke@cybercrime-institute.com) – UNODC

Time and place: 16 April, 14.30-16.00, Cocal

Speakers:

- Gillian Murray, United Nations Office on Drugs and Crime (introductory remarks)
- Nick Lampson, ICMEC
- Alexander Seger, Council of Europe
- T.J. Campana, Microsoft
- Ann Linnarsson, UNICEF
- Gilberto Martins de Almeida, Martins de Almeida Advogados Associados

Rapporteur: Giovanna Maria Sgaria de Morais

Summary

The Internet is a very powerful tool, but there is a lot of trash in it that should not be there, especially because children and teenagers are frequently online. The increase in crimes involving children prompted this session.

APÊNDICE 06 - Res. 55-63 da AG da ONU de 2000 - Combating the criminal misuse of information

General Assembly

Distr.: General
22 January 2001

Fifty-fifth session
Agenda item 105

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,[1] 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,[2] 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,[3] and noting in particular the resolution on computer-related crimes,[4] 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,

---

[1] See resolution 55/2.
[2] See A/55/3, chap. III. For the final text, see *Official Records of the General Assembly, Fifty-fifth Session, Supplement No. 3*.
[3] *Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Havana, 27 August–7 September 1990: report prepared by the Secretariat* (United Nations publication, Sales No. E.91.IV.2), chap I.
[4] Ibid., sect. C, resolution 9.

00 56317

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,[5]

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,[6]

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;

[5] See *Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Vienna, 10–17 April 2000: report prepared by the Secretariat* (United Nations publication, Sales No. E.00.IV.8).
[6] See REMJA-III/doc.14/00 rev. 2, chap. IV.

(*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

APÊNDICE 07 - Res. 56-121 da AG da ONU de 2001 - Combating the criminal misuse of information

General Assembly

Distr.: General
23 January 2002

Fifty-sixth session
Agenda item 110

Resolution adopted by the General Assembly

[*on the report of the Third Committee (A/56/574)*]

56/121. Combating the criminal misuse of information technologies

The General Assembly,

Recalling the United Nations Millennium Declaration,[1] in which Member States resolved to ensure that the benefits of new technologies, especially information and communications technologies, in conformity with the recommendations contained in the ministerial declaration of the high-level segment of the substantive session of 2000 of the Economic and Social Council,[2] are available to all, and its resolution 55/63 of 4 December 2000, in which it invited Member States to take into account measures to combat the criminal misuse of information technologies,

Recognizing that the free flow of information can promote economic and social development, education and democratic governance,

Noting the 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 recognizing also the need to facilitate the transfer of information technologies, in particular to developing countries,

---

[1] See resolution 55/2.

[2] See *Official Records of the General Assembly, Fifty-fifth Session, Supplement No. 3* (A/55/3/Rev.1), chap. III, para. 17.

01 48204

Noting the necessity of preventing the criminal misuse of information technologies,

Recognizing the need for cooperation between States and the private sector 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 the United Nations and other international and regional organizations,

Welcoming the work of the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders,

Recognizing with appreciation the work of the Commission on Crime Prevention and Criminal Justice at its ninth and tenth sessions and the subsequent preparation of a plan of action against high-technology and computer-related crime, which recognizes, inter alia, the need for effective law enforcement and the need to maintain effective protections for privacy and other related basic rights, as well as the need to take into account ongoing work in other forums,[3]

Noting the work of international and regional organizations in combating high-technology crime, including the work of the Council of Europe in elaborating the Convention on Cybercrime,[4] as well as the work of those organizations in promoting dialogue between government and the private sector on safety and confidence in cyberspace,

1. *Invites* Member States, when developing national law, policy and practice to combat the criminal misuse of information technologies, to take into account, as appropriate, the work and achievements of the Commission on Crime Prevention and Criminal Justice and of other international and regional organizations;

2. *Takes note* of the value of the measures set forth in its resolution 55/63, and again invites Member States to take them into account in their efforts to combat the criminal misuse of information technologies;

3. *Decides* to defer consideration of this subject, pending work envisioned in the plan of action against high-technology and computer-related crime of the Commission on Crime Prevention and Criminal Justice.[3]

88th plenary meeting
19 December 2001

[3] See *Official Records of the Economic and Social Council, 2001, Supplement No. 10* (E/2001/30/Rev.1), part two, chap. I.

[4] Council of Europe, *European Treaty Series*, No. 185.

APÊNDICE 08 – Convenção Européia sobre Cibercrimes

European Treaty Series - No. 185

CONVENTION ON CYBERCRIME

Budapest, 23.XI.2001

Preamble

The member States of the Council of Europe and the other States signatory hereto,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recognising the value of fostering co-operation with the other States parties to this Convention;

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, *inter alia*, by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;

Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;

Believing that an effective fight against cybercrime requires increased, rapid and well-functioning 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 part thereof.

3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

5 When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

Chapter III – International co-operation

Section 1 – General principles

Title 1 – General principles relating to international co-operation

Article 23 – General principles relating to international co-operation

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international 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 applicable multilateral or bilateral treaties or arrangements as between the Parties, including the provisions of:

- the European Convention on Extradition, opened for signature in Paris, on 13 December 1957 (ETS No. 24);
- the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 20 April 1959 (ETS No. 30);
- the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 17 March 1978 (ETS No. 99).

2 If two or more Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or have otherwise established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly. However, where Parties establish their relations in respect of the matters dealt with in the present Convention other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention's objectives and principles.

3 Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party.

Article 40 – Declarations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the possibility of requiring additional elements as provided for under Articles 2, 3, 6 paragraph 1.b, 7, 9 paragraph 3, and 27, paragraph 9.e.

Article 41 – Federal clause

1 A federal State may reserve the right to assume obligations under Chapter II of this Convention consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities provided that 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 which the notification is received by the Secretary General, the withdrawal shall take effect on such a later date.

2 A Party that has made a reservation as referred to in Article 42 shall withdraw such reservation, in whole or in part, as soon as circumstances so permit.

3 The Secretary General of the Council of Europe may periodically enquire with Parties that have made one or more reservations as referred to in Article 42 as to the prospects for withdrawing such reservation(s).

Article 44 – Amendments

1 Amendments to this Convention may be proposed by any Party, and shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention as well as to any State which has acceded to, or has been invited to accede to, this Convention in accordance with the provisions of Article 37.

2 Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Committee of Ministers its opinion on that proposed amendment.

3 The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the CDPC and, following consultation with the non-member States Parties to this Convention, may adopt the amendment.

4 The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 of this article shall be forwarded to the Parties for acceptance.

5 Any amendment adopted in accordance with paragraph 3 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

Article 45 – Settlement of disputes

1 The European Committee on Crime Problems (CDPC) shall be kept informed regarding the interpretation and application of this Convention.

2 In case of a dispute between Parties as to the interpretation or application of this Convention, they shall seek a settlement of the dispute through negotiation or any other peaceful means of their choice, including submission of the dispute to the CDPC, to an arbitral tribunal whose decisions shall be binding upon the Parties, or to the International Court of Justice, as agreed upon by the Parties concerned.

Article 46 – Consultations of the Parties

1 The Parties shall, as appropriate, consult periodically with a view to facilitating:

a the effective use and implementation of this Convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under this Convention;

b the exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form;

c consideration of possible supplementation or amendment of the Convention.

2 The European Committee on Crime Problems (CDPC) shall be kept periodically 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.

APÊNDICE 09 - Acompanhamento de Projetos de Lei

	A	B	C	D	E	F
1	**Tipo**	**Número**	**Ano**	**Autor**	**Ementa**	**Explicação da Ementa**
2	PL	4345	1998	Lúcio Alcântara	Institui a obrigatoriedade de as empresas operadoras de cartões de crédito oferecerem uma versão de cartão de crédito com foto digitalizada.	
3	PL	84	1999	Luiz Piauhylino	Dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências.	Caracteriza como crime informático ou virtual os ataques praticados por "hackers" e "crackers", em especial as alterações de "home pages" e a utilização indevida de senhas.
4	PL	1530	1999	Luiz Bittencourt	Acrescenta dois parágrafos ao art. 38 da Lei nº 8.666, de 21 de junho de 1993, que "regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências".	Estabelece que a administração pública deverá manter, na Internet, dados atualizados sobre o andamento dos processos de licitação.
5	PL	3016	2000	Antonio Carlos Pannunzio	Dispõe sobre o registro de transações de acesso a redes de computadores destinados ao uso público, inclusive a Internet.	
6	PLS	248	2002	Romeu Tuma	Acrescenta parágrafo único ao artigo 185 do Decreto-Lei nº 3689, de 3 de outubro de 1941 (Código de Processo Penal), e § 3º ao artigo 792 do mesmo diploma processual, para dispor sobre a realização de interrogatório a distância e a dispensa do comparecimento físico do acusado e das testemunhas nas audiências, mediante a utilização de recursos tecnológicos de presença virtual.	
7	PL	18	2003	Iara Bernardi	Veda o anonimato dos responsáveis por páginas na Internet e endereços eletrônicos registrados no País.	
8	PLS	95	2003	Valmir Amaral	Dispõe sobre a privacidade na Internet.	
9	PLS	279	2003	Delcídio Amaral	Dispõe sobre a prestação dos serviços de correio eletrônico, por intermédio da rede mundial de computadores - Internet, e dá outras providências.	
10	PLS	337	2003	Paulo Paim	Define o crime de veiculação de informações que induzam ou incitem a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional, na rede Internet, ou em outras redes destinadas ao acesso público.	
11	PLS	363	2003	Paulo Octávio	Torna obrigatória a inserção de mensagens alusivas aos danos decorrentes do consumo de drogas nas páginas da Internet.	

	A	B	C	D	E	F
12	PLS	367	2003	Hélio Costa	Coíbe a utilização de mensagens eletrônicas comerciais não solicitadas por meio de rede eletrônica.	
13	PLS	21	2004	Duciomar Costa	Disciplina o envio de mensagens eletrônicas comerciais.	
14	PLS	21	2004	Duciomar Costa	Disciplina o envio de mensagens eletrônicas comerciais.	
15	PLS	36	2004	Antonio Carlos Valadares	Dispõe sobre mensagens não solicitadas no âmbito da rede mundial de computadores (Internet).	
16	PLS	234	2004	Hélio Costa	Altera a Lei nº 9.504, de 30 de setembro de 1997 (Lei Eleitoral), para ampliar a segurança e a fiscalização do voto eletrônico.	
17	PLS	241	2004	Gerson Camata	Altera a Lei nº 9.504, de 30 de setembro de 1997 (Lei Eleitoral), para ampliar a segurança e a fiscalização do voto eletrônico mediante a emissão de comprovante de votação.	
18	PLS	296	2004	Aloísio Mercadante	Modifica a Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências, para tornar obrigatória a apresentação, na rede mundial de computadores (Internet), de documentos que tenham sido desclassificados em virtude do transcurso do prazo estabelecido para sua categoria.	
19	PLS	359	2004	Augusto Botelho	Altera a Lei nº 8.666, de 21 de junho de 1993, para o fim de determinar aos órgãos e entidades da Administração Pública o uso da Rede Mundial de Computadores nos procedimentos licitatórios e atos subseqüentes.	
20	PL	4144	2004	Marcos Abramo	Altera a Lei nº 8.069, de 13 de julho de 1990, a Lei nº 9.296, de 24 de julho de 1996, e o Decreto-Lei nº 2.848, de 7 de dezembro de 1940, e dá outras providências.	Tipifica o crime informático, praticado por "hackers", inclui os crimes de sabotagem, falsidade e fraude informática; autoriza as autoridades a interceptarem dados dos provedores e prevê a pena de reclusão para quem armazena, em meio eletrônico, material pornográfico, envolvendo criança e adolescente.
21	PLS	9	2005	Edison Lobão	Altera a Lei nº 5.172, de 25 de outubro de 1966 (Código Tributário Nacional), para admitir a conservação dos livros obrigatórios de escrituração comercial e fiscal em meio eletrônico que não permita regravação.	

	A	B	C	D	E	F
22	PLS	100	2005	Augusto Botelho	Altera a Lei nº 9.504, de 30 de setembro de 1997 (Lei Eleitoral), para ampliar a segurança e a fiscalização do voto eletrônico mediante a emissão de comprovante físico do voto e adoção de programas de computador abertos.	
23	PLC	114	2005	Wellington Fagundes	Dispõe sobre o atendimento pessoal ao consumidor nas empresas que oferecem atendimento por telefone, internet ou outro meio similar.	
24	PLS	148	2005	Serys Slhessarenko	Regulamenta as relações entre a Internet e a propaganda eleitoral e dá outras providências.	
25	PLS	211	2005	João Capiberibe	Altera o inciso III do art. 31 da Lei nº 8.987, de 13 de fevereiro de 1995, e inclui parágrafo no art. 35 da Lei nº 10.233, de 5 de junho de 2001, para prever publicação, na rede mundial de computadores (Internet), das informações acerca da gestão das prestadoras de serviços públicos e discrimina quais informações devem ser prestadas pelas concessionárias de rodovias.	
26	PLS	229	2005	Pedro Simon	Dispõe sobre a autenticidade e o valor jurídico e probatório de documentos produzidos, emitidos ou recebidos por órgaos públicos federais, estaduais e municipais, por meio eletrônico.	
27	PLS	317	2005	Romero Jucá	Dispõe sobre a tarifa telefônica nas ligações interurbanas a provedores de Internet.	
28	PL	6024	2005	Antonio Carlos Mendes Thame	Dispõe sobre crimes informáticos, alterando o Código Penal e regulando a disponibilidade dos arquivos dos provedores.	
29	PLS	170	2006	Valdir Raupp	Altera o art. 20 da Lei nº 7.716, de 5 de janeiro de 1989, para incluir, entre os crimes nele previstos, o ato de fabricar, importar, distribuir, manter em depósito ou comercializar jogos de videogames ofensivos aos costumes, às tradições dos povos, aos seus cultos, credos, religiões e símbolos.	
30	PLS	227	2006	Comissão Parlamentar Mista de Inquérito dos Correios (RQN 3/05)	Altera dispositivos da Lei nº 8.666, de 21 de junho de 1993 e 10.520, de 17 de julho de 2002, ampliando o âmbito de aplicação do pregão eletrônico e melhorando mecanismos de controle.	

	A	B	C	D	E	F
31	PLS	230	2006	Romeu Tuma	Altera a Lei nº 9.296, de 24 de julho de 1996, que "Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal", para que seja disciplinada a interceptação de comunicações de qualquer natureza.	
32	PLS	323	2006	Demóstenes Torres	Autoriza a utilização da internet como veículo de comunicação oficial.	
33	PL	6931	2006	João Batista	Dispõe sobre tipificação criminal de condutas na Internet.	Tipifica o "crime informático"; altera o Decreto-Lei nº 2.848, de 1940.
34	EMC	11	2007	Moreira Mendes	Dispõe sobre a produção, programação, empacotamento e distribuição de conteúdo eletrônico e dá outras providências.	
35	PRC	102	2007	Miguel Martini	Acrescenta inciso ao art. 37 do Regimento Interno da Câmara dos Deputados.	Determina que findo o trabalho das Comissões Parlamentares de Inquérito sejam digitalizados e disponibilizados, em meio eletrônico, toda a documentação produzida.
36	PLS	146	2007	Magno Malta	Dispõe sobre a digitalização e arquivamento de documentos em mídia ótica ou eletrônica, e dá outras providências.	
37	PLS	154	2007	Lúcia Vânia	Altera a Lei nº 8.078, de 11 de setembro de 1990, que dispõe sobre a proteção do consumidor e dá outras providências, para impor ao fornecedor a disponibilização, nos contratos formalizados por meio eletrônico, de opção para cancelamento de contratos de fornecimento de produtos e de serviços.	
38	PLS	231	2007	Antonio Carlos Valadares	Altera a Lei nº 5.869, de 11 de janeiro de 1973 (Código de Processo Civil), para estabelecer ressalvas ao procedimento de exibição de coisa ou documento quando se tratar de informação armazenada eletronicamente.	
39	PLS	280	2007	Flexa Ribeiro	Dispõe sobre a produção, programação e provimento de conteúdo brasileiro para distribuição por meio eletrônico e dá outras providências.	

	A	B	C	D	E	F
40	PLS	288	2007	Valdir Raupp	Acrescenta parágrafo único ao art. 121, altera o art. 126 e acrescenta parágrafo único ao art. 127 da Lei nº 6.404, de 15 de dezembro de 1976, para permitir a participação em assembléia-geral por meio de assinatura eletrônica e certificação digital, e para instituir o requisito de depósito prévio do instrumento de mandato para a representação do acionista em assembléia-geral.	
41	PLS	538	2007	Adelmir Santana	Dispõe sobre extrato de cadastro eletrônico e os procedimentos a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil na prestação de serviços aos clientes.	
42	PLS	542	2007	Marcelo Crivela	Altera a Lei nº 8.078, de 11 de setembro de 1990, Código de Defesa do Consumidor, para dispor sobre os serviços de atendimento personalizado ao consumidor, realizados por meios eletrônicos, fac-símile, correio de voz, internet e outras formas de Serviço de Atendimento ao Consumidor (SACs) ou Centrais de Atendimento Telefônico (call centers).	
43	PLS	607	2007	Expedito Júnior	Dispõe sobre a regulamentação do exercício da profissão de Analista de Sistemas e suas correlatas, cria o Conselho Federal e os Conselhos Regionais de Informática e dá outras providências.	
44	PL	717	2007	Cezar Silvestri	Estabelece critérios para a inscrição de atos constitutivos no Registro Civil das Pessoas Jurídicas, incorporando o registro eletrônico.	
45	PLS	735	2007	Romeu Tuma	Dispõe sobre o Serviço de Atendimento Pessoal ao Consumidor pelos fornecedores que oferecem atendimento em balcão, por telefone, internet ou outra forma de telecomunicação eletrônica.	
46	PLS	736	2007	Romeu Tuma	Altera dispositivos do Decreto-Lei 3.689, de 3 de outubro de 1941 - Código de Processo Penal, para prever a realização de interrogatório do acusado preso por videoconferência.	

	A	B	C	D	E	F
47	PL	979	2007	Chico Alencar	Acrescenta artigo à Lei nº 8.078, de 11 de setembro de 1990, para obrigar os fornecedores que ofertam ou comercializam produtos ou serviços pela rede mundial de computadores a informarem seu endereço para fins de citação, bem como o número de telefone e endereço eletrônico utilizáveis para atendimento de reclamações de consumidores.	
48	PL	1481	2007	Aloísio Mercadante	Altera a Lei nº 9.394, de 20 de dezembro de 1996, e a Lei nº 9.998, de 17 de agosto de 2000, para dispor sobre o acesso a redes digitais de informação em estabelecimentos de ensino.	Estabelece o prazo até 31 de dezembro de 2013 para que todos os estabelecimentos de educação básica e superior do País disponham de acesso à Internet; destina 75% (setenta e cinco por cento) dos recursos do FUST, a partir de 2008, para equipar os estabelecimentos de ensino com redes digitais de informação e recursos da tecnologia da informação.
49	PL	1704	2007	Rodovalho	Altera o art. 151 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal.	Tipifica como crime de violação de correspondência a violação de correspondências e comunicaçoes eletrônicas.
50	PL	1751	2007	Comissão de Legislação Participativa	Regula a utilização da Internet como veículo de publicação oficial.	
51	PL	2246	2007	Pompeo de Mattos	Veda o uso de telefones celulares nas escolas públicas de todo o país.	
52	PL	2339	2007	Alex Canziani	Altera a Lei nº 6.015, de 31 de dezembro de 1973, na parte relativa ao Registro Civil das Pessoas Jurídicas.	Estabelece critérios para a inscrição de atos constitutivos no Registro Civil das Pessoas Jurídicas, incorporando o registro eletrônico.
53	PL	2344	2007	Marcondes Gadelha	Dispõe sobre obrigatoriedade de segurança eletrônica para cartões de crédito.	
54	PL	2634	2007	Valtenir Pereira	Dispõe sobre a implantação do Sistema Nacional de Cadastro da Saúde a ser utilizado no armazenamento e gerenciamento, on line, dos registros clínicos dos pacientes.	Institui o cartão SUS

	A	B	C	D	E	F
55	PL	2710	2007	Luiz Carlos Busato	Dispõe sobre a implantação do Portal Único de Ações Governamentais e Serviços Eletrônicos com o objetivo de integrar sistemas e disponibilizar na rede mundial de computadores os programas públicos nas esferas federal, estadual e municipais.	
56	PLS	121	2008	Magno Malta	Proíbe as empresas de cartões de pagamento de autorizarem transações relacionadas com jogos de azar e pornografia infantil via rede mundial de computadores.	
57	PLC	170	2008	Sandra Rosado	Acrescenta o art. 375-A à Lei nº 5.869, de 11 de janeiro de 1973 - Código de Processo Civil. (Inclui o e-mail como prova documental).	
58	PLS	291	2008	Expedito Júnior	Altera o art. 36 e o § 3º do art. 45 da Lei n° 9.504, de 30 de setembro de 1997, para permitir a propaganda eleitoral pela Internet.	
59	PLS	296	2008	Gerson Camata	Obriga os estabelecimentos de locação de terminais de computadores a manterem cadastro de seus usuários.	
60	PLS	494	2008	Comissão Parlamentar de Inquérito - Pedofilia	Disciplina a forma, os prazos e os meios de preservação e transferência de dados informáticos mantidos por fornecedores de serviço a autoridades públicas, para fins de investigação de crimes praticados contra crianças e adolescentes, e dá outras providências.	
61	PL	2899	2008	William Woo	Obriga as operadoras de telefonia fixa e móvel ao pagamento de multa em razão de danos decorrentes da ineficiência em garantir a privacidade de seus usuários.	
62	PL	3030	2008	Carlos Bezerra	Dispõe sobre o uso de criptografia em peticionamento eletrônico.	Altera a Lei nº 11.419, de 2006.
63	PL	3369	2008	Carlos Bezerra	Torna obrigatória a inserção nos vídeos dos monitores dos computadores comercializados no país a advertência de que o uso indevido do computador pode gerar infrações que sujeitam o usuário à responsabilização administrativa, penal e cível.	Deverá inserir a seguinte advertência: "O uso indevido do computador pode gerar infrações que sujeitam o usuário à responsabilização administrativa, cível e penal."
64	PL	3456	2008	Costa Ferreira	Dispõe sobre o agravamento da pena cominada a crime praticado através de rede mundial de computadores.	Altera o Decreto-Lei nº 2.848, de 1940.
65	PL	3486	2008	Eliene Lima	Proíbe o uso de aparelhos eletrônicos portáteis nas salas de aula dos estabelecimentos de educação básica e superior.	Inclui o aparelho celular, a internet, MP3 e MP4

	A	B	C	D	E	F
66	PL	4084	2008	Edinho Bez	Altera a Lei nº 5.474, de 18 de julho de 1968, que "Dispõe sobre as duplicatas e dá outras providências" para incluir novo artigo permitindo a emissão de duplicata por meio eletrônico.	
67	PLS	173	2009	João Tenório	Estabelece prazo para que computadores, componentes de computadores e equipamentos de informática em geral, comercializados no Brasil, atendam a requisitos ambientais e de eficiência energética.	
68	PL	5298	2009	Jefferson Campos	Dispõe sobre a identificação dos usuários dos serviços de correio eletrônico.	
69	PL	5322	2009	Cleber Verde	Dispõe sobre o direito de resposta na imprensa falada, escrita, televisiva, cinematográfica e em outros meios de comunicação inclusive eletrônico.	
70	PL	5361	2009	Bispo Gê Tenuta	Cria penalidades civis para a baixa, download ou compartilhamento de arquivos eletrônicos na Internet, que contenham obras artísticas ou técnicas protegidas por direitos de propriedade intelectual, sem autorização dos legítimos titulares das obras.	Altera a Lei nº 9.610, de 1998.
71	PL	5369	2009	Vieira da Cunha	Institui o Programa de Combate ao "Bullying".	

APÊNDICE 10 – Projeto de Lei 84/99

PROJETO DE LEI Nº 84 DE 1999

(Do Sr. Luiz Piauhylino)

Dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências.

O Congresso Nacional decreta:

CAPÍTULO I

DOS PRINCÍPIOS QUE REGULAM A PRESTAÇAO DE SERVIÇO POR REDES DE COMPUTADORES

Art. 1º - O acesso, o processamento e a disseminação de informações através das redes de computadores devem estar a serviço do cidadão e da sociedade, respeitados os critérios de garantia dos direitos individuais e coletivos e de privacidade e segurança de pessoas físicas e jurídicas e da garantia de acesso às informações disseminadas pelos serviços da rede.

Art. 2º - É livre a estruturação e o funcionamento das redes de computadores e seus serviços, ressalvadas as disposições específicas reguladas em lei.

CAPÍTULO II

DO USO DE INFORMAÇÕES DISPONÍVEIS EM COMPUTADORES OU REDES DE COMPUTADORES.

Art. 3º - Para fins desta lei, entende-se por informações privadas aquelas relativas a pessoa física ou jurídica identificada ou identificável.

Parágrafo único. É identificável a pessoa cuja individuação não envolva custos ou prazos desproporcionados.

Art. 4º - Ninguém será obrigado a fornecer informações sobre sua pessoa ou de terceiros, salvo nos casos previstos em lei.

Art. 5º - A coleta, o processamento e a distribuição, com finalidades comerciais, de informações privadas ficam sujeitas à prévia aquiescência da pessoa a que se referem, que poderá ser tomada sem efeito a qualquer momento, ressalvando-se o pagamento de indenizações a terceiros, quando couberem.

§ 1º. A toda pessoa cadastrada dar-se-á conhecimento das informações privadas armazenadas e das respectivas fontes.

§ 2º. Fica assegurado o direito à retificação de qualquer informação privada incorreta.

§ 3º. Salvo por disposição legal ou determinação judicial em contrário, nenhuma informação privada será mantida à revelia da pessoa a que se refere ou além do tempo previsto para a sua validade.

§ 4º. Qualquer pessoa, física ou jurídica, tem o direito de interpelar o proprietário de rede de computadores ou provedor de serviço para saber se mantém informações a seu respeito, e o respectivo teor.

Art. 6º - Os serviços de informações ou de acesso a bancos de dados não distribuirão informações privadas referentes, direta ou indiretamente, a origem racial, opinião política, filosófica, religiosa ou de orientação sexual, e de filiação a qualquer entidade, pública ou privada, salvo autorização expressa do interessado.

Art. 7º - O acesso de terceiros, não autorizados pelos respectivos interessados, a informações privadas mantidas em redes de computadores dependerá de prévia autorização judicial.

CAPÍTULO III

DOS CRIMES DE INFORMÁTICA

Seção I
Dano a dado ou programa de computador

Art. 8º - Apagar, destruir, modificar ou de qualquer forma inutilizar, total ou parcialmente, dado ou programa de computador, de forma indevida ou não autorizada.

Pena: detenção, de um a três anos e multa.

Parágrafo único. *Se* o crime é cometido:

I - contra o interesse da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;

II- com considerável prejuízo para a vítima;

III - com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;

IV - com abuso de confiança;

V - por motivo fútil;

VI - com o uso indevido de senha ou processo de identificação de terceiro , ou

VII - com a utilização de qualquer outro meio fraudulento.

Pena: detenção, de dois a quatro anos e multa.

Seção II
Acesso indevido ou não autorizado

Art. 9º Obter acesso, indevido ou não autorizado, a computador ou rede de computadores.

Pena: detenção, de seis meses a um ano e multa.

Parágrafo primeiro. Na mesma pena incorre quem. sem autorização ou indevidamente, obtém, mantém ou fornece a terceiro qualquer meio de identificação ou acesso a computador ou rede de computadores.

Parágrafo segundo. *Se* o crime é cometido:

I - com acesso a computador ou rede de computadores da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;

II - com considerável prejuízo para a vítima;

III - com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;

IV - com abuso de confiança;

V - por motivo fútil;

VI - com o uso indevido de senha ou processo de identificação de terceiro; ou

VII - com a utilização de qualquer outro meio fraudulento.

Pena: detenção, de um a dois anos e multa.

Seção III
Alteração de senha ou mecanismo de acesso
a programa de computador ou dados

Art. 10. Apagar, destruir, alterar, ou de qualquer fama inutilizar, senha ou qualquer outro mecanismo de acesso a computador, programa de computador ou dados, de forma indevida ou não autorizada.

Pena: detenção, de um a dois anos e multa.

Seção IV
Obtenção indevida ou não autorizada de dado
ou instrução de computador

Parágrafo Único. Se o crime é cometido:

I - com acesso a computador ou rede de computadores da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;

II - com considerável prejuízo para a vítima;

Art. 11 - Obter, manter ou fornecer, sem autorização ou indevidamente, dado ou instrução de computador.

Pena: detenção, de três meses a um ano e multa.

Parágrafo Único. Se o crime é cometido:

I - com acesso a computador ou rede de computadores da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;

II - com considerável prejuízo para a vítima;

III - com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;

IV - com abuso de confiança;

V - por motivo fútil;

VI - com o uso indevido de senha ou processo de identificação de terceiro; ou

VII - com a utilização de qualquer outro meio fraudulento.

Pena: detenção, de um a dois anos e multa.

Seção V
Violação de segredo armazenado em computador, meio magnético ,
de natureza magnética, óptica ou similar

Art. 12. Obter segredos, de indústria ou comércio, ou informações pessoais armazenadas em computador, rede de computadores, meio eletrônico de natureza magnética, óptica ou similar, de forma indevida ou não autorizada.

Pena: detenção, de um a três anos e multa.

Seção VI
Criação, desenvolvimento ou inserção em computador de dados ou programa de computador c nocivos

Art. 13. Criar, desenvolver ou inserir, dado ou programa em computador ou rede de computadores, de forma indevida ou não autorizada com a finalidade de apagar, destruir, inutilizar ou modificar dado ou programa de computador ou de qualquer forma dificultar ou impossibilitar, total ou parcialmente, a utilização de computador ou rede de computadores.

Pena: reclusão, de um a quatro anos e multa.

Parágrafo único. Se o crime é cometido:

I - contra a interesse da União, Estado, Distrito Federal. Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;
II - com considerável prejuízo para a vítima;
III - com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;
IV - com abuso de confiança;
V - por motivo fútil;
VI - com o uso indevid6 de senha ou processo de Identificação de terceiro; ou
VII - com a utilização de qualquer outro meto fraudulento.

Pena: reclusão, de dois a seis anos e multa.

Seção VII
Veiculação de pornografia através de rede de computadores

Art. 14 - Oferecer serviço ou informação de caráter pornográfico, em rede de computadores, sem exibir, previamente, de forma facilmente visível e destacada, aviso sobre sua natureza, indicando o seu conteúdo e a inadequação para criança ou adolescentes.

Pena: detenção, de um a três anos e multa.

CAPITULO IV

DAS DISPOSIÇÕES FINAIS

Art. 15 - Se qualquer dos crimes previstos nesta lei é praticado no exercício de atividade profissional ou funcional, a pena é aumentada de um sexto até a metade.

Art. 16 - Nos crimes definidos nesta lei somente se procede mediante representação do ofendido, salvo se cometidos contra o interesse da União, Estado, Distrito

Federal Município, órgão ou entidade da administração direta ou indireta, empresa concessionária de serviços públicos, fundações instituídas ou mantidas pelo poder público, serviços sociais autônomos, instituições financeiras ou empresas que explorem ramo de atividade controlada pelo poder público, casos em que a ação é pública incondicionada.

Art. 17 - Esta lei regula os crimes relativos à informática sem prejuízo das demais comunicações previstas em outros diplomas legais.

Art 18. Esta lei entra em vigor 30 (trinta) dias a contar da data de sua publicação.

JUSTIFICAÇÃO

Na legislatura passada o ilustre Deputado Cássio Cunha Lima apresentou o PL 1.713196 que dispõe sobre o acesso, a responsabilidade e os crimes cometido nas redes integradas de computadores. Na justificativa do nobre Deputado, houve a preocupação com a informação dessas redes de computadores em verdadeiros mercados, no sentido econômico da palavra, onde pessoas conversam, trocam informações e realizam transações comerciais, não existindo porém nenhuma legislação específica que regule as responsabilidade dos agentes envolvidos.

Distribuído inicialmente à Comissão de Ciência e Tecnologia, Comunicação e Informática, o PL 1.713/96 foi encaminhado a minha pessoa para ser o Relator do mesmo. Iniciei a discussão na comissão, inclusive com convocação de audiência publica e, em seguida com pessoas da área de informática, buscando identificar um texto que tratasse a matéria de uma forma mais global. Sob a coordenação do professor José Henrique Barbosa Moreira Lima Neto formou-se um, grupo composto dos seguintes membros:

- Dr. Damásio Evangelista de Jesus, advogado(SP)
- Dr. Gilberto Martins de Almeida, advogado (RJ)
- Dr. Ivan Lira de Carvalho, Juiz Federal (RN)
- Dr. Mário César Monteiro Machado, Juiz Auditor Militar (RJ) - Dr. Carlos Alberto Etcheverry, Juiz de Direito (RS)
- Dr. Júlio César Finger, Promotor de Justiça (RS)
- Dra. Marília Cohen Goldman, Promotora de Justiça (RS)
- Dra. Lígia Leindecker Futterrleib, advogada (RS)
- Dr. Paulo Sérgio Fabião, Desembargador (RJ).

Este grupo, depois de vários debates "on-line" apresentou-me urna minuta do substitutivo ao referido PL 1.713196. Ocorre que, por falta de tempo suficiente o substitutivo não foi devidamente apreciado, inclusive pelas demais comissões da Câmara dos Deputados, durante a legislatura passada, razão pela qual o PL foi arquivado. Portanto apresento agora o PL acima , o qual é resultado de um trabalho sério, depois de ouvir a sociedade, através de pessoas da mais alta qualificação.

Não podemos permitir que pela falta de lei, que regule os crimes de informática, pessoas inescrupulosas continuem usando computadores e suas redes para propósitos escusos e criminosos. Dai a necessidade de uma lei que, defina os crimes cometidos na rede de informática e suas respectivas penas.

Sala das Sessões, em de de 1.999.

Deputado LUIZ PIAUHYLINO

SUBSTITUTIVO AO PROJETO DE LEI Nº 84, DE 1999

(Do Sr. Luiz Piauhylino)

Dispõe sobre os crimes de informática, suas penalidades e outras providências.

O Congresso Nacional decreta:

CAPÍTULO I

DOS PRINCÍPIOS QUE REGULAM A PRESTAÇÃO DE SERVIÇO POR REDES DE COMPUTADORES

Art. 1º. O acesso, o processamento e a disseminação de informações através das redes de computadores devem estar a serviço das pessoas naturais e jurídicas, estas no que couber, e da sociedade, respeitados os direitos fundamentais, especialmente os direitos à intimidade e à segurança no acesso às informações veiculadas em rede de computadores.

Art. 2º. É livre a estruturação e o funcionamento das redes de computadores e seus serviços, ressalvadas as disposições específicas reguladas em lei.

CAPÍTULO II

DO USO DE INFORMAÇÕES DISPONÍVEIS EM COMPUTADORES OU REDES DE COMPUTADORES

Art. 3º. Para fins desta lei, entende-se por informações privadas aquelas relativas inerentes à pessoa natural ou jurídica identificada ou identificável.

Parágrafo Único. É identificável a pessoa cuja individuação não envolva custos ou prazos desarrazoados.

Art. 4º. Ninguém será obrigado a fornecer informações próprias ou de terceiros, salvo nos casos previstos em lei.

Art. 5º. A coleta, o processamento e a distribuição, com finalidade comercial, de informações privadas ficam sujeitas à prévia autorização da pessoa a que se referem, que poderá ser tornada sem

24/02/99

efeito a qualquer momento, assegurado o ressarcimento por dano material ou moral, quando couber.

§ 1º. A toda pessoa cadastrada dar-se-á conhecimento das informações privadas armazenadas e das respectivas fontes.

§ 2º. Fica assegurado o direito à retificação de qualquer informação privada incorreta, assim como o de contestação ou explicação sobre dado verdadeiro mas justificável e que esteja sob pendência judicial ou amigável.

§ 3º. Salvo por disposição legal ou determinação judicial em contrário, nenhuma informação privada será mantida à revelia da pessoa a que se refere ou além do tempo previsto para a sua validade.

§ 4º. Qualquer pessoa, natural ou jurídica, tem o direito de interpelar o proprietário de rede de computadores ou provedor de serviço para saber se mantém informações a seu respeito e o respectivo teor.

Art. 6º. Os serviços de informações ou de acesso a bancos de dados não distribuirão informações privadas referentes, direta ou indiretamente, a origem racial, opinião política, filosófica, religiosa ou de orientação sexual, e de filiação a qualquer entidade, pública ou privada, salvo autorização expressa do interessado.

Art. 7º. O acesso de terceiros, não autorizados pelos respectivos interessados, a informações privadas mantidas em redes de computadores dependerá de prévia autorização judicial.

CAPÍTULO III

DOS CRIMES DE INFORMÁTICA

Seção I Dano a dado ou programa de computador

Art. 8º. Apagar, destruir, modificar ou de qualquer forma inutilizar, total ou parcialmente, dado ou programa de computador, de forma indevida ou não autorizada:

Pena: detenção, de um a três anos e multa.

Parágrafo único. Se o crime é cometido:

I – contra o interesse da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;

II – com considerável prejuízo material ou moral para a vítima;

III – com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;

IV – com abuso de confiança;

V – com o uso indevido de senha ou processo de identificação de terceiro; ou

VI – com a utilização de qualquer outro meio fraudulento.

Pena: detenção, de dois a quatro anos e multa

Seção II Acesso indevido ou não autorizado

Art. 9º. Acessar de forma indevida ou não autorizada, computador ou rede de computadores:

Pena: detenção, de seis meses a um ano e multa.

§ 1º. Se o crime é cometido:

I – com acesso a computador ou rede de computadores da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;

II – com considerável prejuízo material ou moral para a vítima;

III – com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;

IV – com abuso de confiança;

V – com o uso indevido de senha ou processo de identificação de terceiro; ou

VI – com a utilização de qualquer outro meio fraudulento.

Pena: detenção, de um a dois anos e multa.

§ 2º. Na mesma pena incorre quem obtém ou facilita a obtenção, mantém ou fornece a terceiro qualquer meio de identificação ou acesso a computador ou rede de computadores.

Seção III Alteração de senha ou mecanismo de acesso a Programa de computador ou dados

Art. 10. Apagar, destruir ou de qualquer forma inutilizar, senha ou qualquer outro mecanismo de acesso a computador, programa de computador ou dados, de forma indevida ou não autorizada:

Pena: detenção, de um a dois anos e multa.

Parágrafo único. O autor é punível ainda que permaneça a possibilidade de acesso ao computador, programa de computador ou dados.

Seção IV Obtenção indevida ou não autorizada de dado ou instrução de computador

Art. 11. Obter, manter ou fornecer, sem autorização ou indevidamente, dado ou instrução de computador:

Pena: detenção, de três meses a um ano e multa.

Parágrafo único. Se o crime é cometido:

I – com acesso a computador ou rede de computadores da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;

II – com considerável prejuízo material ou moral para a vítima;

III – com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;

IV – com abuso de confiança;

V – com o uso indevido de senha ou processo de identificação de terceiro; ou

VI – com a utilização de qualquer outro meio fraudulento.

Pena: detenção, de um a dois anos e multa

Seção V Violação de segredo armazenado em computador, meio magnético, de natureza magnética, óptica ou similar

Art. 12. Obter segredos, de indústria ou comércio, ou informações pessoais armazenadas em computador, rede de computadores, meio eletrônico de natureza magnética, óptica ou similar, de forma indevida ou não autorizada:

Pena: detenção, de um a três anos e multa.

§ 1º. Considera-se segredo de indústria um método ou meio especial de fabricação, patenteável ou não que é mantido em sigilo.

§ 2º. Considera-se segredo de comércio todas as informações especiais concernentes ao âmbito dos negócios em geral que devem ser mantidas sob reserva, sob risco de causar prejuízo.

§ 3º. Aplica-se a pena imposta neste artigo sem prejuízo de outros crimes cometidos pelo autor.

Seção VI Criação, desenvolvimento ou inserção em computador de Dados ou programa de computador com fins nocivos

Art. 13. Criar, desenvolver ou inserir, dado ou programa em computador ou rede de computadores, de forma indevida ou não autorizada, com a finalidade de apagar, destruir,

inutilizar ou modificar dado ou programa de computador ou de qualquer forma dificultar ou impossibilitar, total ou parcialmente, a utilização de computador ou rede de computadores:

Pena: reclusão, de um a quatro anos e multa.

Parágrafo único. Se o crime é cometido:

I – contra a interesse da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;

II – com considerável prejuízo material ou moral para a vítima;

III – com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;

IV – com abuso de confiança;

V – com o uso indevido de senha ou processo de identificação de terceiro; ou

VI – com a utilização de qualquer outro meio fraudulento.

Pena: reclusão, de dois a seis anos e multa.

Seção VII Veiculação de pornografia através de rede de computadores

Art. 14. Oferecer serviço ou informação de caráter pornográfico ou de sexo explícito, em rede de computadores, sem exibição prévia, de forma facilmente visível e destacada, aviso sobre sua natureza, indicando o seu conteúdo e a inadequação para criança ou adolescente:

Pena: detenção, de um a três anos e multa.

Art. 15. Publicar em rede de computadores cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:

Pena: reclusão, de dois a seis anos e multa.

CAPÍTULO IV DAS DISPOSIÇÕES FINAIS

Art. 16. Se qualquer dos crimes previstos nesta lei é praticado no exercício de atividade profissional ou funcional, a pena é aumentada de um sexto até a metade.

Art. 17. Os crimes definidos nesta lei somente se procede mediante representação do ofendido, salvo nas hipóteses dos artigos 14 e 15 acima ou se cometidos contra o interesse da União, Estados, Distrito Federal Município, órgão ou entidade da administração direta ou indireta, empresa concessionária de serviços públicos, fundações instituídas ou mantidas pelo poder público, serviços sociais autônomos, instituições financeiras ou empresas que explorem ramo de atividade controlada pelo poder público, casos em que a ação é pública incondicionada.

Art. 18. Esta lei regula os crimes relativos à informática sem prejuízo das demais cominações previstas em outros diplomas legais.

Art. 19. Esta lei entra em vigor 30 (trinta) dias a contar da data de sua publicação.

APÊNDICE 11 - Anteprojeto de Lei do Marco Civil para brasileira

O **CONGRESSO NACIONAL** decreta:

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

(11 Comentários)

Art. 1º

(14 Comentários)

Esta Lei estabelece direitos e deveres relativos ao uso da Internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.

(14 Comentários)

Art. 2º

(10 Comentários)

A disciplina do uso da Internet no Brasil tem como fundamentos o reconhecimento da escala mundial da rede, o exercício da cidadania em meios digitais, os direitos humanos, a pluralidade, a diversidade, a abertura, a livre iniciativa, a livre concorrência e a colaboração, e observará os seguintes princípios:

(14 Comentários)

I – garantia da liberdade de expressão, comunicação e manifestação de pensamento;

(30 Comentários)

II – proteção da privacidade;

(25 Comentários)

III – proteção aos dados pessoais, na forma da lei;

(8 Comentários)

IV – preservação e garantia da neutralidade da rede;

(15 Comentários)

V – preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas; e

(9 Comentários)

VI – preservação da natureza participativa da rede.

(16 Comentários)

Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria, ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

(4 Comentários)

Art. 3º

(4 Comentários)

A disciplina do uso da Internet no Brasil tem os seguintes objetivos:

(4 Comentários)

I – garantir a todos os cidadãos o acesso à Internet;

(18 Comentários)

II – promover o acesso à informação, ao conhecimento e à participação na vida cultural;

(6 Comentários)

III – fortalecer a livre iniciativa e a livre concorrência;

(6 Comentários)

IV – promover a inovação e fomentar a ampla difusão de novas tecnologias e modelos de uso e acesso; e

(4 Comentários)

V – promover a padronização, a acessibilidade e a interoperabilidade, a partir do uso de padrões abertos.

(11 Comentários)

Art. 4º

(5 Comentários)

Para os efeitos desta Lei, considera-se:

(5 Comentários)

I – Internet: o conjunto de meios de transmissão, comutação e roteamento de dados, estruturados em escala mundial, bem como os protocolos necessários à comunicação entre terminais, incluídos ainda os programas de computador específicos para esse fim;

(8 Comentários)

II – terminal: computador ou dispositivo análogo que se conecte à Internet;

(21 Comentários)

III – administrador de sistema autônomo: pessoa jurídica, devidamente cadastrada junto ao Registro de Endereçamento da Internet para América Latina e Caribe (LACNIC), responsável por blocos específicos de número IP (*/internet protocol*) e por um conjunto de roteadores, redes e linhas de comunicação pela Internet que formem uma infraestrutura delimitada por protocolos e métricas comuns.

(6 Comentários)

IV – conexão à Internet: autenticação de um terminal para envio e recebimento de pacotes de dados pela Internet, mediante a atribuição de um número IP;

(8 Comentários)

V – registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à Internet, sua duração e o número IP utilizado pelo terminal para o recebimento de pacotes de dados;

(25 Comentários)

VI – serviços de Internet: conjunto de serviços diversos que podem ser acessados por meio de um terminal conectado à Internet, como, por exemplo, navegação, comunicação instantânea, envio e recebimento de correspondência eletrônica, publicação de obras textuais ou audiovisuais em formato digital, entre outros;

(13 Comentários)

VII – registros de acesso a serviços de Internet: o conjunto de informações referentes à data e hora de uso de um determinado serviço de Internet a partir de um determinado número IP.

(5 Comentários)

Art. 5º

(9 Comentários)

Na interpretação desta Lei, levar-se-ão em conta, além dos fundamentos, princípios e objetivos previstos, a natureza da Internet, seus usos e costumes particulares e sua importância para a promoção do desenvolvimento humano, econômico, social e cultural, as exigências do bem comum, e os direitos e deveres individuais e transindividuais.

(9 Comentários)

CAPÍTULO II
DOS DIREITOS E GARANTIAS DOS USUÁRIOS

(Sem comentários)

Art. 6º

(24 Comentários)

O acesso à Internet é direito do cidadão, fundamental ao exercício da cidadania, às liberdades de manifestação do pensamento e de expressão e à garantia do acesso à informação.

(24 Comentários)

Art. 7º

(7 Comentários)

O usuário de Internet tem direito:

(4 Comentários)

I – à inviolabilidade e ao sigilo de suas comunicações, salvo por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

(19 Comentários)

II – à não suspensão ou degradação da qualidade contratada da conexão à Internet, nos termos do art. 12, salvo por débito diretamente decorrente de sua utilização;

(16 Comentários)

III – a informações claras e completas constantes dos contratos de prestação de serviços, estabelecendo o regime de proteção aos seus dados pessoais, registros de conexão e registros de acesso a serviços de Internet, bem como sobre práticas de gerenciamento da rede que possam afetar a qualidade do serviço oferecido; e

(3 Comentários)

IV – à não divulgação ou uso de seus registros de conexão e registros de acesso a serviços de Internet, salvo mediante seu consentimento expresso ou em decorrência de determinação judicial.

(12 Comentários)

Art. 8º

(Sem comentários)

A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à Internet.

(6 Comentários)

Parágrafo único. O exercício do direito à privacidade e à liberdade de expressão autoriza aos usuários da Internet a livre opção por medidas de segurança direcionadas a salvaguardar a proteção de dados pessoais e o sigilo das comunicações.

(7 Comentários)

CAPÍTULO III
A PROVISÃO DE CONEXÃO E DE SERVIÇOS DE INTERNET

(1 Comentário)

Seção I
Disposições Gerais

(Sem comentários)

Art. 9º

(Sem comentários)

A provisão de conexão à Internet impõe a obrigação de guardar apenas os registros de conexão, nos termos da Subseção I da Seção III deste Capítulo, ficando vedada a guarda de registros de acesso a serviços de Internet pelo provedor.

(25 Comentários)

Parágrafo único. O provedor de conexão a Internet fica impedido de monitorar, filtrar, analisar ou fiscalizar o conteúdo dos pacotes de dados, salvo para administração técnica de tráfego, nos termos do art 12.

(11 Comentários)

Art. 10

(Sem comentários)

A provisão de serviços de Internet, onerosa ou gratuita, não impõe ao provedor a obrigação de monitorar, filtrar, analisar ou fiscalizar o conteúdo dos pacotes de dados, tampouco de guardar registros de acesso a serviços de Internet, salvo, em qualquer dos casos, por ordem judicial específica, observado o disposto no art. 18.

(16 Comentários)

Parágrafo único. Para efeitos deste dispositivo, os usuários que detenham poderes de moderação sobre o conteúdo de terceiros se equiparam aos provedores de serviços de Internet.

(12 Comentários)

Art. 11

(5 Comentários)

A responsabilização do provedor de serviços de Internet por danos decorrentes de conteúdo gerado por terceiros fica condicionada ao descumprimento dos procedimentos previstos na Seção IV deste Capítulo.

(5 Comentários)

Seção II

Do tráfego de dados

(Sem comentários)

Art. 12

(17 Comentários)

O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, conteúdo, serviço, terminal ou aplicativo, sendo vedado estabelecer qualquer discriminação ou degradação do tráfego que não decorra de requisitos técnicos destinados a preservar a qualidade contratual do serviço.

(17 Comentários)

Seção III

Dos registros de dados

(2 Comentários)

Subseção I

Da guarda de registros de conexão

(1 Comentário)

Art. 13

(6 Comentários)

A guarda e a disponibilização dos registros de conexão a que esta lei faz referência devem atender à preservação da intimidade, vida privada, honra e imagem das partes direta ou indiretamente envolvidas.

(6 Comentários)

Art. 14

(1 Comentário)

A provisão de conexão à Internet impõe ao administrador do sistema autônomo respectivo o dever de manter os registros de conexão sob sigilo, em ambiente controlado e de segurança, pelo prazo máximo de 6 (seis) meses, nos termos do regulamento.

(86 Comentários)

Parágrafo único. O dever de manter os registros de conexão não poderá ser transferido.

(8 Comentários)

Art. 15

(1 Comentário)

Na guarda de registros de conexão:

(3 Comentários)

I – os registros de conexão somente poderão ser fornecidos a terceiros mediante ordem judicial ou por autorização prévia e expressa do respectivo usuário;

(11 Comentários)

II – os dados cadastrais somente poderão ser disponibilizados de maneira vinculada aos registros de conexão mediante ordem judicial; e

(17 Comentários)

III – as medidas e procedimentos de segurança e sigilo dos registros de conexão e dos dados cadastrais devem ser informados de forma clara aos usuários.

(5 Comentários)

Parágrafo único. Os procedimentos de segurança necessários à preservação do sigilo e da integridade dos registros de conexão e dos dados cadastrais referidos neste artigo deverão atender a padrões adequados, a serem definidos por meio de regulamento.

(5 Comentários)

Subseção II

Da guarda de registros de acesso a serviços de Internet

(3 Comentários)

Art. 16

(4 Comentários)

A guarda de registros de acesso a serviços de Internet dependerá de autorização expressa do usuário e deverá obedecer ao que segue, sem prejuízo às demais normas e diretrizes relativas à proteção de dados pessoais:

(20 Comentários)

I – informação prévia ao usuário sobre a natureza, finalidade, período de conservação, políticas de segurança e destinação das informações guardadas, facultando-lhe o acesso, retificação e atualização sempre que solicitado;

(3 Comentários)

II – consentimento livre e informado do usuário previamente ao tratamento, à distribuição a terceiros ou à publicação das informações coletadas; e

(2 Comentários)

III – os dados que permitam a identificação do usuário somente poderão ser disponibilizados de maneira vinculada aos registros de acesso a serviços de Internet mediante ordem judicial.

(13 Comentários)

Art. 17

(6 Comentários)

Os danos causados aos titulares de dados pessoais devem ser reparados nos termos da lei.

(6 Comentários)

Subseção III

Da proteção ao sigilo das comunicações pela Internet

(Sem comentários)

Art. 18

(16 Comentários)

Os procedimentos de interceptação, escuta ou disponibilização de conteúdo das comunicações pela Internet somente poderão ocorrer para fins de persecução penal e serão regulados pela lei que trata da interceptação de comunicação telefônica e dados telemáticos.

(16 Comentários)

Seção IV

Da remoção de conteúdo

(16 Comentários)

Art. 19

(12 Comentários)

O provedor de conexão à Internet não será responsabilizado por danos decorrentes de conteúdo gerado por terceiros.

(12 Comentários)

Art. 20

(16 Comentários)

~~O provedor de serviço de Internet somente poderá ser responsabilizado por danos decorrentes de conteúdo gerado por terceiros se for notificado pelo ofendido e não tomar as providências para, no âmbito do seu serviço e dentro do prazo razoável, tornar indisponível o conteúdo apontado como infringente.~~

(62 Comentários)

~~§ 1º Os provedores de serviços de Internet devem oferecer de forma ostensiva ao menos um canal eletrônico dedicado ao recebimento de notificações e contranotificações.~~

(8 Comentários)

~~§ 2º É facultado ao provedor de serviços de Internet criar mecanismo automatizado para atender aos procedimentos dispostos nesta Seção.~~

(6 Comentários)

PROPOSTA DE NOVA REDAÇÃO
O provedor de serviço de internet somente poderá ser responsabilizado por danos decorrentes de conteúdo gerado por terceiros se, após intimado para cumprir ordem judicial a respeito, não tomar as providências para, no âmbito do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente.

(67 Comentários)

Art. 21

(3 Comentários)

~~A notificação de que trata o art. 20 deverá conter, sob pena de invalidade:~~

(Sem comentários)

~~I – identificação do notificante, incluindo seu nome completo, seus números de registro civil e fiscal e dados atuais para contato;~~

(Sem comentários)

~~II – data e hora de envio;~~

(Sem comentários)

~~III – identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material pelo notificado;~~

(Sem comentários)

~~IV – descrição da relação entre o notificante e o conteúdo apontado como infringente; e~~

(Sem comentários)

~~V – justificativa jurídica para a remoção.~~

(2 Comentários)

PROPOSTA DE NOVA REDAÇÃO
A intimação de que trata o art. 20 deverá conter, sob pena de invalidade:

(3 Comentários)

I – identificação da parte que solicitou a remoção do conteúdo, incluindo seu nome completo, seus números de registro civil e fiscal e dados atuais para contato;

(Sem comentários)

II – identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material;

(Sem comentários)

III – descrição da relação existente entre a parte solicitante e o conteúdo apontado como infringente;

(Sem comentários)

IV – justificativa jurídica para a remoção.

(3 Comentários)

Art. 22

(1 Comentário)

~~Ao tornar indisponível o acesso ao conteúdo, caberá ao provedor do serviço informar o fato ao usuário responsável pela publicação, comunicando-lhe o teor da notificação de remoção e fixando prazo razoável para a eliminação definitiva do conteúdo.~~

(7 Comentários)

~~Parágrafo único. Caso o usuário responsável pelo conteúdo infringente não seja identificável ou não possa ser localizado, e desde que presentes os requisitos de validade da notificação, cabe ao provedor de serviço manter o bloqueio.~~

(2 Comentários)

PROPOSTA DE NOVA REDAÇÃO
Ao tornar indisponível o acesso ao conteúdo, caberá ao provedor do serviço informar o fato ao usuário responsável pela publicação, comunicando-lhe o teor da intimação, nos casos em que o usuário responsável seja identificável.

(7 Comentários)

Art. 23

(2 Comentários)

~~É facultado ao usuário responsável pela publicação, observados os requisitos do art. 21, contranotificar o provedor de serviço, requerendo a manutenção do conteúdo e assumindo a responsabilidade exclusiva pelos eventuais danos causados a terceiros, caso em que caberá ao provedor de serviço o dever de restabelecer o acesso ao conteúdo indisponibilizado e informar ao notificante o restabelecimento.~~

(4 Comentários)

~~Parágrafo único. Qualquer outra pessoa interessada, física ou jurídica, observados os requisitos do art. 21, poderá contranotificar o prestador de serviço, assumindo a responsabilidade pela manutenção do conteúdo.~~

(1 Comentário)

PROPOSTA DE NOVA REDAÇÃO
Os usuários que detenham poderes de moderação sobre o conteúdo de terceiros se equiparam aos provedores de serviços de Internet para efeitos do disposto nesta Seção.

(11 Comentários)

Art. 24

(3 Comentários)

~~Tanto o notificante quanto o contranotificante respondem, nos termos da lei, por informações falsas, errôneas e pelo abuso ou má fé.~~

(3 Comentários)

PROPOSTA DE SUPRESSÃO

(Sem comentários)

Art. 25

(22 Comentários)

Os usuários que detenham poderes de moderação sobre o conteúdo de terceiros se equiparam aos provedores de serviços de Internet para efeitos do disposto nesta Seção.

(22 Comentários)

Seção V

Da requisição judicial de registros

(Sem comentários)

Art. 26

(1 Comentário)

A parte interessada poderá, para o exclusivo propósito de formar conjunto probatório em processo judicial, requerer ao juiz a expedição de requisição solicitando, ao responsável pela guarda, o fornecimento de registros de conexão ou de acesso a serviço de Internet.

(5 Comentários)

Parágrafo único. No requerimento de requisição judicial a parte deverá fazer constar:

(Sem comentários)

I – a descrição pormenorizada de indícios razoáveis da ocorrência do ilícito;

(Sem comentários)

II – a justificativa motivada da utilidade dos registros solicitados para fins de investigação do ilícito; e

(1 Comentário)

III – período ao qual se referem os registros.

(1 Comentário)

Art. 27

(Sem comentários)

A requisição judicial de fornecimento de registros obedecerá aos ritos processuais cabíveis, observado o que segue:

(4 Comentários)

§ 1º. A requisição de fornecimento de registros de acesso a serviços de Internet fica sujeita à comprovação de que o responsável mantém a guarda com a autorização expressa dos usuários, obedecido o disposto no art. 16.

(2 Comentários)

§ 2º. Caso o fornecimento dos registros de acesso a serviços de Internet não seja necessário para os fins da investigação, cabe ao juiz limitar a requisição apenas ao fornecimento dos registros de conexão.

(2 Comentários)

§ 3º. Cabe ao juiz tomar as providências necessárias à garantia do sigilo do conteúdo das comunicações e à preservação da intimidade, vida privada, honra e imagem do usuário, podendo, inclusive, determinar o segredo de justiça em relação às informações recebidas.

(Sem comentários)

CAPÍTULO IV

DA ATUAÇÃO DO PODER PÚBLICO

(3 Comentários)

Art. 28

(5 Comentários)

Constituem diretrizes para a atuação da União, dos Estados, do Distrito Federal e dos Municípios no desenvolvimento da Internet no Brasil:

(9 Comentários)

I – estabelecimento de mecanismos de governança transparentes, colaborativos e democráticos, com a participação dos vários setores da sociedade;

(7 Comentários)

II – promoção da racionalização e da interoperabilidade tecnológica dos serviços de governo eletrônico, nos diferentes níveis da federação, para permitir o intercâmbio de informações e a agilização de procedimentos;

(Sem comentários)

III – promoção da interoperabilidade entre sistemas e terminais diversos, inclusive entre os diferentes níveis federativos e diversos setores da sociedade;

(Sem comentários)

IV – adoção preferencial de tecnologias, padrões e formatos abertos;

(8 Comentários)

V – publicização e disseminação de dados e informações públicos, de forma aberta e estruturada;

(4 Comentários)

VI – otimização da infraestrutura das redes, promovendo a qualidade técnica, a inovação e a disseminação dos serviços de Internet, sem prejuízo à abertura, neutralidade e natureza participativa;

(2 Comentários)

VII – desenvolvimento de ações e programas de capacitação para uso da internet;

(1 Comentário)

VIII – promoção da cultura e da cidadania, inclusive pela prestação mais dinâmica e eficiente de serviços públicos;

(1 Comentário)

IX – uso eficiente de recursos públicos e dos serviços finalísticos disponibilizados ao cidadão; e

(Sem comentários)

X – prestação de serviços públicos de atendimento ao cidadão de forma integrada, simplificada e por múltiplos canais de acesso.

(Sem comentários)

Art. 29

(1 Comentário)

Os sítios e portais de entes do Poder Público devem buscar:

(5 Comentários)

I – compatibilidade dos serviços de governo eletrônico com diversos terminais, sistemas operacionais e aplicativos para seu acesso;

(1 Comentário)

II – acessibilidade a todos os interessados, independentemente de suas capacidades físico-motoras, perceptivas, culturais e sociais, resguardados os aspectos de sigilo e restrições administrativas e legais;

(Sem comentários)

III – compatibilidade tanto à leitura humana como ao tratamento por máquinas;

(4 Comentários)

IV – facilidade de uso dos serviços de governo eletrônico; e

(1 Comentário)

V – fortalecimento da democracia participativa.

(10 Comentários)

Art. 30

(Sem comentários)

O cumprimento do dever constitucional do Estado na prestação da educação, em todos os níveis de ensino, abarca a capacitação para o uso da Internet como ferramenta de exercício de cidadania, promoção de cultura e desenvolvimento tecnológico.

(Sem comentários)

§ 1º. Sem prejuízo das atribuições do poder público, o Estado fomentará iniciativas privadas que promovam a Internet como ferramenta educacional.

(Sem comentários)

§ 2º. A capacitação para o uso da Internet deve ocorrer integrada a outras práticas educacionais.

(4 Comentários)

Art. 31

(2 Comentários)

As iniciativas públicas de fomento à cultura digital e de promoção da Internet como ferramenta social devem:

(2 Comentários)

I – buscar minimizar as desigualdades, sobretudo as regionais, no acesso à informação; e

(2 Comentários)

II – promover a inclusão digital de toda a população, especialmente a de baixa renda.

(26 Comentários)

Art. 32

(3 Comentários)

O Estado deve buscar, formular e fomentar estudos periódicos regulares e periodicamente fixar metas, estratégias, planos e cronogramas referentes ao uso e desenvolvimento da Internet no país.

(3 Comentários)

CAPÍTULO V
DISPOSIÇÕES FINAIS

(Sem comentários)

Art. 33

(8 Comentários)

A defesa dos interesses e direitos dos usuários da Internet poderá ser exercida em juízo individualmente ou a título coletivo, na forma do disposto nos artigos 81 e 82 da Lei 8.078, de 11 de setembro de 1990.

(8 Comentários)

Art. 34

(9 Comentários)

Esta Lei entra em vigor na data de sua publicação.

(9 Comentários)

Livros Grátis

(http://www.livrosgratis.com.br)

Milhares de Livros para Download:

Baixar livros de Literatura
Baixar livros de Literatura de Cordel
Baixar livros de Literatura Infantil
Baixar livros de Matemática
Baixar livros de Medicina
Baixar livros de Medicina Veterinária
Baixar livros de Meio Ambiente
Baixar livros de Meteorologia
Baixar Monografias e TCC
Baixar livros Multidisciplinar
Baixar livros de Música
Baixar livros de Psicologia
Baixar livros de Química
Baixar livros de Saúde Coletiva
Baixar livros de Serviço Social
Baixar livros de Sociologia
Baixar livros de Teologia
Baixar livros de Trabalho
Baixar livros de Turismo