A ARTE DA COMPUTAÇÃO EM POLÍTICAS PÚBLICAS: LEGISLAÇÃO, PREVENÇÃO E COMBATE AOS CIBERCRIMES

Aymée Beatriz Vicente

Orientador: Professor Doutor Martin Jayo

Monografia final de conclusão de curso de graduação apresentada à Escola de Artes, Ciências e Humanidades para obtenção do título de Bacharel em Gestão de Políticas Públicas.

USP – São Paulo

2014.

Universidade de São Paulo - Escola de Artes, Ciências e Humanidades - Biblioteca.
Ficha automatizada com os dados inseridos pelo(a) autor(a).

Vicente, Aymee Beatriz
A ARTE DA COMPUTAÇÃO EM POLÍTICAS PÚBLICAS: LEGISLAÇÃO, PREVENÇÃO E COMBATE AOS CIBERCRIMES / Aymee Beatriz Vicente ; orientador, Martin Jayo. 2014.
75 f: il.

Monografia (Bacharelado em Gestao de Politicas Públicas) - Escola de Artes, Ciências e Humanidades, Universidade de São Paulo, São Paulo, 2014.

1. TICs. 2. cibercrimes. 3. legislação. 4. prevenção. 5. segurança. I. Jayo, Martin, orient. II. Título.

SUMÁRIO

AGRADECIMENTOS

“Mais importante que a vontade de vencer é a coragem de começar. É justamente a possibilidade de realizar um sonho que torna a vida interessante”.

Agradeço ao meu Deus, fiel e justo para comigo nestes 21 anos. Tu és meu guia, me sondas e me conheces. Grata sou pelo Seu infinito amor e misericórdia pela minha vida!

À minha família, meu muito obrigada. Sem vocês, sem seu apoio, essa jornada não seria possível. Juntos, vencemos mais uma etapa! Sinto orgulho e enorme alegria em poder dividir este momento com vocês. Mãe, irmãos, avós Augusta e Prisco e Vicente e Guiomar, meu muito obrigada por partilharem este momento comigo.

Mãe, obrigada por nunca desistirem de nós, por sempre me incentivar a crescer e a ir em frente. Amo vocês, mais do que tudo. Mãe e vó Augusta, muito obrigada por ser a minha segunda mãe; por todo carinho, por todos os bons momentos, por todas as broncas e conselhos. Hoje eu não estaria aqui se não fosse por vocês! Obrigada!!!

Para ser irmão, não é preciso ser de sangue, não é mesmo? Aos meus irmãos de coração e de longa jornada, obrigada por tornarem estes quatro anos de graduação tão alegres e tão mais significativos!

Aos meus professores, agradeço pelo aprendizado e pela oportunidade de crescer, tanto intelectualmente quanto como pessoalmente. Vocês serão sempre importantes em minha vida. Todo o aprendizado e toda a formação, desde a pré-escola ao término desta graduação, não seriam possíveis sem vocês. Sou grata a todos, de uma maneira muito especial.

Agradeço, também, ao meu querido orientador, Martin Jayo, por ter paciência para ler todas as versões deste trabalho, por me orientar e por me ensinar. Tenho um carinho enorme pelo senhor e, sem dúvida, sem a sua orientação não seria possível concluir esta etapa. Sou muito grata por isso!

Agradeço, também, a todos que torceram por mim. Espero que vocês saibam que a minha vitória é de vocês, também, e que tenho enorme alegria em poder tê-los presentes em minha vida!

DEDICATÓRIA

“As dificuldades que você encontra se resolverão conforme você avançar. Prossiga, e a luz aparecerá, e brilhará com clareza crescente em seu caminho”.

Dedico este trabalho aos meus avós, pais e irmãos, que sempre estiveram ao meu lado. Apesar das dificuldades, vencemos cada uma delas juntos, e este trabalho é a prova de que mais uma etapa foi vencida. Obrigada pelo apoio, compreensão, fé e amor por mim. Amo imensamente a vida de vocês. Obrigada, também, por me ensinarem a ter foco no objetivo, força pra lutar e fé para crer e vencer barreiras. Tudo é possível se houver um sonho a se realizar!

Aos meus amigos e irmãos de fé, aos quais eu não preciso citar – vocês sabem – obrigada pelo companheirismo. Sem vocês, eu nada seria; essa vitória é nossa e eu os amo! Obrigada por serem tão especiais em minha vida. Para termos irmãos, não necessariamente precisam ser de sangue, certo? Irmãos do coração! Vou levá-los por toda a minha vida!

Esta é uma conquista, e toda conquista é feita de sonhos. Sonhos que vocês sonharam comigo. Um dia sonharam que eu venceria, e eu venci. Cheguei aqui e agradeço o amor que tiveram para comigo. Nem sempre a vida é fácil, mas quem tem família e amigos-irmãos tem força para lutar e vencer qualquer desafio! Sempre juntos!

Por último, mas acima de tudo, agradeço ao Senhor, meu Deus! Este trabalho é fruto daquilo que derramaste sobre mim: determinação, esforço e vontade para vencer. Tu és maravilhoso para em minha vida e eu te amo mais do que tudo! Obrigada por me dar a oportunidade de crescer, de romper barreiras, de sonhar e de concretizar sonhos. Eu nada seria sem o Teu amor! Obrigada por não deixar, em momento algum, que eu perdesse a minha fé. Obrigada por me amparar, por me cercar de amor e por me fazer filha!

RESUMO

Com a criação da Internet pelos EUA, entre as décadas de 1960 e 1980, para fins militares, surgia a maior rede de comunicação já estabelecida. O cenário mundial trazia a tensão gerada pela Guerra Fria, em que a URSS e os EUA se preparavam para um possível conflito de proporções gigantescas - que, por sorte, não aconteceu. O objetivo da criação desta rede, denominada *Arpanet*, seria o de estabelecer uma comunicação contínua caso os Estados Unidos viessem a sofrer um ataque que destruísse os meios de comunicação convencionais daquela época. Embora não tenha ocorrido o conflito, a Arpanet (atualmente conhecida como Internet) tornou-se uma grande ferramenta para uso acadêmico ao longo dos anos. A internet se popularizou muito desde a sua criação, em meados da década de 1960. Inicialmente criada para propósitos militares pela *Advanced Research Project Agency (Arpanet)*, o objetivo desta instituição era implantar uma rede de comunicações que pudesse fluir normalmente para diversas localidades caso houvesse ataques que culminassem com a destruição de parte dessa. Funcionando através de um sistema denominado “chaveamento de pacotes” (sistema de transmissão de dados em rede, pelas quais as informações são divididas de maneira que pudessem ser remontadas pelo destinatário), deu-se início ao maior fenômeno midiático e computacional do século XX: a internet, atingindo em aproximadamente 4 anos, 50 milhões de usuários (SOUZA E STEVANS, s/d). O surgimento massivo de provedores de serviços online e a facilidade em comunicação e informação em tempo real contribuíram para este avanço desenfreado de usuários e serviços. Ao passo em que a quantidade de serviços e de usuários crescia novas formas de se cometerem delitos também surgiam.À medida em que a informatização e a incorporação da internet chegaram também à administração pública (CUNHA, 1994; DINIZ, 2005), governo e organizações públicas também se tornaram vulneráveis a diferentes tipos de delitos virtuais. Nesse sentido, este trabalho tem como objetivo contextualizar a administração pública brasileira no cenário da informatização, estudar as legislações a respeito deste tema e fazer uma análise das medidas tomadas, tanto em âmbito federal, estadual e municipal, bem como o papel da sociedade civil para se prevenir e combater os cibercrimes.

Palavras-chave: TICs, administração pública, cibercrimes, legislação, prevenção, combate, segurança.

ABSTRACT

With the creation of the Internet by the U.S. between the 1960s and 1980s, for military purposes, emerged the largest network of communication already established. The world scenario brought the tension generated by the Cold War, when the USSR and the U.S. were preparing for a possible conflict of gigantic proportions - which, luckily, did not happen. The purpose of creating this network, called ARPANET, would be to establish a continuous communication if the U.S. were to suffer an attack that destroyed the conventional media of that time. Although there was no conflict, Arpanet (now known as the Internet) has become a great tool for academic use over the years. The internet is very popular since its inception in the mid-1960s. Originally designed for military purposes by the Advanced Research Project Agency (ARPANET), the aim of this institution was to deploy a communications network that would normally flow to different locations if they had attacks that culminate with the destruction of part thereof. Working through a system called "packet switching" (system data transmission network, for which the information is divided so that they could be reassembled by the recipient), has begun the biggest media phenomenon and computational twentieth century: the internet, reaching approximately 4 years, 50 million users (SOUZA E Stevans, s / d). The emergence of massive online service providers and facility in communication and real-time information contributed to this advance rampant users and services. While in the quantity of users and services growing new ways to commit crimes also arose. With the arrival of computers and internet to Public Administration (CUNHA, 1994; DINIZ, 2005), government and public organizations have also become vulnerable to different types of virtual crimes. In this sense, this research aims to contextualize the Brazilian public administration in the setting of computerization, study the laws regarding this issue and make an analysis of the measures taken, both at the federal, state and municipal levels as measures taken by civil society to prevent and combat cybercrime.

Keywords: ICT, public administration, cybercrime, law, prevention, response, security.

CAPÍTULO 1 – INTRODUÇÃO

1.1 Contexto da pesquisa

A administração pública brasileira, ao longo dos anos, vem incorporando de forma crescente Tecnologias de Informação e Comunicação (TICs) às suas práticas de gestão. Presentes em nosso cotidiano, as TICs facilitam o nosso dia a dia enquanto cidadãos e usuários de serviços públicos, economizam tempo e oferecem, de maneira prática e rápida na maioria das vezes, a resolução de problemas que sem o seu uso nos trariam uma infinidade de dificuldades operacionais.

Por outro lado, o avanço das Tecnologias de Informação dá margem para que crimes de natureza virtual sejam cometidos de diversas maneiras, pois as políticas de segurança eletrônica do governo e das empresas envolvidas nem sempre acompanham com velocidade suficiente o crescimento de tais práticas.

Neste trabalho, abordarei a questão da introdução das Tecnologias de Informação e Comunicação na administração pública brasileira e como ocorrem os crimes virtuais no Brasil. Dentre os vários tipos de crimes virtuais existentes (desde vazamentos de informações pessoais até fraudes e invasão de dados dos entes da União), estudarei os ataques virtuais (invasão de bancos de dados, vazamento de informações secretas, fraudes em bancos de dados, entre outros), explicando como a legislação existente em nosso país se aplica – ou não – aos ataques virtuais cometidos, quais tipos de delitos podem existir, como os governos Federal, estaduais e municipais agem na tentativa de inibirem este tipo de ação e qual o papel da sociedade civil para que ações de segurança *on line* sejam desenvolvidas.

1.2 Tema e Justificativa do trabalho

O tema deste trabalho é a implementação de TICs na Administração Pública brasileira, bem como a legislação no que tange aos crimes cibernéticos – aqui serão adotados os ataques virtuais às informações e bancos de dados – e as ações dos governos em nível federal, municipal e estadual para o combate aos mesmos, bem como as ações desenvolvidas pela sociedade civil.

Para justificar este trabalho, aponto que, embora a quantidade de artigos e trabalhos, acadêmicos e não acadêmicos, sobre o assunto seja considerável, não foi realizado antes, até onde foi possível avaliar, um estudo que englobasse os diversos aspectos deste problema em um só trabalho.

Além do mais, sabe-se que o setor público – e o setor público brasileiro não foge à regra– tem uma maior dificuldade ou morosidade em acompanhar a evolução das TICs e desenvolver maneiras de garantir a segurança em bancos de dados. Seja por limitações burocráticas, orçamentárias etc., os órgãos públicos tendem a ter mais dificuldades para tomar medidas eficazes na prevenção e no combate aos crimes virtuais.

Portanto, pergunto: quais políticas públicas existem ou podem ser desenvolvidas para fomentar a área das TICs no governo, bem como combater o cibercrime?

1.3 Objetivo

Este trabalho tem como objetivo contextualizar a administração pública brasileira no cenário da informatização, estudar as legislações a respeito deste tema e fazer uma análise das medidas tomadas, tanto em âmbito federal, estadual e municipal, bem como o papel da sociedade civil para se prevenir e combater os cibercrimes.

Assim, proponho responder algumas questões que nortearão o meu trabalho: Em qual patamar o Brasil se encontra no que tange às políticas públicas de combate e prevenção aos crimes virtuais do tipo “ataques cibernéticos”? Como os entes da União e a sociedade civil se mobilizam para a prevenção e combate destes problemas? E, por último, quais são as políticas públicas desenvolvidas para esta área?

A fim de entender como Estado e sociedade civil se organizam em torno ao tema, o foco da pesquisa recairá em duas entidades selecionadas: o Comitê Gestor de Internet no Brasil e da Safernet, sendo a que o primeiro é a principal organização voltada para a regulamentação da Internet no Brasil, enquanto a segunda volta seus esforços à prevenção, combate e investigação de crimes ocorridos no meio virtual. Justifica-se a escolha destas duas organizações dada a sua relevância no cenário da Internet no Brasil

1.4 Metodologia

Para atingir o objetivo deste trabalho, a pesquisa se baseará em uma revisão de literatura sobre o assunto. Será realizada uma revisão bibliográfica de trabalhos, artigos e publicações referentes ao tema, bem como uma análise da legislação brasileira em comparação à legislação de países europeus e dos Estados Unidos, bem como as medidas tomadas por países latino-americanos para legislação, prevenção, e combate aos cibercrimes.

1.5 Estrutura do trabalho

Para a consecução do objetivo apresentado em 1.2, o trabalho se compõe de 6 capítulos, incluindo este capítulo introdutório:

- Capítulo 2: composto por uma revisão bibliográfica que irá contextualizar, de uma maneira geral, a incorporação das Tecnologias de Informação e Comunicação na Administração Pública brasileira. Neste mesmo capítulo, serão apontados os desafios para se combater os cibercrimes e os descompassos existentes nessa área. Será apresentada uma revisão de literatura que contextualizará, de maneira geral, a incorporação de Tecnologias de Informação na administração pública. Apontaremos essa incorporação de um lado e as atividades criminosas, de outro, apontando desafios e possíveis descompassos existentes nesta área.
- Capítulo 3 – Abordará o conceito de Cibercrimes e suas tipificações.
- Capítulo 4: baseado em revisão bibliográfica, descreverá as legislações adotadas por diversos países para combater os crimes cibernéticos. Assim, busca-se um *benchmark* para o caso brasileiro. O mesmo capítulo faz uma análise do estado da arte do Brasil, no que se refere à legislação de combate ao cibercrime.
- Capítulo 5 – Baseado em revisão de literatura e em coleta própria de dados, abordará o papel das delegacias especializadas do Comitê Gestor da Internet na área de regulamentação e gestão da Internet no Brasil, bem como o papel da SaferNet (Associação Civil de direito privado que atua nacionalmente) como um agente social no combate a crimes virtuais.
- Capítulo 6 – Considerações finais.

CAPÍTULO 2 - ADMINISTRAÇÃO PÚBLICA E TICS

Neste capítulo, trarei um panorama do uso das Tecnologias de Informação e Comunicação para informatizar e aperfeiçoar a Administração Pública Brasileira, utilizando, principalmente, a obra de Diniz (2005)[1], além de outas referências relevantes sobre o assunto.

O início da informatização na administração pública, segundo Diniz, remonta à década de 1970 e fundamentou-se quase que exclusivamente na gestão de receitas e despesas, até as experiências mais recentes, com ênfase na entrega de serviços aos cidadãos. Ao longo destes anos, o que veio a se conhecer por "informática pública" vivenciou diversos usos de TICs e modelos de gestão de informação, diferenciando-se somente da trajetória de implementação da informática no setor privado pelo tempo de adoção da tecnologia – tanto para decidir sobre o seu uso como quanto para implementá-la (DINIZ, 2005).

Apesar dessa relativa defasagem em relação às organizações privadas, a administração pública brasileira passou por um intenso processo de modernização tecnológica nas últimas décadas. Desde a informatização de órgãos à criação do governo eletrônico, muitos avanços já foram realizados.

A incorporação da informática nas empresas e organizações brasileiras dividiu-se em algumas fases específicas, conforme se pode classificá-las (MUSEU DO COMPUTADOR, S/D). A primeira fase compreende o período de 1958 a 1975, caracterizada, principalmente, pela importação das tecnologias de informação de países de capitalismo avançado – com destaque para os Estados Unidos. No que tangia ao processamento eletrônico de dados, o mesmo era realizado em computadores de grande porte que se localizavam em grandes empresas, universidades, órgãos governamentais e agências de serviços.

Na década de 1970, o volume de vendas de máquinas representava um mercado para o estabelecimento de fabricantes nacionais – que até então não existiam – pressionando e justificando a instalação de multinacionais no Brasil. Aos poucos começou a se desenvolver no Brasil uma competência tecnológica que só foi possível

[1] Vagner Diniz é presidente do Instituto CONIP Conhecimento, Inovação e Práticas de TI na Gestão Pública, uma organização não governamental dedicada à disseminação do conhecimento sobre o uso das novas tecnologias da informação e comunicação na gestão pública para o fortalecimento da democracia, desenvolvimento da cidadania e mais eficiência da gestão pública. É formado em Engenharia Eletrônica pelo Centro Federal de Tecnologia do Rio de Janeiro, com especializações em Administração de Empresas pela Fundação Getúlio Vargas e em Educação e Cultura, pela Universidade de Genebra. A carreira profissional tem foco na promoção do uso intensivo das TICs nos governos.

graças a alguns trabalhos de universidades como a USP, a PUC/RJ e a Universidade Estadual de Campinas.

Em 1972 o primeiro computador nacional foi construído na Universidade de São Paulo e apelidado de “Patinho Feio”. Dois anos depois, a Marinha de Guerra necessitava de equipamentos para seu programa de nacionalização eletrônica de bordo e recorreu ao projeto G-10, da USP e da PUC/RJ.

Ainda em 1972, com o interesse gerado pelo assunto e a busca por conquistar uma independência tecnológica, foi criado, em 1972, a Comissão de Coordenação das Atividades de Processamento Eletrônico (CAPRE), cujo objetivo principal pautava-se em propor uma política governamental de desenvolvimento do setor. Em 1974, por sua vez, foi criada a primeira empresa nacional fabricante de computadores, a Computadores Brasileiros S.A. (COBRA).

A segunda etapa do desenvolvimento da informática no Brasil pautou-se pelo crescimento da indústria nacional: os primeiros microcomputadores foram fabricados por cinco empresas autorizadas pelo governo federal.

Com o aumento da intervenção estatal na área, em 1979 foi criada a Secretaria Especial de Informática (antiga SEI, hoje conhecida como a Secretaria Especial de Ciência e Tecnologia), ligada ao Conselho de Segurança Nacional (órgão que, até hoje, é responsável pelos assuntos referentes à área) e, em 1984, foi sancionada a lei nº 7232, que fixava a Política Nacional de Informática, que oficializava a reserva de alguns segmentos específicos do mercado em meados da década de 1980, o Brasil registrou níveis de crescimento de até 30% ao ano no setor).

No que diz respeito especificamente à implementação de informática na administração pública brasileira, Diniz (2005) distingue três fases distintas: a) de 1970 a 1992; b) 1993 a 1998; e por último, c) 1999 em diante.

2.1 De 1970 a 1992: A Declaração do Imposto de Renda (DIR)

Na década de 1960, o Ministério da Fazenda já fazia uso dos primeiros equipamentos de processamento de dados para a execução de suas atividades – trabalho realizado pelos Técnicos de Mecanização ou Técnicos Auxiliares de Mecanização – sendo a principal falha a falta de coordenação técnica unificada e a pouca quantidade de profissionais especialistas. Em 1º de dezembro de 1964 foi criado, através da Lei nº 4.516, o Serviço Federal de Processamento de Dados (Serpro - vinculada ao Ministério da Fazenda), cujo objetivo era executar, através de processos eletrônicos, todos os serviços de processamento de dados e tratamento de informações

dos órgãos do Ministério. Posteriormente, através do Decreto nº 55.827 de 11 de março de 1965, foram estipuladas a sua organização e funcionamento.

Neste período, o foco do uso das TICs se deu na gestão interna, através do uso de aplicações que fossem voltadas para a melhoria da gestão pública interna e que também fosse voltada para a eficiência dos processos administrativos.

Diniz (2005) afirma, no entanto, que a iniciativa mais simbólica e de maior expressão só se daria com a implementação da Declaração do Imposto de Renda através de meios eletrônicos.

Surgido nos anos 90, a DIR por meio eletrônico alcançou o patamar de uma das aplicações mais utilizadas globalmente, graças às suas características de eficiência, volume e confiabilidade. O autor aponta que hoje, quase 100% das declarações são feitas via internet, pois esta é uma ferramenta que gera um alto grau de confiabilidade e reconhecida pelo contribuinte.

Diniz (2005) traz ao debate que o uso das TICs pela administração pública na década de 70 (em seu começo), "estava restrito às áreas financeiras, mormente a automação do controle de arrecadação (gestão tributária) e das despesas, em especial a folha de pagamento".

As Secretarias da Fazenda estaduais, e algumas municipais, tiveram destaque especial na definição de um modelo de gestão da informação, baseado em empresas públicas prestadoras de serviços e, em grande parte, detentoras do monopólio dos serviços de TI no setor público. Cabe salientar que, como aponta Diniz (2005), estes sistemas acabaram por gerar mais velocidade no processamento de informações, além de maior segurança tanto no armazenamento como na capacidade de gerir a esfera pública.

2.2 De 1993 a 1998: Foco nos Serviços de Atendimento ao Cidadão – aplicações e processos voltados para apoiar a prestação de serviços ao cidadão, pessoalmente ou via telefone.

Nesta fase, o que se destaca são os Serviços de Atendimento ao Cidadão (os SACs), cujas iniciativas iniciais aconteceram no estado da Bahia e no município de Curitiba, Paraná. O SAC da Bahia merece maior destaque, pois reuniu em um espaço físico único a maior quantidade de serviços públicos possíveis – até então, cada órgão público realizava o atendimento aos cidadãos em diversos endereços, de acordo com as especialidades. A fragmentação do serviço público acabava por gerar um deslocamento gigantesco dos usuários em busca de atendimento e uma grande falta de integração das informações, quando geradas por órgãos diferentes.

Assim, a ideia dos Serviços de Atendimento ao Cidadão trouxe um novo conceito no atendimento ao cidadão, ao passo em que:

a) passou a reunir os serviços em um lugar, somente;
b) integrou serviços e processos;
c) pessoal especializado no atendimento ao público; e
d) espaço físico adequado para realizar o atendimento.

Assim, aliados ao uso da tecnologia, os serviços públicos foram levados para mais perto do cidadão, cujos pontos principais apontados pelos usuários foram o atendimento personalizado, qualificado, rápido e eficiente.

Em São Paulo, a expressão que melhor se encaixa neste conceito é o Poupatempo, implementado na década seguinte. Os vários postos de atendimento ao cidadão, espalhados pelo estado, fazem uso maciço da TI. O Poupatempo atende milhões de pessoas por ano, com eficiência de 98% no índice de satisfação do cidadão.

Conforme aponta Diniz (2005), “muito mais que equipamentos menores e mais baratos, alterou-se quantitativa e qualitativamente o centro da produção de conhecimento mediado pelo computador. Muito mais pessoas passaram a usar o computador como ferramenta de produção de conhecimento, como também estes novos agentes introduziram novas demandas por aplicações.

No campo do comportamento, o novo Código Brasileiro do Consumidor garantiu direitos aos cidadãos antes nunca vistos, chamando a atenção para o personagem central da cadeia de valores nos negócios. O Código consolidou um conjunto de aspirações dos cidadãos no que se convencionou chamar de Direitos do Consumidor.

Assim como a microcomputação permite a individualização e a personalização do uso das ferramentas de tecnologia da informação, os direitos do consumidor também personalizam a expressão da opinião e vontades pessoais no campo do consumo de bens e serviços”.

Conforme apontado por Vaz (2008), a importância em focar o atendimento no cidadão “situa-se como um princípio central de reorganização do Estado, entre os princípios do modelo gerencial. Não somente a prestação de serviços em si é reestruturada, mas se pretende que todo o funcionamento do aparelho estatal se e mude redirecione suas prioridades a partir das demandas entendidas como aquelas prioritárias dos cidadãos. É um Estado *para* o cidadão”.

2.3 De 1999 a 2004: foco na entrega de serviços via internet – aprendizado e domínio das TICs

Nesta fase, Diniz (2005) aponta “a era dos portais de serviços públicos via internet”, que acabou por consolidar um conjunto de inciativas, sobretudo de governos estaduais, para se firmar como canal de prestação de serviços *online*. Dentre os serviços, destacam-se:

- Registro via Internet de ocorrências policiais, de natureza não complexa (furtos simples, desaparecimentos, denúncias) sem a intermediação policial.
- Veículos –Por meio das aplicações existentes é possível verificar a situação de regularidade do veículo perante a autoridade competente (registro e multas), fazer pagamentos de licenças e multas, em ação conjunta com a rede bancária e a verificação da situação de regularidade do motorista (registro e pontuação).
- Pregão eletrônico – aplicação que permite ao Governo do Estado de São Paulo a realização de compras eletrônicas completamente via Internet. O processo é simples e eficiente: as unidades compradoras tornam pública a sua intenção de compra. No prazo determinado, os fornecedores cadastrados podem registrar a sua intenção de participação no leilão. Em dia publicamente divulgado e ajustado, os fornecedores participantes do pregão eletrônico entregam as suas propostas. E de acordo com regras de um leilão reverso, os fornecedores podem oferecer lances cujos preços sejam menores que o menor oferecido.

Com o tempo tais aplicações foram crescendo e se popularizando, constituindo o que Vaz (2008) descreve como sendo uma prestação de serviços públicos de forma cada vez mais integrada e eficiente, e com foco no atendimento das necessidades do cidadão.

2.4 Considerações finais do capítulo

Vinte anos atrás, Cunha (1994) já afirmava que a importância do uso das TICs na administração pública é uma tendência cada vez mais forte, que tem por objetivo melhorar a qualidade do serviço oferecido e aumentar a eficiência do serviço prestado. Além disso, como destacam essa autora e também Vaz (2008), seu uso tem como

objetivo facilitar o processo de ampliação e melhoria dos serviços prestados, sendo essencial para a melhor utilização dos recursos e maximização de benefícios agregados e aumento do nível de serviços prestados ao cidadão e à sociedade.

Para Cunha (1994),

> *"a TI afeta a organização pública de forma semelhante ao modo como afeta a empresa privada. Entre as dimensões já citadas em capítulo anterior, afeta a habilidade da organização em inovar, afeta a estrutura da organização, afeta o controle, afeta poder e influência do indivíduo, afeta produtos e mercados, suporta e provoca reengenharia, permite o surgimento de groupware[2], aumenta as habilidades e a capacidade de decisão do decisor público, permite descentralização com os benefícios de se manter um controle centralizado, permite a criação de sistemas interorganizacionais, e utilizada estrategicamente, consegue, se não avanços em mercados competitivos como na iniciativa privada, a melhoria dos serviços ao cidadão. A TI permite clarificação, padronização e especialização de tarefas, permite o feedback em relação às tarefas realizadas, aumento da motivação pelo emprego da TI, e delegação de tomada de decisão, mantendo-se um controle centralizado"* (CUNHA, 1994, pág. 31)

Por último, Cunha aponta que o uso das TICs tem 4 impactos positivos na gestão pública:

1) Modernização: a TI é um instrumento de modernização dos serviços públicos oferecidos ao cidadão-cliente;
2) Alteração na relação de força entre o Estado e a Administração Pública: a informática acaba por facilitar o processo de modificação das relações firmadas entre o Estado e a sociedade local. O desenvolvimento de redes nacionais e regionais, bem como a interatividade com reder internacionais colabora para o processo de reagrupamento municipal, permitindo, além deste, a transparência no que se refere à fiscalização de contas por parte dos cidadãos.
3) Transparência e Administração: o principal intuito da informática é "sustentar a liberdade de todos na transparência, ao invés de preservar os privilégios e as fraudes de alguns, em detrimento de outros ou do conjunto da sociedade (...). Sistemas de informação podem conduzir a mecanismos de verificação da sociedade sobre aqueles que a dirigem" (CUNHA, 1994).
4) Reengenharia no serviço público: através da informatização do setor público, é possível viabilizar alterações fundamentais em processos, ou até mesmo realizá-los sem levar em consideração os antigos paradigmas e formas de executar tarefas.

[2]*Groupware:* conhecido como 'software colaborativo', é um software que apoia o trabalho em grupo, coletivamente. Pode ser definido como um "sistema baseado em computador que auxilia grupos de pessoas envolvidas em tarefas comuns (ou objetivos) e que provê interface para um ambiente compartilhado.

Adachi[3] (2004), por sua vez, aponta que a gestão de segurança de um canal deve abranger algumas áreas que visem minimizar riscos em sua atuação. Para tal, deve-se ter um padrão de segurança que abranja desde a infraestrutura tecnológica até o marketing/gestão pública. Para que isso ocorra, a autora divide em três camadas a gestão de segurança: física, lógica e humana.

Abaixo trazemos as definições de cada camada, bem como a sua importância para a informatização do Administração Pública:

1) Camada física: espaço em que se encontram os equipamentos informáticos (*hardwares)*. A gestão de segurança, nesta camada, é o controle de acesso que pode ser feito através do uso de senhas, biometrias ou documentos específicos.
2) Camada lógica: conjunto de informações dispostas de maneira lógica para serem inteligíveis por um *software*. Este adquire um papel básico, voltado somente para lidar com uma aplicação específica, efetuando e administrando transações realizadas na base de dados de seus respectivos bancos de dados, até a encriptação e decriptação de senhas e mensagens.
3) Camada humana: esta última é composta pelos recursos humanos que englobam todos o ambiente de redes e sua execução, manutenção e uso. Esta camada geralmente é a mais fraca entre as três, pois é a responsável, cronicamente, pela falha dos sistemas de segurança.

Assim, seguindo os autores, ao mesmo tempo em que a informatização do setor público traz avanços ao mesmo, acaba por gerar riscos. Por mais que as primeiras duas camadas possam ser mais seguras, o usuário – a camada humana – pode comprometer essa segurança.

Ao passo em que o Estado se moderniza, as Tecnologias de Informação e Comunicação são aperfeiçoadas, tentando coibir, de alguma maneira, falhas que possam prejudicar, de alguma maneira, o setor público. Infelizmente, nem sempre é possível.

Cada país acaba por criar maneiras de se assegurar de tais falhas, seja através do aperfeiçoamento de *softwares*, seja através de melhorias, readequação e criação de legislações específicas que sejam voltadas para esta questão. Cabe, acima de tudo, entender a importância da legislação em nosso país e como cada país aborda esta questão.

[3] Embora o estudo da autora refira-se ao *Internet Banking*, alguns princípios por ela abordados podem ser aplicados na Administração Pública.

Portanto, cabe perguntar: qual a posição do Brasil frente aos cibercrimes? Como outros países aborda essa questão? O que podemos aprender com as experiências deles?

CAPÍTULO 3 - CIBERCRIME: O CONCEITO E SUAS CLASSIFICAÇÕES

Antes de abordarmos a legislação brasileira, é necessário definir o que são os cibercrimes e suas classificações. Podemos defini-los como todo ato ilícito que cause danos morais ou patrimoniais à vítima, sendo estes danos cometidos através da internet. Estes dividem-se em 3 categorias: puros, mistos e comuns, conforme aponta Pinheiro (2000).

Os cibercrimes classificados como puros são aqueles cuja conduta ilícita visa única e exclusivamente o sistema computacional, através de atentado físico ou técnico do equipamento e seus componentes – hardwares e softwares. Aqui, podemos citar os ataques a sites por parte de hackers – ataques, estes, realizados com a finalidade de tirá-los do ar, por exemplo.

Os crimes mistos são aqueles em que o uso da internet legitima a ação, sendo condição necessária à sua efetivação, ainda que o bem visado não seja restrito ao meio computacional – um exemplo deste tipo de crime ocorre quando da transferência de recursos financeiros de uma conta para outra de maneira ilegal através dos *Internet Bankings*.

Os cibercrimes comuns são aqueles que ocorrem através da internet, porém não se restringem unicamente ao seu meio para sua realização. Geralmente são crimes já vinculados a uma lei – por exemplo, a pornografia infantil, antes restrita a vídeos e fotos.

A partir deste ponto podemos citar dois grandes problemas em nosso país: a nossa legislação é precária e ineficaz e as nossas polícias não são devidamente capacitadas para investigarem e ou reprimirem estes tipos de ações. Novamente, dividiremos a argumentação em duas partes: legislações e análises técnico-científicas.

Destaca-se como fator-chave para a prevenção e punição de crimes cometidos por *hackers,* pessoas que sejam treinadas de acordo e a adoção de conjuntos e normas que regulamentem a cooperação internacional. Hoje, a falta de recursos e pessoal capacitado prejudica o andamento das investigações e punição dos mesmos, além da definição de estratégias internacionais.

Podemos afirmar que graças ao anonimato oferecido pela internet, a mesma se tornou um lugar propenso ao cometimento de delitos ao oferecer para o criminoso um maior índice de segurança, dada a facilidade de não serem identificados. Embora as inovações tecnológicas somente acrescentaram um novo cenário para o cometimento de crimes, não há previsão constante na lei que defina ou não a internet como uma nova possibilidade de se cometer alguma infração.

As facilidades geradas pelo desenvolvimento de softwares e hardwares e pela quantidade de informações armazenadas em bancos de dados fornecem o necessário

para que qualquer pessoa que tenha conhecimento mínimo sobre informática se torne um criminoso em potencial.

De acordo com Monteiro (2003), os criminosos virtuais são, em sua maioria, pessoas que trabalham na área de informática – são *insiders* e vinculam-se a uma empresa (via de regra) e são motivados, geralmente, pela ideia de lucro rápido. Além disso, escondem-se atrás da ideia de "anonimato" oferecido pela web para cometer crimes. As condutas ilícitas apontadas por Monteiro (2003) dividem-se em três fases de motivação, conforme aponta:

1) Instinto aventureiro: os criminosos são movidos pelo desejo de superar a máquina, o que leva ao estágio 2;
2) O segundo estágio define-se como um meio "fácil e seguro" de ganhar dinheiro extra;
3) É caracterizado por uma extensão do estágio anterior, uma vez que os infratores continuam a cometer crimes somente para manterem seus gastos – que costumam ser altos – e com equipamentos de informática de última geração.

Aos infratores, também são atribuídas classificações que correspondem ao tipo de "especificação" do delito. Antes de entrarmos neste tipo de classificação, vamos explicar o conceito da palavra *hacker* – comumente atribuída a todo delinquente virtual (MONTEIRO, 2003).

A origem da palavra *hacker* associa-se a criação e desenvolvimento dos primeiros sistemas de informação e, de maneira simplificada, pode ser traduzido como "aqueles que, burlando os sistemas de segurança de redes de computadores, conseguem acesso não autorizado ao sistema ou recurso por este disponibilizado (MONTEIRO, 2003)".

No mundo virtual há uma diferença quase que sagrada entre *hackers* bons e os ruins – conhecidos como *crackers*. Os primeiros têm como principal objetivo invadir sistemas virtuais para verificar a segurança da rede ou para aperfeiçoarem suas técnicas. Em contrapartida, o segundo grupo invade sistemas para fins pessoais; porém ambos violam os a privacidade e sigilo das informações contidas nestes sistemas.

Vianna (2003) classifica os criminosos em seis tipos, conforme segue:

1) Crackers de Servidores: hackers que invadem computadores ligados em rede;
2) Crackers de Programas: hackers que quebram proteções de softwares cedidos a título de demonstração para usá-los por tempo indeterminado;

3) Phreakers: hackers especialistas em telefonia móvel ou fixa;
4) Desenvolvedores de Vírus, *Worms* e *Trojans*: programadores que criam pequenos softwares que causam algum dano ao usuário;
5) Piratas: Indivíduos que clonam programas fraudando direitos autorais;
6) Distribuidores de *Warez: webmaters* que disponibilizam em suas páginas softwares sem autorização dos detentores dos direitos autorais.

Ainda de acordo com o autor, os *hackers* podem ser classificados como membros do grupo dos (VIANNA, 2003):

1) Curiosos: não causam nenhum tipo de lesão aos dados armazenados ou em transmissão pelas redes, querendo somente acessar dados;
2) Pichadores digitais: seu único objetivo é o reconhecimento e fama dentro do mundo virtual;
3) Revanchistas: grupo geralmente formado por antigos funcionários ou desempregados que fazem uso dos conhecimentos adquiridos para prejudicá-la;
4) Vândalos: seu único objetivo é lesar a vítima;
5) Espiões: seu único objetivo é obter informações particulares/secretas que estejam armazenadas nos computadores das vítimas;
6) Ciberterroristas: motivados por questões política ou religião, estes criminosos fazem uso do meio digital para cometerem atividades criminosas em prol de seus ideais;
7) Ladrões e estelionatários: lesam o patrimônio de suas vítimas.

Segundo Monteiro (2003), “a realidade social e cultural que permeia o ambiente digital torna extremamente complexa a confecção de um perfil do chamado criminoso virtual. Contudo, a complexidade de relações ilícitas potencializadas pela utilização das redes informáticas, bem como as inúmeras possibilidades de classificação desses criminosos, o que torna essa atividade muito mais *sui generis,* fazem com que a criminologia cada vez mais se interesse pelo tema e busque, dentro de seus pressupostos científicos, erigir um conceito científico a ser adotado pelo direito penal”.

A diversidade de ordens jurídicas atualmente existentes, bem como as diferentes concepções de atos ilícitos no meio virtual leva a um impasse: apesar de ser composta por uma rede internacional de usuários, quando um crime é praticado, é necessário determinar qual a lei é aplicável, variando, esta, de país para país. A dúvida gerada é: a lei aplicada deve ser a do país onde está o servidor utilizado pelo infrator, onde o infrator praticou o crime, onde o infrator reside ou onde os resultados de suas condutas são

produzidos e verificados em diversos países? (DIAS, 2012). Daí a importância de analisarmos como os diferentes países, e o Brasil em particular, estão construídas suas legislações, objeto de análise no capítulo seguinte.

CAPÍTULO 4 – ANÁLISE DA LEGISLAÇÃO: EM BUSCA DE UM *BENCHMARK*

Por ser constituída por um conjunto de redes interconectados globalmente, não há uma legislação, órgão internacional ou entidade que exerça domínio sobre a Internet. A regulamentação de seu uso, bem como as leis e punições acometidas ficam sob responsabilidade de cada país.

A fim de comparar com a legislação brasileira de combate a delitos virtuais, procurou-se pesquisar legislações internacionais, dando ênfase à legislação dos Estados Unidos da América, país que julgamos mais avançado em combates e prevenção aos crimes virtuais, dada a sua posição de destaque e por ter sido o país que começou a pensar primeiramente em delitos deste tipo. Tomaremos como referencial os estudos de Andrade (2006) e Santos (2011).

O capítulo se divide da seguinte forma: a seção 4.1 trata das legislações internacionais, e a seção 4.2 se foca no estado da arte no Brasil.

4.1 Experiências no exterior

4.1.1 Estados Unidos da América

Nos EUA, por exemplo, a ideia de se regulamentar a criminalização dos delitos informáticos se iniciou em 1977, após o Senado ter recebido um Projeto de Lei do Senador Ribikoff – que não foi aprovado. Em 1984, por sua vez, o Congresso norte-americano aprovou o *Electronic Communication Privacy Act* (ECPA), a primeira legislação no mundo referente ao e controle de um computador. Após sua aprovação, tanto o FBI quanto os Estados federados passaram a adotar o ECPA como principal ação para inibir os crimes cometidos. Em 1986 o Congresso aprovou a *Computer Fraud and Abuse Act*, vigorando até os dias de hoje.

Neste país, os cibercrimes são considerados crimes graves e o sistema judiciário deste país tem sido acusado de opressor por importantes segmentos da opinião pública. Em janeiro de 2013, por exemplo, o corpo de Aaron Swartz, 26 anos, foi encontrado em seu apartamento; o motivo: enforcamento. O ciberativista, que defendia o livre acesso a documentos e informações na rede, foi preso em julho de 2011 sob a acusação de ter invadido alguns computadores e ter roubado mais de 4 mil arquivos confidenciais do *Massachusetts Institute of Technology* (MIT) e do *Jstor* (arquivo de revistas e trabalhos científicos). Caso fosse condenado, deveria pagar US$ 1 milhão em multas e enfrentar 35 anos de reclusão. Após o fato, a senadora Zoe Lofgren propôs o projeto de lei

nomeado de “Lei Aaron”, cujo objetivo principal é modificar a já conhecida Lei de Fraude e Abuso de Computadores, de 1984, bem como o estatuto de fraude eletrônica.

Retornando à legislação e doutrinas realizadas neste país, uma medida apresentada no Congresso dos EUA – e diga-se de passagem, uma das mais polêmicas – foi a proposta do Projeto de Lei S.O.P.A (Stop Online Piracy Act). Seu principal objetivo era o encerramento de qualquer de qualquer site que fosse considerado suspeito de armazenar e divulgar materiais que, porventura, violassem os direitos autorais ou de propriedade intelectual de seu proprietário original e que fossem usados sem a sua permissão. As medidas propostas causaram um grande reboliço e um protesto de dimensões gigantescas foi realizado.

O projeto de lei SOPA recebeu apoio da indústria cinematográfica de Hollywood e da indústria musical, porém, enfrentou constantes manifestações pró liberdade de expressão, argumentando que esta lei permitiria ao governo encerrar sites – inclusive no exterior.

Em maio de 1990 houve o primeiro grande caso envolvendo o governo dos EUA e Roberto Tappan Morris. O réu era acusado de colocar um dos primeiros *worms*[4] na rede, com a finalidade de explorar vulnerabilidades nos sistemas. O destaque para este caso é simples: uma vez conectado à rede e situado em diferentes estados, estes computadores eram considerados como sendo de interesse federal. Assim, qualquer crime cometido seria julgado como crime federal, baseando-se no *Computer Fraud and Abuse Act (CFAA)*.

Podemos apontar como condutas criminosas definidas pelo CFAA (18 U.S.C. § 1030):

a) Acessar um computador sem autorização, objetivando a obtenção de dados da segurança nacional;
b) Acessar um computador com intenções de obter de maneira dolosa: 1b) informações de sistema financeiro/instituição fiscal; 2b) informações de um departamento ou agência do governo; 3b) informações armazenadas em qualquer computador protegido;
c) Acessar de maneira dolosa e sem autorização, um computador do governo;
d) Acessar um computador protegido ou exceder a permissão de acesso para prática de estelionato;

[4] O conceito de *worm* pode ser definido como um subgrupo de vírus; é um programa que se multiplica, porém sem infectar outras máquinas. Para seu funcionamento, é preciso que este vírus se instale em um computador e se espalhe para outros através de conexões em rede.

e) Causar danos em um computador ou arquivo armazenado em um computador e;
f) Fornecer senhas ou informações sensíveis de computadores do governo americano.

Nos EUA, há inúmeras leis que, como já citado, visam a proibição de acesso aos dados sigilosos dos cidadãos. Uma das mais referenciadas quando falamos de crimes virtuais é a lei 18 U.S.C § 1029 que tipifica a criação, distribuição e utilização de códigos e aparelhos que forneçam acesso aos sistemas de dados norte-americano. A lei 18 § 1030 proíbe o acesso a computadores do governo e tem grande importância no que diz respeito ao combate de crimes digitais. Para os crimes que sejam tipificados como leves, as punições variam em até seis meses de condicional, enquanto delitos mais graves podem chegar a 20 anos de prisão (STRICKLAND, s/d).

Outra lei muito comum nos EUA é a Lei de Privacidade (*Privacy Act*, 1974), que visa regulamentar a coleta, uso e disseminação de informações de caráter pessoal de cada cidadão cujos dados são mantidos em um banco de dados do governo.

Essa lei estipula medidas para o próprio governo, que abrangem desde a revelação de informações pessoais, a localização e bem-estar do cidadão ou questões legais até a revelação de quaisquer informações sobre um cidadão americano para qualquer outra pessoa – incluindo familiares – ou para a mídia oi governos estrangeiros. Esta Lei estipula que só será possível a revelação dessas informações se, e somente se, houver a emissão de uma permissão escrita pelo próprio cidadão.

Para investigar crimes praticados através do mundo virtual, O F.B.I tem desenvolvido diversas estratégias para fazer frente às crescentes e complexas investigações praticadas no mundo virtual, dentro e fora dos E.U.A. Os escritórios do FBI, tanto nacionais quanto em outros países, utilizam técnicas avançadas para investigar e coordenar incidentes cibernéticos ao redor do planeta.

Nos EUA há uma parceria entre o Internet Crime Complaint Center, conhecido como IC3, o FBI e o National White Collar Crime Center (NW3C), com o objetivo de processar denúncias de crimes cibernéticos e coordenar as investigações cibercriminais. O FBI conta, ainda, com uma Cyber Division (Divisão Cibernética) – com sede em Washington DC – cujo objetivo é coordenar investigações em redes ou computadores que porventura sejam utilizados como instrumentos em ações criminosas ou em casos em que se tornaram vítimas de ações delituosas. Em casos em que organizações criminosas/terroristas estão envolvidas ou há algum tipo de ‘operação de inteligência’ patrocinada por governos de outros países, as investigações assumem caráter de prioridade alto.

Todos os agentes do FBI, segundo informações disponíveis para consulta pública, são treinados e certificados em informática forense. Também trabalham em escritórios de campo para recuperar/preservar evidências virtuais. Além disso, é mantido um laboratório forense na capital dos EUA cujo objetivo é fazer uso de técnicas avançadas para recuperar evidências, pesquisas e desenvolvimento de novas técnicas. Na maioria destes escritórios, há esquadrões especializados em ações virtuais, conhecidos como “Cyber Action Teams” ou CATS, responsáveis por fornecer assistência especializada nas investigações criminais e persecuções em juízo.

O FBI ainda classifica os crimes cibernéticos em duas categorias: crimes que são praticados com o uso do computador e crimes nos quais um computador uma rede se torna o alvo do delito. Quando usado como instrumento de auxílio, pode incluir o armazenamento de registros de fraudes, uso de identidades falsas, a reprodução e distribuição de material que infrinja os direitos autorais, pornografia infantil, entre outros crimes.

Em crimes em que o alvo é o computador em si, por sua vez, o FBI aponta que ações criminosas podem vir a causar algum tipo de dano ou alteração no mesmo, implicando que os equipamentos venham a ser comprometidos e que possam ser usados como objetos de ataques contra outros computadores ou redes.

A vasta legislação existente neste país também implica em uma investigação que seja praticada por meios eletrônicos, sendo o principal foco de preocupação uma eventual exposição pública da vítima.

Assim, qualquer decisão que remeta a uma investigação é tomada conjuntamente entre o FBI e a Procuradoria norte-americana.

Recentemente, a Kaspersky Labs, empresa voltada para segurança virtual, proteção de softwares e antivírus, divulgou a descoberta de um *malware*[5] cujo alvo eram instituições governamentais – como embaixadas, centros de investigações nucleares, entre outros - projetado para roubar arquivos criptografados e, indo além, sua capacidade incluía recuperar arquivos que foram apagados.

Segundo Alan Woodward, professor da University of Surrey – Inglaterra, este ciber ataque é bastante significativo, pois lidou com arquivos específicos – haja visto os arquivos criptografados.

A Kaspersky informou, através de um comunicado, que o foco principal deste ciber ataque direcionou-se aos países da Europa Oriental, como as antigas repúblicas da ex União das Repúblicas Socialistas Soviéticas, além de países da Ásia Central, embora tenham sido descobertas vítimas em todo o mundo – como na Europa Ocidental e América Latina.

---

[5] *Malware*: em português, programa malicioso.

Vitaly Kamluk, responsável pelas pesquisas realizadas pela Kaspersky, disse que as vítimas foram selecionadas de maneira bem cuidadosa e que, embora o *malware* venha comprometendo sistemas de 2007, o mesmo só foi descoberto em outubro de 2012.

Apelidada de “Red October” (Rocra e, em português, Outubro Vermelho – em alusão ao submarino russo da obra de Tom Clancy), chama a atenção a semelhança que apresenta quando comparado ao “Flame”, um código malicioso, também descoberto no ano passado e cujas semelhanças entre ambos aponta a composição de vários módulos distintos, cada um com seu objetivo definido ou com função especificada.

Além disso, Woodward aponta que a capacidade do “Red October” em esconder-se em um software, dando a impressão de que foi excluído – embora seja ativado assim que uma tarefa básica é realizada, como quando o usuário envia um e-mail – chamou e muito a atenção do professor.

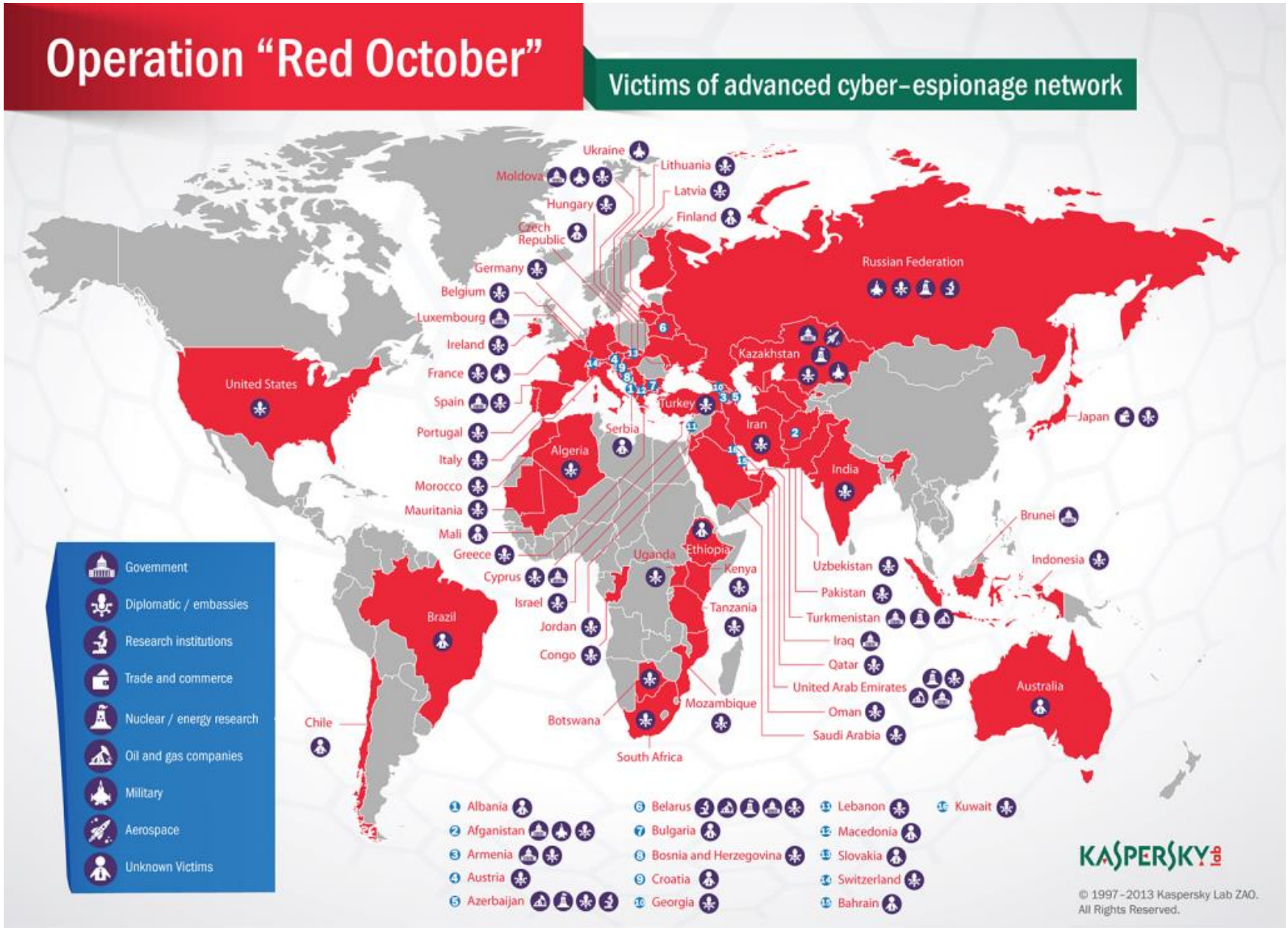
Uma análise realizada no *malware* apontou, ainda, a existência de um módulo destinado a trabalhar com arquivos criptografados com um sistema conhecido como “Cryptofiler”, amplamente utilizado por agências de inteligência antigamente – porém, ainda é utilizado por agentes da OTAN, que buscavam proteger sua privacidade e informações com alto valor.

Infelizmente ainda não há nenhuma pista sobre a origem deste programa, embora tenha sido encontrado em diversas partes de seu código, vocábulos de origem russa – o que levantaria suspeitas dos programadores e de sua localidade. Porém, este tipo de evidência em nada se torna significativo ao passo que, no mundo virtual, o investigador pode ser direcionado a chegar em uma falsa conclusão, somente baseado em evidências que, porventura, viessem a ser implantadas.

Fica divulgado pela Kaspersky, ainda, que o “Red October” teve 55 mil alvos de conexão dentro de 25º diferentes endereços de IP, o que, traduzindo para a linguagem comum, aponta que um grande número de computadores foi infectado de maneira individual – equipamentos de organizações governamentais, usuários comuns, Embaixadas, Institutos de Pesquisa e organizações voltadas para a pesquisa de fontes nucleares de energia, companhias de óleo e gás, bancos de dados militares e bancos de dados espaciais. Abaixo segue um mapa da Operação “Red October”, divulgado pela Kaspesky, mostrando a localidade e órgãos dos países afetados.

Operation “Red October”

Victims of advanced cyber-espionage network



KASPERSKY lab

Segundo os pesquisadores da Kaspersky, os ataques são provenientes da Rússia e da China. Disseram, ainda que os códigos possuem gírias que dificilmente um programador que não é russo saberia utilizar, e os domínios da operação foram todos registrados em serviços russos. No entanto, as falhas de segurança utilizadas são típicas de ataques chineses, mas, mesmo assim, o código programado diferencia-se de códigos utilizados pelo país asiático.

Acreditando que o ataque tenha finalidade política, os pesquisadores apontaram que não é possível identificar com precisão o local de origem deste vírus; a Rocra infectou não só redes governamentais, mas, também, computadores, smartphones e dispositivos de armazenamento removíveis (como, por exemplo, pen drives).

Ativa há cinco anos, todos os aparelhos e redes afetados foram infectados através de uma falha no sistema operacional da Microsoft – mais precisamente, através dos softwares Word e Excel. A partir daí, os computadores enviavam mensagens para os servidores centrais do ataque para receber arquivos maliciosos customizados com mais de 20 dígitos, desenvolvidos para cada alvo em específico.

A Kaspersky identificou, ainda, centenas de infecções e mais de mil módulos maliciosos que são capazes de recuperar mensagens do Outlook, tirar *screenshots*[6] da tela, acessar documentos e arquivos, extrair senhas salvas e roubar dados de telefones conectados (iOS, Windows Phone, Nokia) aos computadores centrais. Outra capacidade do *malware* é a de roubar até arquivos excluídos de pen drives.

O chefe de pesquisas da instituição, Vitaly Kamluk, disse que as vítimas foram cuidadosamente selecionadas. "(O ataque) foi descoberto em outubro. Começamos nossas checagens e rapidamente compreendemos que essa é uma enorme campanha de ataque cibernético. Há um conjunto bem limitado de alvos afetados - cuidadosamente selecionados. Eles parecem estar relacionados a algumas organizações de alto perfil.

Há um módulo especial para a recuperação de arquivos apagados de cartões de memória". Para encerrar, o pesquisador afirmou, ainda, que "ele (o *malware*) monitora quando um cartão de memória é plugado e tenta então recuperar arquivos apagados. Nunca havíamos visto isso antes em um *malware*"[7], observa.

---

[6] *Screenshots*: em português, o tema traduz-se como "imagens". Neste caso, o malware "copiava" a tela do usuário e direcionava as imagens ao servidor central.

[7] **Descoberto vírus "que roubava documentos desde 2007"** Disponível em: http://www.bbc.co.uk/portuguese/noticias/2013/01/130115_malware_red_october_rw.shtml. Atualizado em 15 de janeiro de 2013.

4.1.2 Europa e Convenção de Budapeste

Levando a discussão de cibercrimes para a Europa, é de conhecimento público que o Conselho Europeu assinou a Convenção sobre o Cibercrime, em Budapeste, no ano de 2001. A Convenção de Budapeste – ou Convenção sobre o Cibercrime – criada pelo Conselho da Europa e realizada na Hungria, em 2001, tipifica os crimes ocorridos através da internet.

Prioriza, ainda, uma política criminal que seja comum aos países-membros da UE, objetivando a proteção da sociedade contra a criminalidade no espaço virtual e que seja designada através da adoção de uma legislação adequada, além da melhoria da cooperação internacional.

O documento divide-se em quatro capítulos (Terminologia, Medidas a Tomar a Nível Nacional, Cooperação Internacional e Disposições Finais) e conta com 48 artigos. Em seu preâmbulo, dispõe que *"considerando que o objetivo do Conselho da Europa é realizar uma união mais estreita entre os seus membros"* e visando "*intensificar a cooperação com os outros Estados (com) o objetivo de proteger a sociedade contra a criminalidade no ciberespaço"*, é necessária para impedir os atos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos (CONSELHO EUROPEU, 2001).

A Convenção de Budapeste foi aprovada sem a participação do Brasil (o Capítulo 3 da própria Convenção, sob o Título de "Auxílio Mútuo" entre países, explicita que "o Comitê de Ministros do Conselho da Europa pode (…) convidar qualquer Estado não membro do Conselho e que não tenha participado na sua elaboração, a aderir à presente Convenção" (COUNCIL OF EUROPE, 2001).

Embora várias conversas de cunho diplomático entre representantes governamentais brasileiros e europeus foram realizadas, não foi verificado um grande empenho brasileiro em se tornar país signatário da Convenção), entrando em vigor, somente, em 2004 – após a ratificação de, somente, cinco países. Embora aberta à adesão de qualquer país do mundo, até hoje e texto foi ratificado por mais 25 países, principalmente países do Leste Europeu e parte da Europa Central.

O Brasil, até o momento, não aprovou o texto, mesmo depois de ser analisado pelos mais diversos órgãos do governo (desde o Ministério da Justiça até pelo Gabinete de Segurança Institucional da Presidência da República passando, ainda, pelo crivo do Departamento de Polícia Federal, pelo Ministério e Ciência e Tecnologia e pelo Ministério de Relações Exteriores).

Os países que adotaram a Convenção são, principalmente, países que já cumpriram a tarefa de regulamentar a Internet – do ponto de vista civil e, somente depois disso, estabeleceram parâmetros criminais para a rede. Em contrapartida, nós não podemos tentar

harmonizar nossa legislação com essa convenção (que sequer foi aprovada pelo governo brasileiro), pois podemos correr o risco de seguir a via inversa: criar primeiro punições criminais, sem antes regulamentar técnica e civilmente a Internet no país.

Na tabela a seguir, são apresentados os países signatários da Convenção de Budapeste[8] até dezembro de 2013:

[8] Lista oficial de países signatários da Convenção de Budapeste, atualizada em 02 de dezembro de 2013, divulgada pelo próprio Conselho Europeu em seu sítio eletrônico. Mais informações podem ser obtidas no endereço: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG. Acessado em 21 de novembro de 2013.

Council of Europe

Treaty Office

Convention on Cybercrime
CETS No.: 185

Treaty open for signature by the member States and the non-member States which have participated in its elaboration and for accession by other non-member States

Opening for signature
Place: Budapest
Date : 23/11/2001

Entry into force
Conditions: 5 Ratifications including at least 3 member States of the Council of Europe
Date : 1/7/2004

Status as of: 5/12/2013

Member States of the Council of Europe

	Signature	Ratification	Entry into force	Notes	R.	D.	A.	T.	C.	O.
Albania	23/11/2001	20/6/2002	1/7/2004				X			
Andorra	23/4/2013									
Armenia	23/11/2001	12/10/2006	1/2/2007				X			
Austria	23/11/2001	13/6/2012	1/10/2012		X	X	X			
Azerbaijan	30/6/2008	15/3/2010	1/7/2010		X	X	X	X		
Belgium	23/11/2001	20/8/2012	1/12/2012		X	X	X			
Bosnia and Herzegovina	9/2/2005	19/5/2006	1/9/2006				X			
Bulgaria	23/11/2001	7/4/2005	1/8/2005		X	X	X			
Croatia	23/11/2001	17/10/2002	1/7/2004				X			
Cyprus	23/11/2001	19/1/2005	1/5/2005				X			
Czech Republic	9/2/2005	22/8/2013	1/12/2013		X	X	X			
Denmark	22/4/2003	21/6/2005	1/10/2005		X		X	X		
Estonia	23/11/2001	12/5/2003	1/7/2004				X			
Finland	23/11/2001	24/5/2007	1/9/2007		X	X	X			
France	23/11/2001	10/1/2006	1/5/2006		X	X	X			
Georgia	1/4/2008	6/6/2012	1/10/2012			X				
Germany	23/11/2001	9/3/2009	1/7/2009		X	X	X			
Greece	23/11/2001									
Hungary	23/11/2001	4/12/2003	1/7/2004		X	X	X			
Iceland	30/11/2001	29/1/2007	1/5/2007		X		X			
Ireland	28/2/2002									
Italy	23/11/2001	5/6/2008	1/10/2008				X			
Latvia	5/5/2004	14/2/2007	1/6/2007		X		X			
Liechtenstein	17/11/2008									
Lithuania	23/6/2003	18/3/2004	1/7/2004		X	X	X			
Luxembourg	28/1/2003									
Malta	17/1/2002	12/4/2012	1/8/2012			X				
Moldova	23/11/2001	12/5/2009	1/9/2009			X	X	X		
Monaco	2/5/2013									
Montenegro	7/4/2005	3/3/2010	1/7/2010	55	X		X			
Netherlands	23/11/2001	16/11/2006	1/3/2007				X	X		
Norway	23/11/2001	30/6/2006	1/10/2006		X	X	X			
Poland	23/11/2001									
Portugal	23/11/2001	24/3/2010	1/7/2010			X	X			
Romania	23/11/2001	12/5/2004	1/9/2004				X			
Russia										
San Marino										
Serbia	7/4/2005	14/4/2009	1/8/2009	55			X			
Slovakia	4/2/2005	8/1/2008	1/5/2008		X	X	X			
Slovenia	24/7/2002	8/9/2004	1/1/2005				X			
Spain	23/11/2001	3/6/2010	1/10/2010			X	X			

Sweden	23/11/2001									
Switzerland	23/11/2001	21/9/2011	1/1/2012		X	X	X			
The former Yugoslav Republic of Macedonia	23/11/2001	15/9/2004	1/1/2005				X			
Turkey	10/11/2010									
Ukraine	23/11/2001	10/3/2006	1/7/2006		X		X			
United Kingdom	23/11/2001	25/5/2011	1/9/2011		X		X			

Non-members of the Council of Europe

	Signature	Ratification	Entry into force	Notes	R.	D.	A.	T.	C.	O.
Argentina										
Australia		30/11/2012 a	1/3/2013		X		X			
Canada	23/11/2001									
Chile										
Colombia										
Costa Rica										
Dominican Republic		7/2/2013 a	1/6/2013			X	X			
Israel										
Japan	23/11/2001	3/7/2012	1/11/2012		X	X	X			
Mauritius		15/11/2013 a	1/3/2014				X			
Mexico										
Morocco										
Panama										
Philippines										
Senegal										
South Africa	23/11/2001									
United States of America	23/11/2001	29/9/2006	1/1/2007		X	X	X			

Total number of signatures not followed by ratifications:	11
Total number of ratifications/accessions:	41

Notes:
(55) Date of signature by the state union of Serbia and Montenegro.
a: Accession - s: Signature without reservation as to ratification - su: Succession - r: Signature "ad referendum".
R.: Reservations - D.: Declarations - A.: Authorities - T.: Territorial Application - C.: Communication - O.: Objection.

Source : Treaty Office on http://conventions.coe.int – * Disclaimer

O texto da Convenção é dividido e tipificado da seguinte maneira:

- Capítulo 1: Terminologia (Artigo 1);
- Capítulo 2: Medidas a tomar a nível nacional (Artigos 2 a 22);
- Capítulo 3: Cooperação Internacional (Artigos 23 a 35);
- Capítulo 4: Disposições finais (Artigos 35 a 48).

Passando rapidamente pela adoção da Convenção de Budapeste na Europa, alguns países membros – como Portugal e Itália – embora tenham assinado o tratado, só começaram a realizar algumas mudanças anos depois: a Convenção passou a valer comente em 1º de julho de 2004. Brevemente, os casos de Portugal e Itália serão abordados.

Portugal foi um dos países que adotou a Convenção tardiamente: ratificou o Tratado em 2009, para o seu ordenamento jurídico interno, criando a Lei do Cibercrime (Lei 109/2009), definindo como crimes de informática:

a) Falsidade informática (disposta no artigo 3º);
b) Danos relativos a programas ou outros dados informáticos (artigo 4º);
c) Sabotagem informática (artigo 5º);
d) Acesso ilegítimo a dados/informações (artigo 6º);
e) Interceptação ilegítima (artigo 7º) e;
f) Reprodução ilegítima de um programa protegido (artigo 8º).

Para Andrade (2006), a legislação portuguesa é uma das mais completas sobre o tema: é ampla e há previsões tanto no Código Penal quanto em leis esparsas. Atualmente, vigora a Lei da Criminalidade Informática (Lei 109/91) no país; além de tipificar crimes, também define conceitos-chave restrito, normalmente, ao mundo da informática.

A Lei da Criminalidade Informática (LCI) portuguesa, por sua vez, é composta por:

a) Responsabilidade criminal das pessoas coletivas;
b) Subsidiariedade do Código Penal;
c) Falsidade Informática;
d) Dado relativo a dados ou programas informáticos;
e) Sabotagem informática;
f) Acesso ilegítimo;
g) Intercepção ilegítima;
h) Reprodução ilegítima de programa protegido.

Os delitos cometidos, por sua vez, classificam-se em seis classes: falsidade informática, danos relativos a dados ou programas informáticos, sabotagem informática, acesso ilegítimo, interceptação ilegítima e reprodução ilegítima de programa protegido (ANDRADE, 2006).

Já a Itália, um dos países que fazem parte da Convenção de Budapeste, aborda em sua legislação significativos temas para a investigação e combate aos cibercrimes. Embora seja um dos países signatários da Convenção, o sistema italiano desenvolveu, também, uma

legislação interna específica para os cibercrimes. Segundo Vito Cuscianna[9], especialista em crimes informáticos e membro da Polizia di Stato, do Servizio Polizia Postale e delle Comunicazioni – Roma, atuando na Sezione Investigazioni Informatiche, a estrutura de investigação dos cibercrimes cometidos é bastante grande e possui núcleos diferenciados para cada área – por exemplo, crimes de pedofilia, fraude, terrorismo e/ou organizações criminosas.

Andrade (2006) também aponta a importância da legislação italiana, definindo-a como uma das mais avançadas no que remete à identificação, investigação, combate e prevenção dos cibercrimes. A Lei nº 547/93 define seis figuras essenciais que se caracterizam como crimes com maior grau de gravidade: sabotagem, acesso ilegal de informações e dados, violação de segredos informáticos e sigilo, falsificações em geral, fraudes informáticas e a violação dos direitos do autor no que tange a propriedade de registro da concepção de softwares (ANDRADE, 2006).

Além destes o autor também aponta que o envio de qualquer tipo de vírus também é considerado como crime no país italiano, sendo tipificado pelo artigo 615 do Código Penal Italiano, que prevê a conduta daquele que dissemina, menciona ou envia um programa informática malicioso que interrompa o funcionamento de um sistema/computador de maneira total ou parcial – ao contrário da legislação brasileira que defende a existência de um crime se, e somente se, o vírus enviado provoque algum dano material ao destinatário.

4.1.3 América Latina

Trazendo o nosso trabalho para um âmbito mais “familiar”, uma das primeiras ações tomadas na América Latina, focando a proteção de dados pessoais, ocorreu no ano de 2003, na Bolívia. A *XII Cumbre Iberoamericana de Jefes de Estado y de Gobierno*, realizada nos dias 14 e 15 de novembro na cidade de Santa Cruz de la Sierra reconheceu como direito fundamental do indivíduo a garantia da proteção de seus dados.

Antes, a Argentina foi um dos primeiros países a adotar medidas cabíveis sobre este assunto. A sanção da Lei nº 25.326 em 04 de outubro de 2000 e promulgada em 30 de outubro deste mesmo ano afirmava, como objetivo principal, a proteção de dados pessoais que fossem armazenados de maneira integral em arquivos, registros, bancos de dados ou quaisquer outros meios utilizados para o tratamento de dados.

---

[9] Delegado gaúcho troca experiências com policial italiano sobre cibercrimes. Disponível em: http://www.internetlegal.com.br/2010/01/delegado-gaucho-troca-experiencias-com-policial-italiano-sobre-cibercrimes/

Em 2008 a Lei nº 25.326 foi alterada e no Código Penal Argentino foi inserida a regulamentação das condutas consideradas crimes, conforme seguem: armazenamento, distribuição ou divulgação de materiais que contenham pornografia infantil; acesso e interceptação da comunicação eletrônica; acesso ilegal aos dados armazenados num sistema informacional protegido.

A publicação de informações que causem quaisquer tipos de danos ou prejuízos a terceiros; acesso ilegítimo ao sistema informacional que armazena dados informáticos; alteração do funcionamento normal e correto de um sistema informático; destruição, inutilização ou alteração de programas ou dados que estejam armazenados em um banco de dados ou sistema e, por último, a interrupção da comunicação eletrônica.

Em 30 de outubro de 2001 a Venezuela também tomou medidas relacionadas aos crimes virtuais e promulgou a Lei Especial Contra os Delitos Informáticos, sendo considerada por Andrade (2006) “como um dos mais completos da América Latina sobre o tema”.

Conforme aponta o autor, “as principais condutas descritas como crime pela referida legislação são:

a) acesso indevido (artigo 6º);
b) sabotar ou danificar um sistema informático (artigo 7º);
c) acesso indevido de um sistema informático protegido (artigo 9º);
d) espionagem informática (artigo 11);
e) violação da privacidade de dado ou informação de caráter pessoal (artigo 20);
f) violação da privacidade das comunicações (artigo 21);
g) revelação indevida de dado ou informação de caráter pessoal (artigo 22);
h) difusão ou exibição de material pornográfico infantil (artigo 23)”.

Após as discussões sobre legislação e gerenciamento da Internet no mundo, apresentamos o caso brasileiro, foco de nosso estudo, a seguir.

4.2 E no Brasil, como estamos?

Uma vez feitas algumas considerações sobre a legislação adotada em outros países, entraremos no estudo da legislação brasileira, comparando-a com a legislação dos EUA (muitas vezes, adotada como modelo no combate e prevenção de cibercrimes).

A fim de analisar quão distantes ou o quão atrasados estamos ou o quanto falta para alcançar as medidas tomadas pelo governo norte-americano na proteção de interesses civis e governamentais, faremos uma análise do nosso cenário legislativo interno.

Há algum tempo o Brasil procurou melhorar a sua imagem perante a comunidade internacional no que remete a assuntos penais. De acordo com Silva (2012), por ser a sexta maior economia global, o Brasil se tornou vítima de altas taxas de delitos transnacionais, estreitando o elo brasileiro com a comunidade internacional no que compete à legislação penal.

Com base nas informações levantadas para o desenvolvimento da pesquisa, ficou claro que há uma grande dificuldade no cenário brasileiro em formular legislações específicas e desenvolver punições à altura dos crimes cibernéticos cometidos.

Com o grande crescimento do número de usuários brasileiros da rede[10] ao longo dos anos, mais comuns são os crimes cometidos através dela.

Quando falamos do princípio da reserva legal, que consta no 1º Artigo do Código Penal Brasileiro, em que "não há crime sem lei anterior que o defina", é necessário reforçar a necessidade de uma legislação que seja específica para crimes informáticos.

Enquanto as inovações tecnológicas avançam consideravelmente, é necessário aceitar que a legislação brasileira ficou para trás, e que diante desta situação, não é possível apenas falar em prevenção, sendo necessário uma política criminal de caráter repressivo. Alguns pesquisadores desta área julgam mais eficientes políticas de prevenção do que previsão legal.

O Projeto de Lei nº 84/99, proposto pelo deputado Luiz Piauhylino e conhecido como "Lei Azeredo", *"pode causar profunda alteração no ordenamento jurídico Brasileiro"*, conforme apontado por Rezende (2008), pois pretende alterar os Códigos Penal e de Processo Penal, atualizando as leis já existentes - Lei Ordinária 12.735/2012.

Dispõe, ainda, sobre os crimes, penalidades e providências relacionadas à área de informática. Logo no Artigo 1º é descrito que "a disseminação de informações através da rede de computadores (deve respeitar) os critérios de garantia dos direitos individuais e coletivos e de privacidade segurança de pessoas físicas e jurídicas".

A Lei Azeredo foi o pontapé inicial para gerar uma mobilização social acerca de questões sobre a Internet no Brasil – embora este tenha vindo de um desarquivamento de

[10] Segundo dados divulgados pela F/Nazca Datafolha, em abril de 2011, o Brasil já contava com 81,3 milhões de usuários da rede. Disponível em: http://www.fnazca.com.br/wp-content/uploads/2011/08/fradar_9a_edicao.pdf. Acessado em 15 de novembro de 2013.

versão modificada de um PL proposto em 2006 (CGI.br, 2011). Ganhou destaque (e diferenciou-se dos outros Projetos de Lei propostos anteriormente) quando propôs a conjugação da “criminalização excessiva de condutas tidas como cotidianas, banais ou indispensáveis à inovação na rede”.

Além de criar crimes para a Internet, este projeto também criou obrigações de vigilância e ampliou consideravelmente o poder de investigação da polícia neste âmbito – sendo denominado por alguns ativistas como “AI-5 Digital”.

O PL 84/99 impôs aos provedores de serviços de Internet e aos provedores de conexão que guardassem os registros de conexão e de acesso de cada usuário por u7m período de 3 anos; criava também o dever destes servidores em informar às autoridades, de maneira sigilosa, qualquer suspeita de que algum usuário estivesse praticando algum crime. Adicionalmente, criminalizava o acesso não autorizado a um sistema informatizado (artigo 285-A).

Um outro problema que pode ser apontado neste projeto ocorre em sua redação: por ser imprecisa, a redação dos artigos tratava assuntos como a proteção de dados pessoais com pouco rigor técnico, corroborando com a ameaça dos direitos fundamentais do cidadão-usuário.

As críticas feitas ao PL 84/99 apontam que, mesmo que considerássemos o contexto atual da legislação brasileira e da redação do projeto, a sua aprovação traria grandes riscos do que muitos chamam de “desenvolvimento pleno da Internet no Brasil”. Estes riscos se apresentam como desincentivo à existência de um ambiente que fosse propício à inovação.

Em contrapartida, uma das principais justificativas utilizadas pelos defensores da aprovação deste PL remetia à harmonização da legislação brasileira com a Convenção de Budapeste (também conhecida como a Convenção do *Cybercrime* e já mencionada anteriormente).

A insegurança transmitida neste cenário de ameaças das liberdades básicas acabou por gerar a convicção geral de que a existência do PL 84/99, por si só, oferecia um grande risco ao mundo virtual e aos seus usuários – o que acabou por gerar uma mobilização da sociedade civil, da academia, das indústrias e de outras organizações (públicas e privadas). Destacou-se a criação da petição *on-line* “Em Defesa da Liberdade e do Progresso do Conhecimento na Internet Brasileira”, contando com mais de 160 mil assinaturas. O intuito desta petição era solicitar ao Senado Federal a não aprovação deste Projeto.

O engajamento social foi tão grande que acabou por incentivar a participação popular a participar diretamente no processo de regulação da internet no Brasil. Através deste engajamento, duas medidas extremamente importantes podem ser destacadas no processo

de regulação da Internet no Brasil: o Marco Civil da Internet e a Lei de Proteção aos Dados Pessoais.

Além destes, duas audiências públicas merecem destaque: a primeira, realizada em julho de 2011, foi promovida pelas comissões de Ciência e Tecnologia, Comunicação e Informática, Direitos Humanos e Minorias e, por último, de Segurança Pública e Combate ao Crime Organizado, e contou com a entrega da petição contrária ao PL 84/99 às mãos do próprio deputado Eduardo Azeredo.

A segunda audiência, realizada em novembro de 2011, contou com a participação de diversos segmentos da sociedade civil e das instituições de pesquisa e ensino para discutir alternativas à redação do projeto e dos PLs até então pensados.

Foi neste mesmo mês, em uma estratégia para a não aprovação do "AI-5 Digital", que o Deputado Paulo Teixeira (PT), propôs (em conjunto com outros deputados) o PL. 2.793/2011, dispondo sobre a tipificação dos cibercrimes, porém estando de acordo com as sugestões e recomendações elaboradas pelo Centro de Tecnologia e Sociedade da FGV Direito – RJ. O PL apresentado por Teixeira buscava ser aprovado contendo o mínimo necessário para coibir as práticas graves de delitos cometidos através da Internet, e deixando como incumbência do Marco Civil da Internet todo o papel de regulação da rede.

O Marco Civil da Internet, por sua vez, é a principal – e mais reconhecida – iniciativa de regulamentação da Internet, no Brasil. A sua criação – e redação, de coautoria do senador Eduardo Teixeira – ligam-se diretamente à mobilização contrária ao PL 84/99, sendo a principal estratégia para impedir o avanço desse projeto.

À época, o então Presidente da República, Luiz Inácio Lula da Silva, lançou o X Fórum Internacional do *Software* Livre (FISL), em 2009, com o principal objetivo de incitar a proposição de um Marco Civil para a Internet no Brasil. Assim, a Secretaria de Assuntos Legislativos do Ministério da Justiça, inspirou-se nos Princípios para a Governança e Uso da Internet (publicado pelo Comitê Gestor de Internet – CGI.br.) e, em parceria com o Centro de Tecnologia e Sociedade da Escola de Direito do Rio de Janeiro (CTS – FGV), deu início a um processo que fosse aberto, e colaborativo, de discussão *on-line* para a criação de uma lei básica para a Internet em nosso país.

O Marco Civil da Internet apresentou grandes inovações no cenário da rede brasileira. A principal delas remete ao processo de participação popular para a discussão do que deveria estar presente neste documento. Para que a participação pudesse, de fato, ser efetiva e concretizada, criou-se um sistema voltado para o recebimento de sugestões e comentários através do site Cultura Digital.

As consultas públicas dividiram-se em duas etapas. A primeira etapa iniciou-se em outubro de 2009, iniciada pelo Ministério da Justiça e durou, aproximadamente, 45 dias. Tinha como principal objetivo apresentar um documento que contivesse os princípios gerais para a regulação da rede (tendo sua inspiração na publicação dos "Princípios para a Governança e Uso da Internet no Brasil", publicado pelo CGI.br.).

A primeira fase de consulta contou com 800 comentários sobre o documento apresentado, sendo sistematizados e que se traduziram no texto do anteprojeto também posto em consulta pública *on-line*, encerrando-se em 30 de maio de 2010 e recebendo mais de 1.200 comentários ao longo do texto. Nesta fase, houve a participação de integrantes da sociedade civil e de empresas e associações voltadas para a indústria cultural e tecnológica (nacionais e internacionais) – o que aumentou ainda mais a diversidade de opiniões sobre o tema e, por consequência, a legitimidade do processo em si.

A segunda fase consistiu na leitura e comentários aos dispositivos propostos na Minuta de anteprojeto de lei; nesta fase, a discussão segue basicamente o mesmo formato adotado na primeira fase, mas tem como parâmetro a minuta de anteprojeto de lei. Mais uma vez, cada artigo, parágrafo, inciso ou alínea esteve aberto para apresentação de comentário por qualquer interessado.

Também os foros de discussão serão usados para o amadurecimento de ideias e para uma discussão irrestrita. A duração desta foi de 45 dias. Em ambas as fases de consultas públicas, o intuito era aumentar a participação popular no processo decisório, reconhecendo a relevância da opinião pública na construção do Marco Civil.

Depois de ser definido, o texto do Marco Civil foi dividido em cinco capítulos[11] (e 25 Artigos), a saber:

1) Disposições Preliminares;
2) Dos Direitos e Garantias dos Usuários;
3) Da Provisão de Conexão e de Aplicações de Internet;
4) Da Atuação do Poder Público;
5) Disposições finais.

O Marco Civil tornou-se inédito em relação aos projetos apresentados anteriormente ao prever os direitos e garantias dos usuários da Internet no âmbito civil, como já citado

[11] Disponível em: http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=32316#.Uoj1YMSfiP8. Acessado em 15 de novembro de 2013.

anteriormente – em oposição ao projeto de lei do senador Eduardo Azeredo. O Marco Civil da Internet tramita na Câmara, aguardando aprovação.

Além da L.O. 12.735/2012, podemos citar a Lei Ordinária 12.737/2012, também conhecida como Lei Carolina Dieckmann (de coautoria do Deputado Federal Paulo Teixeira), que entrou em vigor no mês de abril deste ano. Um dos delitos que passaram a ter tipificação legal é a invasão de computadores, produção e disseminação de dados maliciosos e a clonagem de cartões (FLORO, 2013). A seguir, segue um trecho da nova Lei:

> ***"Invasão de dispositivo informático***
>
> *Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:*
> *Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.*
> *§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no* ***caput****.*
> *§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.*
> *§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:*
> *Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.*
> *§ 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas.*
> *§ 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:*
> *I - Presidente da República, governadores e prefeitos;*
> *II - Presidente do Supremo Tribunal Federal;*
> *III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou*
> *IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal." (LEI Nº 12.737/2012).*

Além de enquadrar estes atos como penalmente puníveis, a Lei 12.737 traz algumas alterações em nosso Código Penal Brasileiro. A nova Lei trata determinadas condutas de realizadas na internet de modo a atender antigas demandas da sociedade civil. Uma das maiores mudanças se devem ao direito de defesa no Direito Civil e no Direito Penal.

Quando lesada no primeiro, cabe ao próprio cidadão se proteger, buscar um advogado, reunir provas que atestam sua inocência e mover uma ação contra aquele que o lesou. Já para o Direito Penal, a vítima passa a usufruir dos instrumentos estatais para sua proteção.

Um novo recurso que o cidadão poderá usufruir com a promulgação desta lei remete à criação de delegacias especializadas em crimes virtuais nas polícias Civil e Federal. Para o delegado Carlos Eduardo Sobral (FLORO, 2013),

> *"o cidadão poderá recorrer a essas delegacias para encontrar o amparo necessário para uma investigação e identificação de quem feriu o seu direito. Ao trazer o Estado junto à sociedade para garantir a segurança na internet, a lei garante também a liberdade plena daquelas pessoas que usam a rede como ferramenta de comunicação, integração e interação social"*.

Um dos grandes pontos tratados no que tange ao mundo cibernético no cenário brasileiro é a tipificação de crimes já previstos, em sua maioria, em nosso Código Penal (95% dos crimes cometidos na web são tipificados pelo CPB[12]), porém tratados como realizados num mundo paralelo – o virtual.

Em nosso cenário, as legislações específicas mais aplicadas remetem ao uso de logomarca de empresas sem autorização (crime previsto no artigo 195 da Lei 9.279/96, contra a propriedade industrial), monitoramento não avisado previamente (interceptação de comunicações informáticas – Lei 9.296/96, artigo 10) e cópia de software sem licença (crimes contra Pirataria, previstos no artigo 12 da Lei 9.609/98).

O órgão público responsável pelo julgamento de infrações virtuais é o Superior Tribunal Federal, cuja aplicação da lei consolida, cada vez mais, o uso dos dispositivos constitucionais existentes em diversos casos julgados. Casos de pedofilia, por exemplo, são enquadrados na Lei 8.069/90, artigo 241, definindo que apresentar, produzir, vender, fornecer, divulgar ou publicar – por qualquer meio de comunicação, inclusive a internet – fotografias ou imagens com pornografia ou cenas de sexo explícito que envolvam crianças ou adolescentes.

Para os casos em que a nossa legislação apresenta 'buracos', fica claro que ainda falta considerar o meio ou forma pelos quais os crimes são cometidos, já que 95%[13] dos mesmos já estão previstos no código penal, porém não considerando o meio virtual como cenário de um crime.

Além das leis citadas anteriormente, um novo Projeto de Lei do Deputado Federal Paulo Teixeira já circulava pelas casas em 2011, porém somente após o caso da divulgação de fotos íntimas da atriz Carolina Dieckmann que ficou claro fraqueza pela qual os crimes cibernéticos são tratados.

---

[12] **Justiça usa Código Penal para combater crime virtual. Disponível em:** http://www.stj.gov.br/portal_stj/publicacao/engine.wsp?tmp.area=398&tmp.texto=9010

[13] **Justiça usa Código Penal para combater crime virtual. Disponível em:** http://www.stj.gov.br/portal_stj/publicacao/engine.wsp?tmp.area=398&tmp.texto=9010

Em maio de 2013 foi aprovado o primeiro texto do Projeto de Lei 2793/11, e enviado, em seguida, para o Senado Federal. Objetivando tipificar criminalmente os delitos informáticos cometidos e dando outras providências, inclui em nosso Código Penal leis específicas, detalhadas e ajustadas, incluindo a penalização por crimes cometidos a partir de fraudes virtuais (roubo de senhas usadas para acessar conta bancária pela internet, por exemplo).

O principal objetivo deste PL é a garantia de segurança pessoal de cada cidadão e a proteção de seus direitos, garantindo que a navegação na internet ocorra de forma agradável e segura, sem o medo ou risco de que criminosos invadam suas máquinas e roubem informações sem correrem o risco de serem corretamente penalizados. Tornou-se previsto como crime neste mesmo PL a falsificação de cartões de crédito, a criação e distribuição de aplicativos cujo objetivo seja roubar, danificar e prejudicar o funcionamento de aparelhos eletrônicos (LEMOS, 2012).

Comparando ao caso brasileiro, por exemplo, há um problema na legislação norte-americana: o sistema judiciário deste país é intimidador e exagerado. O que leva a crer que a legislação poderia ser um pouco mais branda.

No Brasil, podemos afirmar que, embora o crescimento dos serviços de informação tenha aumentado grandemente, o ordenamento jurídico de nosso país não acompanhou com a mesma velocidade o crescimento das TICs.

Ao contrário do que ocorre nos EUA, a lentidão do poder legislativo em classificar e julgar estes crimes que são cometidos dão uma falsa sensação de um país sem leis, em que os criminosos sabem das dificuldades do sistema legislativo e tem a certeza de que não serão punidos por seus atos criminosos.

O nosso país ainda está atrasado em relação ao estado da arte internacional quando tratamos de medidas punitivas tomadas para inibir os cibercrimes. Ainda fomos muito insuficientes quando, por falta de recursos, especialistas ou, até mesmo, legislação, deixamos um cidadão sofrer algum tipo de lesão.

Como protetor, o Estado peca em fornecer segurança, em trabalhar para evitar que estes crimes aconteçam, ao contrário dos Estados Unidos, que tomam medidas de prevenção e punem de maneira mais rigorosa o infrator.

CAPÍTULO 5 – POLÍTICAS DE PREVENÇÃO, COMBATE E INVESTIGAÇÃO DE CIBERCRIMES E POLÍTICAS DE REGULAMENTAÇÃO E GESTÃO DA INTERNET NO BRASIL.

Uma vez discutida, no capítulo anterior, a legislação brasileira de combate ao cibercrime e suas limitações, cabe agora abordar o papel de dois importantes atores brasileiros na área de regulamentação e gestão da Internet no Brasil: o Comitê Gestor da Internet, bem como o papel da SaferNet (Associação Civil de direito privado que atua nacionalmente) como agentes sociais que têm seu papel no combate a crimes virtuais.

Atuando na área de ensino, combate, prevenção, regulação e promoção dos Direitos Humanos, estas duas organizações, dentre várias, destacam-se pelos trabalhos realizados em prol de uma rede mais segura. A seguir, as organizações.

5.1 O Comitê Gestor de Internet no Brasil

Criado em 31 de maio de 1995 através da Portaria Interministerial nº 147, o Comitê Gestor Internet do Brasil tem a função de efetivar a participação da sociedade civil nas decisões que competem à implantação, administração e fruição da internet. É composto por 21 membros, sendo 9 do governo e os demais 12 da sociedade civil.

- **Nove representantes do Governo Federal**
    - Ministério da Ciência, Tecnologia e Inovação;
    - Ministério das Comunicações;
    - Casa Civil da Presidência da República;
    - Ministério da Defesa;
    - Ministério do Desenvolvimento, Indústria e Comércio Exterior;
    - Ministério do Planejamento, Orçamento e Gestão;
    - Agência Nacional de Telecomunicações;
    - Conselho Nacional de Desenvolvimento Científico e Tecnológico;
    - Conselho Nacional dos Secretários Estaduais para Assuntos de Ciência, Tecnologia e Informação - CONSECTI.

- **Quatro representantes do setor empresarial**
    - Provedores de acesso e conteúdo;

- Provedores de infraestrutura de telecomunicações;
- Indústria de bens de informática, telecomunicações e software;
- Segmento das empresas usuárias da Internet.

- **Quatro representantes do terceiro setor**
- **Três representantes da comunidade científica e tecnológica**
- **Um representante de notório saber em assuntos de Internet**

Suas atribuições estão definidas no Decreto nº 4.829, de 3 de setembro de 2003, dentre as quais podemos destacar:

- A proposição de normas e procedimentos relativos à regulamentação das atividades na internet;
- A recomendação de padrões e procedimentos técnicos operacionais para a internet no Brasil;
- O estabelecimento de diretrizes estratégicas relacionadas ao uso e desenvolvimento da internet no Brasil;
- A promoção de estudos e padrões técnicos para a segurança das redes e serviços no país;
- A coordenação da atribuição de endereços internet (IP[14]s) e do registro de nomes de domínios usando <.br>;
- A coleta, organização e disseminação de informações sobre os serviços internet, incluindo indicadores e estatísticas.

A história do Comitê Gestor remete ao período em que a Internet ainda era pouco difundida no Brasil, não havendo muitos milhares de domínios de Internet registrados.

Hoje, em parceria com o Centro de Tecnologia e Sociedade da Escola de Direito da Fundação Getúlio Vargas, no Rio de Janeiro (CTS/FGV), foi criado o Observatório Brasileiro de Políticas Digitais – ou Observatório da Internet Brasileira, como ficou conhecido.

O Comitê Gestor da Internet no Brasil (CGI.br) foi criado com o objetivo de coordenar e integrar todas as iniciativas que remetem ao uso e fornecimento de serviços via Internet, no

[14] Os números de IP, ou *Internet Protocol*, é formado por quatro octetos, uma série de números que vão de 0 a 255, abrangendo o formato xxx.xxx.xxx.xxx. É através do número de IP que computadores, páginas na Internet, bancos de dados, servidores (internos e externos) recebem um número único de identificação e possam ser encontrados na rede. O IP divide-se em duas partes: o sufixo, que identifica a rede física em que o dispositivo está conectado, e o sufixo, que o identifica de forma única nesta rede.

país. O CGI.br promove a qualidade técnica, inovação e disseminação dos serviços ofertados via Internet, baseando-se em princípios de multilateralidade, transparência e democracia, efetivando-se como um órgão-modelo de governança, participação e administração da Internet no Brasil.

Em 2009, o CGI desenvolveu uma série intitulada “Os princípios para uso e governança da Internet no Brasil”. Publicado como a resolução CGI.br/RES/2009/003/P, estes princípios tornaram-se o norte para o desenvolvimento da Internet que buscamos. São eles:

1) **Liberdade, privacidade e direitos humanos:** o uso da Internet deve reconhecer estes princípios como fundamentais para a preservação de uma rede de informações e de uma sociedade justas e democráticas;
2) **Governança democrática e participativa:** a governança da Internet deve ser feita de maneira justa, de forma transparente, multilateral e democrática. Deve, também, contar com a participação dos vários setores da sociedade;
3) **Universalidade:** o acesso à Internet deve ser universal, de maneira que resulte em um meio de desenvolvimento social e humano. Deve contribuir, também, para a construção de uma sociedade inclusiva;
4) **Diversidade:** a diversidade cultural deve ser respeitada e preservada e sua expressão deve ser estimulada, sem a imposição de crenças, costumes ou valores;
5) **Inovação:** a governança da Internet deve promover a inovação e difusão de novas tecnologias e modelos de uso e acesso da Internet;
6) **Neutralidade da rede:** filtragem ou privilégios de tráfego devem respeitar apenas critérios técnicos e éticos, não sendo admissíveis motivos políticos, comerciais, religiosos, culturais, ou qualquer outra forma de discriminação ou favorecimento.
7) **Inimputabilidade da rede:** o combate a ilícitos na rede deve atingir os responsáveis finais e não os meios de acesso e transporte, sempre preservando os princípios maiores de defesa da liberdade, da privacidade e do respeito aos direitos humanos.
8) **Funcionalidade, segurança e estabilidade:** a estabilidade, a segurança e a funcionalidade globais da rede devem ser preservadas de forma ativa através de medidas técnicas compatíveis com os padrões internacionais e estímulo ao uso das boas práticas.
9) **Padronização e interoperabilidade:** a Internet deve basear-se em padrões abertos que permitam a interoperabilidade e a participação de todos em seu desenvolvimento.

10) **Ambiente legal e regulatório:** o ambiente legal e regulatório deve preservar a dinâmica da Internet como espaço de colaboração. O CGi.br atua diretamente na regulamentação da Internet no Brasil. Além disso, trabalha com a questão da segurança

O CGI.br traz, dentro daquilo que lhe compete, recomendações voltadas especificamente para temas cuja relevância para o desenvolvimento e operação da Internet no país estejam pontuados. Assim, busca estabelecer maior segurança e desempenho na rede.

O Comitê Gestor da Internet detectou que, em decorrência de uma série de ataques dirigidos ao usuário final, havia a necessidade de se criar um manual de prevenção ao usuário da rede.

Uma vez que os prejuízos gerados por ciberataques atingem diversas camadas, conforme citado anteriormente, o CGI.br passou a solicitar, por parte dos provedores, que as condições mínimas de proteção do usuário enquanto o mesmo navega, fossem garantidas.

De acordo com o Cetic.br, “com o uso crescente da Internet e das redes sociais, impulsionado principalmente pela popularização dos dispositivos móveis e facilidades de conexão, constatou-se a necessidade de abordar novos conteúdos e agrupar os assuntos de maneira diferente”. Nasce, assim, a Cartilha de Segurança para Internet, visando disseminar a questão da segurança para navegação.

Composta por 14 capítulos, a Cartilha aborda temas variados. Dividida em três partes, estrutura-se da seguinte maneira: o Capítulo 1 apresenta uma introdução sobre a importância de uso da Internet, os riscos a que os usuários estão sujeitos e os cuidados a serem tomados. Do Capítulo 2 ao 6 os riscos são apresentados de forma mais detalhada, enquanto do Capítulo 7 ao 14 o foco principal são os cuidados a serem tomados e os mecanismos de segurança existentes.

A Cartilha é formulada em linguagem clara e objetiva, trazendo ao usuário uma série de explicações sobre como o usuário deve se prevenir de um ciberataques. Estruturada em temas específicos, a Cartilha trata dos seguintes temas:

1) Segurança na Internet;
2) Golpes na Internet;
3) Ataques na Internet;
4) Códigos Maliciosos;
5) Spam;

6) Outros riscos (como Cookies, Códigos Móveis, Pop Ups, entre outros);
7) Mecanismos de Segurança;
8) Contas e senhas;
9) Criptografia;
10) Uso Seguro da Internet;
11) Privacidade;
12) Segurança de Computadores;
13) Segurança de Redes; e
14) Segurança em Dispositivos Móveis.

Além da Cartilha, o Comitê Gestor da Internet desenvolve uma série de ações voltada para a criação de uma Internet mais justa, equânime, neutra e segura. A coleta, organização e disseminação de informações sobre os serviços internet, incluindo indicadores e estatísticas.

O Comitê divide-se, ainda, em vários grupos de pesquisa, voltados para estudos de temas e áreas diversas – áreas, estas, de importância fundamental para o funcionamento e o desenvolvimento da internet no país. Para executar suas atividades, o CGI.br criou uma entidade civil, sem fins lucrativos, denominada "Núcleo de Informação e Coordenação do Ponto BR" - NIC.br.

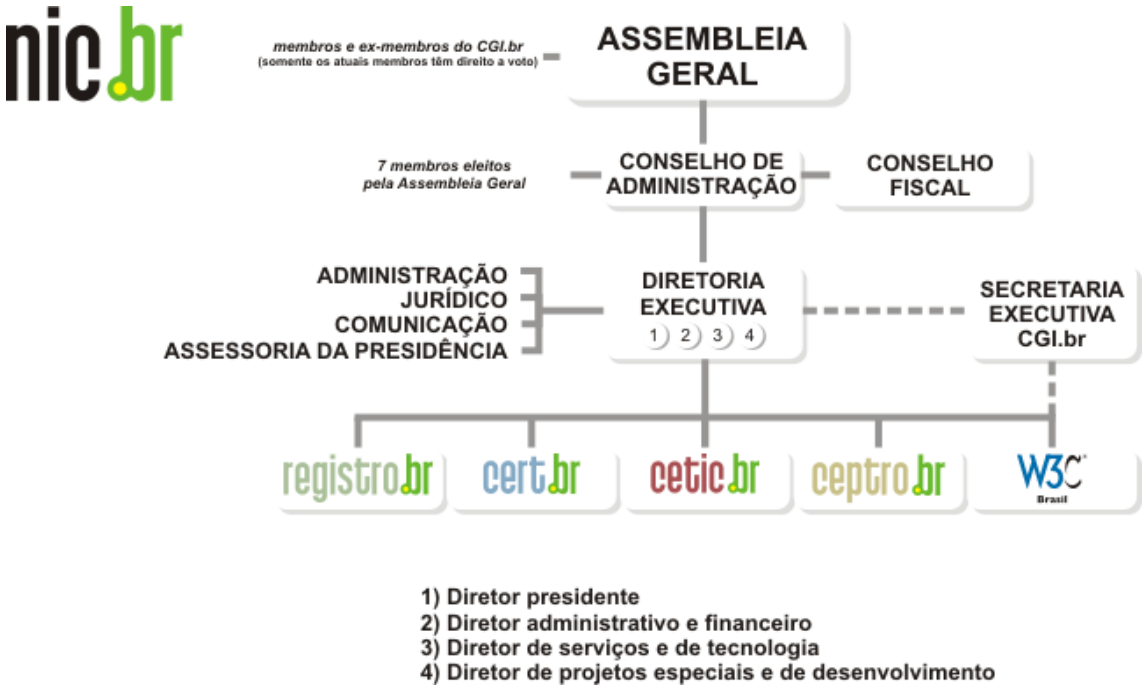
O Núcleo de Informação e Coordenação do Ponto BR (ou NIC.br) foi criado para implementar as decisões e os projetos do CGI.br, responsável por coordenar e integrar as iniciativas e serviços da Internet no País.

O NIC.br é considerado o braço executivo do CGI.br. Dentre suas atribuições estão:

- Realizar o registro e manutenção dos nomes de domínios que usam o <.br>, e a distribuição de números de Sistema Autônomo (ASN) e endereços IPv4 e IPv6 no País, via Registro.br;
- Realizar o tratamento e resposta a incidentes de segurança em computadores envolvendo redes conectadas à Internet no Brasil, via CERT. br;
- Desenvolver projetos que apoiem ou aperfeiçoem a infraestrutura de redes no País, como a interconexão direta entre redes (PTT.br) e a distribuição da Hora Legal brasileira (NTP.br) – destaca para o CEPTRO.br, responsável por estes projetos;

- Realizar a produção e divulgação de indicadores, estatísticas e informações estratégicas sobre o desenvolvimento da Internet no Brasil, sob responsabilidade do CETIC.br;
- Promover estudos e recomendar procedimentos, normas e padrões técnicos e operacionais, para a segurança das redes e serviços de Internet, bem assim para a sua crescente e adequada utilização pela sociedade.
- Realizar o suporte técnico e operacional ao LACNIC, Registro de Endereços da Internet para a América Latina e Caribe.
- Hospedar o Escritório brasileiro do W3C, que tem como principal atribuição desenvolver padrões para Web.

O NIC.br é composto por quatros Centros, quatro grandes Assessorias e, ainda, o escritório brasileiro do W3C, conforme segue:



Fonte: NIC.br

Compõem o NIC.br, ainda, uma série de serviços ligados à Diretoria Executiva e à Secretaria Executiva (no caso do W3C[15]). São eles:

[15] O World Wide Web Consortium (W3C) é a principal organização de padronização da World Wide Web. É um consórcio internacional com quase 400 membros[1] , agrega empresas, órgãos governamentais e organizações independentes com a finalidade de estabelecer padrões para a criação e a interpretação de conteúdos para a Web.

- **REGISTRO.br:** O Registro.br é órgão responsável por, dentre outras funções, registrar os nomes de domínios, administração e publicação do DNS[16] para o domínio
;
- **CERT.br:** o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, CERT.br, realiza atividades de apoio aos administradores de redes e usuários de internet no país. Um dos destaques do CERT.br é a produção de documentos sobre segurança de redes, manutenção de estatísticas sobre spam, entre outras. Atua, ainda, na conscientização sobre problemas de segurança em âmbito virtual e auxilia;
- **CETIC.br:** o Centro de Estudos sobre as Tecnologias da Informação e da Comunicação é responsável por produzir indicadores e estatísticas sobre o uso da Internet e sua disponibilidade em âmbito nacional. Divulga informações periódicas sobre o avanço da rede no Brasil e, através dos dados obtidos, monitora e avalia o impacto socioeconômico das Tecnologias de Informação e Comunicação no país.
- **CEPTRO.br:** o Centro de Estudos e Pesquisas em Tecnologia de Redes e Operações é o órgão responsável por gerir projetos que estimulem a melhora da qualidade da Internet no país, disseminando seu uso. Seu foco é voltado para gerenciar aspectos técnicos e a infraestrutura destes projetos.
- **W3C:** O W3C é um Consórcio internacional que envolve mais de 400 organizações, em todo o mundo. O objetivo do W3C é conduzir a Internet ao seu potencial máximo, desenvolvendo padrões e normas que promovam a evolução constante da rede.

O Comitê Gestor da Internet no Brasil é, hoje, o órgão responsável por coordenar e integrar todas as atividades referentes ao uso da Internet no Brasil, atuando através do NIC.br. Através dos 10 Princípios de Governança, o Comitê Gestor visa a garantia dos direitos fundamentais do usuário no âmbito da rede, considerado um avanço quando comparado à outros países[17].

---

[16] O DNS, do inglês Domain Name System (Sistema de Nomes de Domínios), funciona como um sistema de tradução de endereços IP para nomes de domínios. O sistema de distribuição de nomes de domínio foi introduzido em 1984, e com ele, os nomes de *hosts* (hospedeiro, em português, direciona um arquivo a um endereço de IP) residentes em um banco de dados pode ser distribuído entre servidores múltiplos.

[17] Segundo Tim Berners-Lee, criador da web, "muitos países estão fazendo esforços em prol da neutralidade da rede, mas o Brasil lidera com o Marco Civil, porque olha a questão pelo ângulo correto, que é o dos direitos humanos", o que o coloca em "posição de liderança mundial" quando comparado aos demais países. (FONTE: Marco Civil: Apoio é o que não falta. Novembro de 2013. Disponível em: http://www.cgi.br/publicacoes/revista/edicao05/cgibr-revistabr-ed5.pdf)

Em decorrência da falta de leis sobre a proteção de dados pessoais no Brasil, a questão do investimento, segundo especialistas, também sofreu retaliação, uma vez que *data centers*[18] só trocam informações com *data centers* que estejam localizados em países com altíssimo nível nos padrões de segurança de dados.

Além de regular, o CGI.br adota estratégias de conscientização e disseminação de informações sobre segurança na rede que vão além da Cartilha de Segurança, por exemplo. Adotando mídias de divulgação como vídeos, apresentações, minifilmes, entrevistas, entre outros, o Comitê Gestor da Internet no Brasil desenvolve maneiras de trabalhar o processo de informação, prevenção e combate aos cibercrimes e à proteção de dados na rede.

Um outro órgão que também trabalha na prevenção e combate aos delitos cometidos no mundo virtual é a Safernet; mas ao contrário do CGi.br, a Safernet foi fundada através da organização da sociedade civil, que também verificou a necessidade de combater os crimes virtuais.

5.2 A SAFERNET

Fundada em 20 de dezembro de 2005, a SaferNet é uma organização de origem civil de direito privado, voltada para o desenvolvimento de políticas de prevenção e combate aos cibercrimes.

Buscando, através de parcerias com organizações públicas, criar um ambiente virtual que seja mais seguro para a população, conta com órgãos parceiros como o Ministério Público da União e as Delegacias especializadas em crimes eletrônicos (no estado de São Paulo, destaca-se a DIG, vinculada ao DEIC[19]) para a promoção da justiça, do combate e da prevenção aos delitos cometidos em âmbito virtual.

---

[18] Data center = central de dados.

[19] Visando combater estes tipos de crimes, a 4ª Delegacia de Delitos Cometidos por Meios Eletrônicos trabalha com a resolução de crimes virtuais e o estabelecimento de investigações sobre crimes que usam, de maneira direta ou não, a internet. A 4ª Delegacia de Delitos Cometidos por Meios Eletrônicos (DIG/DEIC). Foi implantada, em 2001, a 4ª Delegacia de Delitos Cometidos por Meios Eletrônicos do Deic (Departamento de Investigação sobre o Crime Organizado; os delitos, que vão desde crimes de difamação até casos mais graves como extorsão e roubo. O DEIC é a unidade da Polícia Civil responsável pela investigação e combate aos grupos criminosos que atuam no estado de São Paulo, visando diminuir seu impacto na sociedade. É estruturado em campos específicos de atuação – tendo a DIG um campo específico de ação. A DIG estrutura-se em 4 Delegacias, cada uma com atribuições específicas. São elas:

- 1ª Delegacia – Antipirataria: prevenir e reprimir crimes contra a propriedade imaterial;
- 2ª Delegacia - Fé Pública: investiga crimes que envolvem falsificações de documentos;
- 3ª Delegacia – Estelionato: investiga grupos especializados em golpes contra pessoas e empresas;
- 4ª Delegacia - Delitos praticados por Meios Eletrônicos: investigar e adotar providências destinadas à apuração da responsabilidade criminal pelo uso indevido de computadores, da internet e de meios eletrônicos.

A SaferNet atua em nível nacional, sendo uma organização sem fins lucrativos ou econômicos. Fundada por um grupo de cientistas da computação, professores, pesquisadores e bacharéis em Direito, a Safernet surgiu como a consolidação de pesquisas e projetos sociais, com ênfase no combate à pornografia infantil.

Consolidando-se como uma das entidades de referência nacional no que tange ao enfrentamento dos crimes e violações dos Direitos Humanos na Internet, a organização tem se fortalecido e ganhado espaço em âmbito nacional e internacional, graças à facilidade de articulação, mobilização, produção de conteúdo e aplicação e uso de novas tecnologias voltadas para o enfrentamento e resolução de crimes cibernéticos.

Conduz ações para viabilizar, de maneira compartilhada, a gestão da Internet em um âmbito ético, responsável, e que permita o desenvolvimento e ampliação de suas relações sociais de maneira segura[20], organizando-se em um órgão central e três grandes eixos: Assembleia Geral, composta pelos Conselhos Consultivo, Fiscal e Administrativo.

A SaferNet tem como missão “promover o uso seguro das Tecnologias da Informação e Comunicação, e criar as condições necessárias para garantir a efetiva proteção dos Direitos Humanos na Sociedade da Informação, contribuindo para uma cultura de responsabilidade e habilitando crianças, jovens e adultos para construírem relações sociais saudáveis e seguras através do uso adequado das tecnologias” – princípios defendidos pelo Comitê Gestor da Internet, através do Marco Civil.

Objetivando desenvolver metodologias que remetam à defesa, orientação e proteção dos Direitos Humanos – com destaque para os direitos das Crianças e dos Adolescentes – a SaferNet faz uso do desenvolvimento de documentação, ferramentas e aplicações de softwares, pesquisas científicas e desenvolvimento de tecnologias alternativas e computacionais.

Dentro da área científica, a SaferNet destaca-se na organização e participação de congressos, seminários, cursos, simpósios e conferências sobre o assunto, buscando a promoção de intercâmbios técnicos, culturais e científicos, em parceria com outras organizações, nacionais e estrangeiras.

Assim como pressuposto na CF/88, a SaferNet também presa pelos princípios da legalidade, impessoalidade, moralidade, publicidade, economicidade e eficiência para guiar as suas ações. Para tal, a organização também atua, de forma direta ou indireta, na execução de projetos, programas e planos de ações; na doação de recursos físicos, humanos e

[20] Este é um dos principais objetivos da organização.

financeiros, e até mesmo na prestação de serviços intermediários de apoio a outros ONGs, organizações privadas e organizações públicas.

A SaferNet também lançou a Central Nacional de Denúncias de Crimes Cibernéticos (CNDC), única na América Latina. Em média, recebe 2.500 denúncias por dia, envolvendo desde páginas da Internet com evidências de crimes de Pornografia Infantil ou Pedofilia a Racismo, Xenofobia, maus tratos aos animais, incitação a crimes contra a vida, entre outros.

Para a criação da CNDC, foi necessário desenvolver um sistema de gestão de denúncias, automatizado e baseado em Software Livre[21], o que permite ao usuário acompanhar o andamento das denúncias em tempo real, mas a CNDC também permite a realização de denúncias anônimas – do total de denúncias recebidas, 99% dos internautas optam por fazer a denúncia de maneira anônima, mas aos 1% restantes, o anonimato é garantido.

A CNDC é um esforço de corresponder aos esforços internacionais da rede INHOPE, composta, atualmente, por 22 países que trabalham para coibir o uso indevido da internet. Para realizar uma denúncia através da SaferNet.

Para realizar uma denúncia, o usuário deve:

1) Na página da SaferNet há uma aba voltada exclusivamente para a realização de **Denúncia** (Denunciar Crimes na Web – tela 1).
2) O usuário deve clicar neste ícone e, dentre os crimes tipificados pela organização (Crimes Contra os Direitos Humanos na Internet? Denuncie! – tela 2) selecionar aquele em que a denúncia se enquadra e enviar o link do site, gerando um protocolo de denúncia (tela 3).
3) As denúncias podem ser realizadas anonimamente.

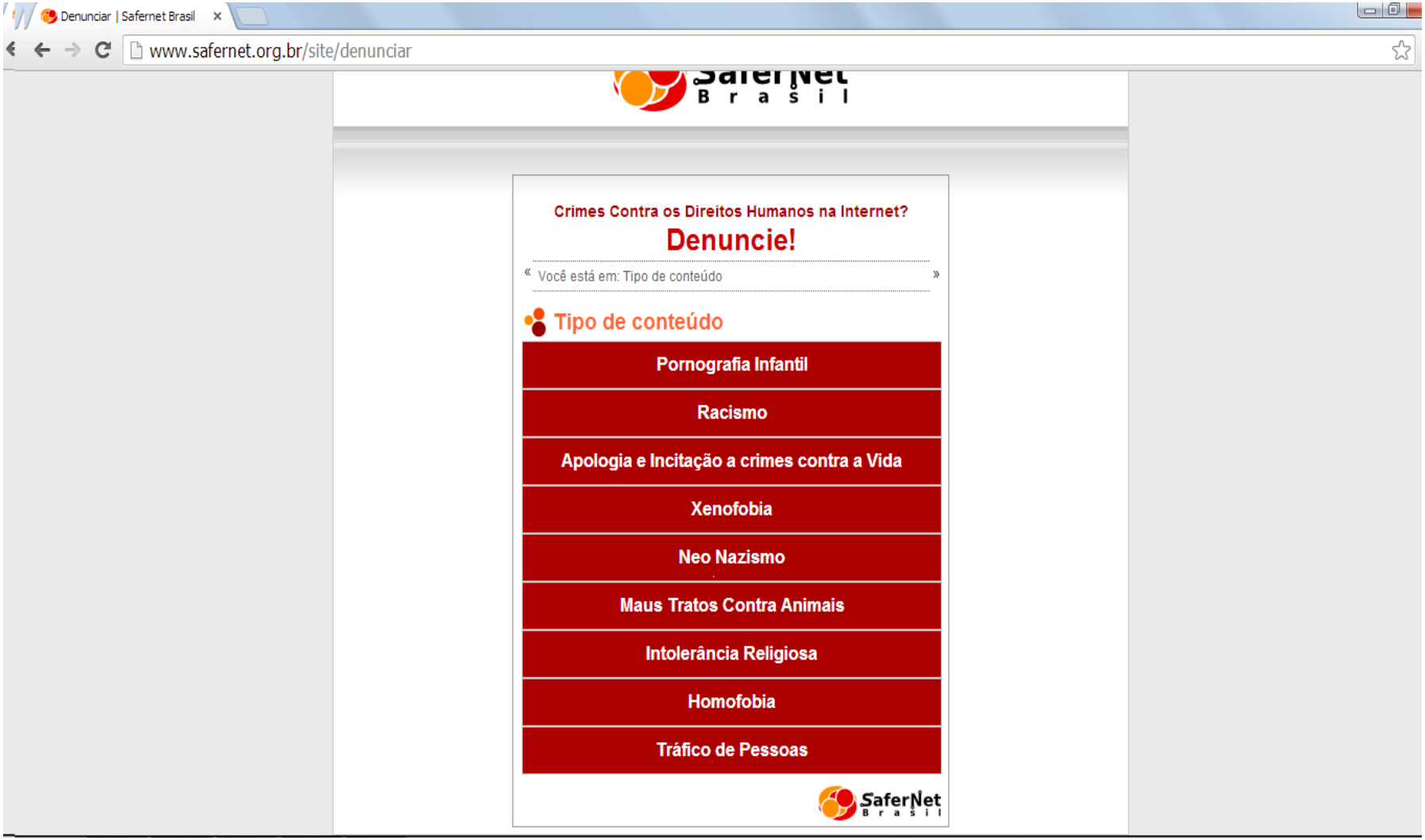
[21] A SaferNet Brasil adotou para si a ideologia da rede de Software Livre, cujo foco principal é a garantia dos direitos do usuário para executar, distribuir, repassar e modificar alterações. Ao fazer uso de um Software Livre, o usuário tem assegurado sobre si, 4 tipos de liberdades – são elas:

1) Liberdade de execução do programa, para qualquer propósito;
2) Liberdade de estudar o funcionamento do programa e de adaptá-lo, se necessário, às suas necessidades;
3) Liberdade para redistribuir cópias, beneficiando o próximo;
4) A liberdade de aperfeiçoar o programa, e liberar os seus aperfeiçoamentos, de modo que toda a comunidade se beneficie.

Tela 1


Safernet Brasil | Protegendo
www.safernet.org.br/site/
SaferNet Brasil
Quem somos
Indicadores
Colaborar
Prevenção
Orientação
Denuncie
Buscar neste site:
Buscar
SaferNet Brasil
Prevenir & Educar
Denunciar Crimes na Web
Obter Ajuda e Orientação
Acompanhamento de Denúncia
Código da denúncia:
Verificar Andamento »
Notícias
Para Jornalistas
Releases
Nacionais
Internacionais
20/12/2013 Boletim Nº 16: Edição Dia da Internet Segura 2014
12/12/2013 SAFERNET BRASIL VENCE PRÊMIO DE DIREITOS HUMANOS
16/10/2013 Com auditório lotado, jornada discutiu desafios da educação para a cidadania na Internet
16/10/2013 Com auditório lotado, jornada discutiu desafios da educação para a cidadania na Internet
Ver Todos
1 de 42 »
Vídeos
Debate do Dia da Internet Segura 2013
SaferNet Brasil - 22/02/2013
Dia da Internet Segura
Debate via Hangout entre Maria do Rosário (ministra da Secretaria de Direitos Humanos da Presidência da República), Marcelo Tas (jornalista e comunicador de TV) e Jean Wyllys (deputado federal).
Debate on-line com Jean Wyllys, Marcelo Tas e ministra dos direitos humanos Maria do Rosário marca Dia Mundial da Internet Segura
Mais Vídeos

Tela 2


Denunciar | Safernet Brasil
www.safernet.org.br/site/denunciar
Crimes Contra os Direitos Humanos na Internet?
Denuncie!
« Você está em: Tipo de conteúdo »
Tipo de conteúdo
Pornografia Infantil
Racismo
Apologia e Incitação a crimes contra a Vida
Xenofobia
Neo Nazismo
Maus Tratos Contra Animais
Intolerância Religiosa
Homofobia
Tráfico de Pessoas

Tela 3

4) A segunda etapa é a **Análise de Conteúdo**, que fica a cargo de uma equipe de especialistas da SaferNet. Após a verificação de que, de fato a denúncia é válida, a mesma seguirá para uma próxima fase, em que os analistas da SaferNet constataram indício de crime contra os Direitos Humanos e cuja ação penal seja pública e incondicionada à representação, ou seja, quando a vítima é a sociedade em si, não apenas um de seus membros. Isso exclui do âmbito de ação da SaferNet crimes como ameaça, difamação, falsa identidade etc.

5) Após comprovar que há indícios de crimes, as informações pertinentes – e que estão disponíveis publicamente na rede – são levantadas, objetivando a **comprovação da materialidade** e a documentação dos indícios de autoria.

6) Após estes passos, a equipe de especialistas da SaferNet **elabora um relatório** de rastreamento, baseado na legislação penal e processual penal vigente.

7) Se as denúncias contiverem evidências relacionadas a sites hospedados em âmbito nacional, o relatório é enviado às autoridades para que se inicie a investigação criminal (**Polícia Federal e Ministério Público Federal**). Denúncias estrangeiras são encaminhadas aos Canais de Denúncias Internacionais.

Além deste tipo de atuação, a SaferNet também trabalha nas áreas de **Prevenção e Educação** e **Obter Ajuda e Orientação** aos internautas. A primeira trabalha crianças, adolescentes, adultos e idosos através de Cartilhas, Recursos (área voltada para educadores, trabalha a prevenção e educação através de vídeos,

quadrinhos, cartilhas, notícias, entre outros), Quadrinhos, Jogos, entre outros (há publicações voltadas exclusivamente para Adolescentes e Educadores).

Já a segunda vertente, Obter Ajuda e Orientação, funciona através do **HELPLINE.br**, uma equipe de psicólogos que realizam orientações gratuitas e encontram-se à disposição da população para esclarecer dúvidas, ensinar formas seguras de uso da Internet e, também, para orientar crianças e adolescentes e/ou seus próximos, que sofreram ou vivenciaram algum tipo de violência online, como humilhações, intimidações, chantagem, tentativa de violência sexual ou exposição forçada em fotos ou filmes sensuais. O atendimento é realizado através de e-mail ou chat.

A Central Nacional de Denúncias de Crimes Cibernéticos dispões de uma gama de indicadores que traduzem o cenário dos cibercrimes no Brasil. Em 07 anos, a SaferNet recebeu e processou nada mais nada menos do que 3.173.061 denúncias anônimas, que envolviam 472.840 URLs[22] diferentes, escritos em 9 idiomas diferentes, hospedadas em 52.962 hosts[23] diferentes, conectados à Internet através de 28.131 números de IPs diferentes, relacionados a 90 países diferentes, por todos os continentes.

A seguir, disponibilizamos a relação de denúncias registradas entre janeiro de 2006 e outubro de 2012, conforme veiculação na mídia:

[22] URL (*Uniform Resource Locator),* é o endereço de uma página na rede, seja a rede internet ou intranet. Em português é conhecido por Localizador Padrão de Recursos.
[23] Hosts: hospedeiro, em português, direciona um arquivo a um endereço de IP.

Crimes denunciados no Brasil entre janeiro de 2006 e outubro de 2012	
Pornografia infantil	4.161 denúncias (38,65%)
Racismo	2.349 denúncias (21,8%)
Apologia ao crime	1.691 denúncias (15,7%)
Homofobia	692 denúncias (6,4%)
Intolerância religiosa	625 denúncias (5,8%)
Maus tratos contra animais	353 denúncias (3,27%)
Xenofobia	349 denúncias (3,24%)
Neonazismo	207 denúncias (1,92%)
Tráfico de pessoas	171 denúncias (1,58%)
Não-classificado	167 denúncias (1,55%)

Fonte: G1

A SaferNet desenvolveu, ainda, o Observatório do Legislativo, com o objetivo de coletar, sistematizar e analisar as informações relativas à Câmara dos Deputados e do Senado Federal. Seu objetivo é facilitar a participação ativa e qualificada dos mais variados atores da sociedade civil nas questões relacionadas aos cibercrimes. O Observatório Legislativo se faz um instrumento de disseminação de informações, acompanhamento, avaliação e pesquisa sobre procedimentos legislativos e Projetos de Lei que estão tramitando no Congresso. Este é um dos muitos meios de participação da organização no que compete à prevenção, combate, denúncia e investigação e legislação para os cibercrimes.

A SaferNet possui, ainda, parcerias com diversas organizações, conforme seguem:

1) **Childhood Brasil:** iniciando a parceria em 2007, esta organização deu o suporte necessário à SaferNet quando estava prestes a encerrar suas atividades por falta de recursos financeiros – o apoio da Childhood foi fundamental, resultando na criação da Central de Denúncias de Crimes Cibernéticos. Ao renovar a parceria com a SaferNet, em 2008, a Childhood Brasil aperfeiçoou os softwares utilizados para o recebimento e processamento das denúncias, desenvolvimento e implantação do sistema de indicadores, de

backup, entre outros. Além disso, iniciaram uma série de atividades conjuntas na área da educação. A equipe de prevenção da SaferNet realizou uma série de oficinas para educadores da rede de ensino fundamental de São Paulo, voltadas para a segurança na Internet – o trabalho se estendeu até o ano de 2009.

2) **NIC.br (CGI.br):** firmando um Termo de Cooperação com o NIC.br em julho de 2008, a SaferNet assumiu o compromisso de desenvolver e encaminhar relatórios periódicos com informações sobre o recebimento, processamento e encaminhamento online das denúncias anônimas sobre crimes ou violações praticados na Internet, além da tipificação legal destes delitos cometidos – todos estes dados, resultados das ações adotadas pela SaferNet, para o combate destes crimes. O termo de cooperação assinado pelas organizações prevê, ainda sigilo destas informações, de maneira confidencial, de todos os serviços prestados, com exceção das autoridades competentes, que possuem livre acesso às informações.

3) **Petrobrás:** o contrato foi assinado em dezembro de 2008, após a aprovação do projeto da "Central Nacional de Denúncias de Crimes Cibernéticos: Enfrentamento articulado e prevenção da Pornografia Infantil e Pedofilia na rede Internet no Brasil". A parceria com a Petrobras tem ainda, como objetivo, aumentar o enfrentamento da distribuição de pornografia infantil pela Internet brasileira através do aumento da capacidade de processamento, monitoramento, geração e encaminhamento e notícias-crimes e denúncias ao Ministério Público Federal.

4) **Parceria com o Ministério Público Federal:** o primeiro MPF a assinar um Termo de Mútua Cooperação Técnica, Científica e Operacional com a SaferNet foi o MPF de São Paulo, em 29 de março de 2006. Desde então, a CNDC e o MPF/SP tem unido forças para combater a pornografia, o racismo e outras formas de discriminação cometidas através da rede. Além da assinatura do Termo de Cooperação com o MPF de São Paulo, foram assinados termos com os MPFs do Rio de Janeiro (13/11/06), Rio Grande do Sul (25/10/06), Goiás (12/03/07) e Paraná (14/06/07).

Assim, de acordo com Thiago de Oliveira, diretor da SaferNet Brasil, vale lembrar que além dos “sigilos fiscal, bancário e telefônico, (...) existem outros tipos de sigilos igualmente importantes que devem ser protegidos pela lei”.

A SaferNet se coloca, portanto, como um dos agentes difusores dos Direitos Humanos na Internet, colocando-se como um dos principais atores na promoção destes Direitos e no desenvolvimento de uma rede segura para o usuário. Maior prova disso foi receber o Prêmio de Direitos Humanos 2013, em 12 de dezembro de 2013.

Por ser referência na promoção dos Direitos Humanos na Internet, a ONG SaferNet venceu o Prêmio de Direitos Humanos 2013 na categoria “Educação em Direitos Humanos”. A cerimônia ocorreu no Fórum Mundial de Direitos Humanos, sendo este prêmio considerado o mais importante prêmio concedido pelo Governo Federal brasileiro – daí a importância da SaferNet no campo de prevenção, educação, combate e conscientização dos Direitos dos usuários na rede.

Mencionado anteriormente, mas merecendo um destaque especial, as Cartilhas elaboradas pela organização destacam-se no processo de proteção, conscientização e divulgação dos Direitos Humanos na Internet. A ONG já publicou 12 cartilhas, todas disponíveis para download gratuito. São cartilhas de fácil compreensão, ilustradas e com finalidades diferentes:

1) **Cartilha Helpline –** composta por ilustrações e um Quis, esta cartilha ilustra o papel do *Helpline* BR: ser um canal de atendimento online e gratuito formulado especialmente para sanar dúvidas sobre os perigos na Internet e como é possível ajudar usuários que sofrem algum tipo de violência, chantagem ou discriminação na rede.

2) **Cartilha SaferDic@s 5ª Edição** – a Cartilha SaferDic@s foi desenvolvida pensando no desenvolvimento e promoção do uso ético, responsável e seguro da Internet no Brasil. Foi elaborada com linguagem simples e muitas ilustrações, uma vez que seu público-alvo é grande e passar por todas as faixas etárias.

3) **Cartilha SaferDic@s HQ** – esta Cartilha foi pensada para demonstrar que atividades rotineiras também podem se tornar alvo de problemas no mundo cibernético. As personagens desta cartilha vivem as mais variadas situações na rede, oferecendo dicas ao usuário para que evitem riscos e exerçam suas atividades e cidadania no ciberespaço.

4) **Guia Responsável de Uso da Internet –** Guia de orientação para uso responsável da Internet. Com ilustrações, quadrinhos e muitas dicas, esta Cartilha induz ao leitor a pensar sobre os cuidados a serem adotados na rede.

5) **Bullying Não é brincadeira** – esta cartilha traz explicações, dicas e exemplos de como se prevenir e se defender das situações de *bullying*.

6) **Direitos Humanos do Menino Maluquinho** – esta cartilha, criada pelo Ziraldo em parceria com a Secretaria dos Direitos Humanos da Presidência da República, traz uma discussão divertida, simples e de fácil entendimento sobre os Direitos Humanos.

7) **Segurança em Redes Sociais** – esta cartilha traz dicas e orientações sobre como configurar com segurança e privacidade nas redes sociais, como o Facebook, o Twitter e o Orkut. Esta cartilha traz um tutorial simples, elaborado pelo Centro de Atendimento a Incidentes de Segurança (CAIS), pela Rede Nacional de Pesquisa (RNP), pelo Ministério da Educação e pelo Ministério de Ciência e Tecnologia para o Dia Internacional de Segurança em Informática (DISI).

8) **Navegar com Segurança 2012 –** desenvolvida em parceria com a Childhood, esta cartilha é voltada para todos aqueles que estão próximos, são responsáveis, cuidam ou educam crianças e adolescentes para pensar sobre as oportunidades criadas pela internet e os cuidados necessários para que ela seja usada com ética e segurança.

9) **Guias Ética e Cidadania na escola** – este guia tem por objetivo contribuir para a criação de ambientes éticos no ambiente educativo, traduzindo a educação no que tange à promoção da democracia e justiça no âmbito social.

10) **Plano Nacional de Educação em Direitos Humanos (PNEDH)** – fruto do trabalho do Comitê Nacional de Educação em Direitos Humanos, (Portaria 66 – 12/05/2003), o PNEDH é o estabelecimento de um compromisso do Estado para firmar os Direitos Humanos em prol da construção de uma sociedade civil organizada. O PNEDH traz informações baseadas nos principais documentos internacionais no âmbito dos direitos fundamentais do usuário.

11) **Programa Ética e Cidadania** – em parceria com o MEC, o Programa Ética e Cidadania tem por objetivo incorporar, no dia a dia das salas de aula, os valores éticos, democráticos e de justiça. Através da implementação de Fóruns Escolares de Ética e de Cidadania nas escolas, municípios e estados, o Programa exerce o desenvolvimento da cidadania, respeito, solidariedade e responsabilidade, usando o diálogo como ferramenta necessária para alcançar estes objetivos.

12) **Guia de Referência** – esta Cartilha foi desenvolvida em parceria com a *Childhood* Brasil (Instituto WCF) e a Secretaria Municipal de Educação de São Paulo. Voltada aos educadores da rede municipal, tem por objetivo auxiliar o educador a desempenhar, de forma cada vez melhor, o seu papel no enfrentamento da violência sexual. Para tal, os órgãos parceiros desenvolveram o Projeto Redes de Proteção na Educação.

5.3 Considerações finais sobre o capítulo

O capítulo se debruçou sobre duas organizações brasileiras que possuem um importante papel a desempenhar no uso da internet e no combate ao cibercrime: O Comitê Gestor da Internet (CGI) e a SaferNet. Vimos que a SaferNet possui um amplo escopo de atuação, o que a torna referência na promoção dos Direitos Humanos no âmbito virtual. Seu trabalho também merece destaque nos campos de prevenção, educação e combate aos delitos virtuais, mas seu maior destaque fica por conta da Central de Denúncias.

A Central de Denúncias, a maior Central deste tipo em toda a América Latina, tem papel de destaque na apuração destes delitos, bem como nas etapas de investigação e ação penal, através dos órgãos de competência legais. Assim, a SaferNet se apresenta como atora fundamental na promoção dos direitos do usuário e na promoção de uma Internet mais justa.

Por outro lado, temos a atuação do Comitê Gestor da Internet no Brasil, órgão responsável pela regulamentação da rede em âmbito nacional. Além da regulamentação, o CGI.br desenvolve pesquisas sobre o uso da Internet no Brasil e atua como peça fundamental na promoção de uma internet mais justa e segura, através do Marco Civil da Internet e de seus princípios de governança, garantias, direitos e deveres dos usuários da rede.

O CGI.br promove anualmente, Fóruns para a discussão da Internet no Brasil. São eventos abertos ao público e que permitem a participação da sociedade civil, fazendo uma troca de conhecimentos, opiniões e experiências entre palestrantes e participantes. Assim, o Comitê Gestor coloca-se como um dos atores fundamentais no estabelecimento de uma

Internet segura, e o processo de construção deste cenário, por sua vez, atende os princípios democráticos, uma vez que conta com a sociedade civil para tal finalidade.

CAPÍTULO 6 – CONSIDERAÇÕES FINAIS

Constantemente, é noticiado o aumento dos delitos cometidos através da Internet; delitos, estes, que variam desde fraudes bancárias a ataques às fontes de dados de governos.

Conhecidos como ciberataques ou cibercrimes, tornaram-se cada vez mais frequentes, gerando transtornos e ameaças à democracia, infringindo os direitos fundamentais do cidadão.

A perícia forense computacional[24] tem se mostrado, juntamente com as legislações específicas, importantes ferramentas de prevenção, investigação e combate a estes delitos, porém ainda fica claro que a falta de recursos humanos realmente capacitados é grande.

No Brasil, a maior dificuldade se dá no âmbito penal; embora previstos no Código Penal Brasileiro, as instâncias em que os delitos devem ser julgados geram dúvidas: condena-se através da legislação do local de origem do ataque? Ou da legislação do local em que a vítima sofreu o ataque (se forem de países diferentes, por exemplo).

Um outro empecilho, no âmbito brasileiro, é a falta de uma legislação específica para a Internet – quadro que tem sofrido alterações desde a Proposta do Marco Civil da Internet, a mais significativa, neste sentido.

Em nível global, verificamos que, mesmo com avançadas tecnologias, nem sempre os países estão livres de sofrerem ataques virtuais, e muitas vezes, a origem destes ataques pode ser duvidosa (a exemplo da Red October). Também fica claro que legislações muito rígidas podem acarretar outros tipos de crimes, como os Crimes contra a Vida (como no caso do jovem Aaron Swartz, 26 anos).

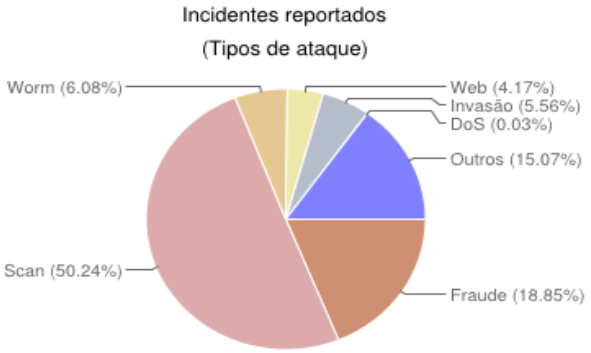
Voltando às questões que incialmente propus, acredito que, após o analisado, o Brasil encontra-se em um patamar mediano no que tange às políticas públicas de combate e prevenção em relação aos ataques virtuais. Embora haja legislação e meios de proteção, o Brasil sofre ataques cibernéticos dos mais variados tipos. Fica claro, conforme os gráficos abaixo (dados obtidos através de informações repassadas à CERT.br) que os maiores tipos

---

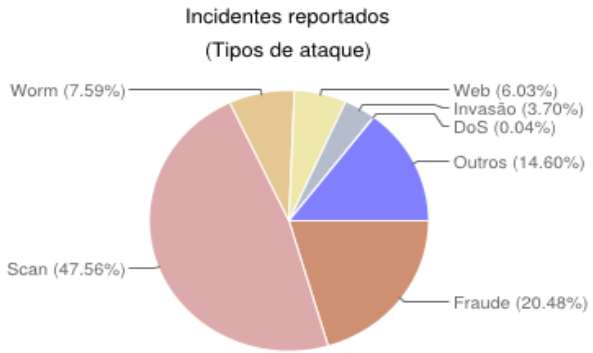
[24] A Perícia Forense Computacional é a ciência responsável por investigar e extrair vestígios eletrônicos em computadores. Embora a segurança na rede e ferramentas de segurança tenham aumentado consideravelmente nos últimos tempos, novas maneiras de se burlar a segurança, graças à complexidade de softwares, redes e sistemas cresceu inúmeras vezes mais. Assim, faz-se necessário maneiras de chegar ao usuário-infrator; nasce a Perícia Forense Computacional. Ela pode ser definida como "a inspeção científica e sistemática em ambientes computacionais, com a finalidade de angariar evidências derivadas de fontes digitais, tendo como objetivo, promover a reconstituição dos eventos encontrados (podendo assim, determinar se o ambiente em análise foi utilizado na realização de atividades ilegais ou não autorizadas)" (PALMER and Corporation, 2001). De acordo com Freitas (2007), a perícia forense baseia-se em quatro evidências principais: i) identificadas, ii) preservadas, iii) analisadas, iv) apresentadas. Quando cometidos através do computador, as evidências de tais crimes normalmente são dados lógicos e virtuais que ficam acondicionados na máquina e na rede; assim, cabe ao perito identificar, de forma correta e aplicável, ao meio em que estas provas se encontram e a melhor e mais correta forma de armazená-las.

de ataques sofridos são os ataques do tipo “Scan”, em que o atacante vasculha dados da vítima em potencial, analisando o seu perfil.

Incidentes Reportados ao CERT.br -- Janeiro a Março de 2013



Incidentes Reportados ao CERT.br -- Abril a Junho de 2013



Incidentes Reportados ao CERT.br -- Julho a Setembro de 2013

Legenda:

- **worm**: notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede.
- **dos** (DoS -- *Denial of Service*): notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.
- **invasão**: um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede.
- **web**: um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet.
- **scan**: notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.
- **fraude**: segundo Houaiss, é "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem.
- **outros**: notificações de incidentes que não se enquadram nas categorias anteriores.

Obs.: Vale lembrar que **não se deve confundir scan com scam**. Scams (com "m") são quaisquer esquemas para enganar um usuário, geralmente, com finalidade de obter vantagens financeiras. Ataques deste tipo são enquadrados na categoria fraude.

Destaca-se, também, a grande incidência de Spams emitidos pelo Brasil. Segundo informações levantadas pela TrenMicro, em 2013, 38% do e-mails maliciosos eram advindos do Brasil:

Fonte: TrendMicro

Um outro problema identificado no estudo desenvolvido pela TrendMicro é a hospedagem de URLs Maliciosas: o Brasil hospeda 58% destas. Além disso, destaca-se pela quantidade de fraudes bancárias que aqui ocorrem[25].

A organização dos entes federativos para prevenção e combate, por sua vez, se dá através de parcerias entre organizações da sociedade civil, órgãos investigativos federais e poderes locais (estados e municípios), bem como através de Decretos presidenciais, para o combate e prevenção destes delitos. Embora tenham sido abordadas neste trabalho a SaferNet e o Comitê Gestor da Internet, muitas outras organizações atuam em âmbito de prevenção, investigação e combate (como, por exemplo, as Delegacias Especializadas, a própria TrendMicro, entre outras).

[25] Na Cúpula de Segurança do Setor Financeiro (Fórum Econômico Mundial), realizada em junho de 2013, as instituições bancárias brasileiras observaram o aumento exponencial das fraudes online no primeiro trimestre de 2013.

Por último, as políticas públicas desenvolvidas para esta área são frutos destas articulações. Aqui foram citados inúmeros Projetos de Lei – com destaque para o PL 2.793/2011, de autoria do Deputado Eduardo Teixeira, e o próprio Marco Civil da Internet, de coautoria deste mesmo deputado. Além disso, campanhas para combate e prevenção aos cibercrimes ocorrem através de vídeos, propagandas, cartilhas, jogos, Fóruns, entre outras formas de divulgação.

Fica claro que, quando comparados a outros países, o Brasil ainda está em processo de crescimento, aperfeiçoamento e captação de especialistas para a área. Embora o país tenha evoluído grandemente, há muito o que se construir. Talvez, o primeiro passo para a garantia dos Direitos Humanos e, por consequência, a proteção do usuário da rede, seja a aprovação do Marco Civil da Internet – defendido, internacionalmente, como um modelo a ser adotado em âmbito internacional, pois aborda os direitos do usuário.

BIBLIOGRAFIA

ADACHI, T. **312 – Gestão de Segurança de *Internet Banking* por meio de camadas**. Trabalho apresentado nos Anais do Congresso Anual de Tecnologia da Informação – CATI 2004 – FGV-EAESP. São Paulo, 2004.

AGÊNCIA BRASIL E SENADO FEDERAL. **Leis que garantem punição para crimes na internet são sancionadas**. Publicado em 04 de dezembro de 2012 e acessado em 01 de fevereiro de 2013. Disponível em: http://www.brasil.gov.br/noticias/arquivos/2012/12/04/leis-que-garantem-punicao-para-crimes-na-internet-sao-sancionadas

ANDRADE, W. A. **Crimes na Internet: uma Realidade na Sociedade de Informação**. Presidente Prudente, 2006. Disponível em: http://intertemas.unitoledo.br/revista/index.php/Juridica/article/view/486/480. Acessado em 20 de fevereiro de 2013

Ataque cibernético denominado "Red October" comprometeu sistemas de mais de 40 países desde de 2007. Publicado em 15 de janeiro de 2013. Acessado em 15 de fevereiro de 2013. Disponível em: http://mariano.delegadodepolicia.com/tag/cybercrime/

CERT.br. **Cartilha de Segurança para Internet.** Disponível em: http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf. Publicado em 2012. Acessado em 20 de dezembro de 2013.

Comitê Gestor da Internet no Brasil **Quem somos**. Disponível em http://www.cgi.br/sobre-cg/definicao.htm. Acessado em 03 de fevereiro de 2013.

Convenção sobre o cibercrime. Budapeste, 23 de novembro de 2011. Disponível em: http://www.coe.int/t/dghl/standardsetting/t-cy/ETS_185_Portugese.pdf. Acessado em 01 de abril de 2013.

Como o F.B.I. investiga os crimes praticados por meios eletrônicos. Publicado em 18 de janeiro de 2010. Acessado em 09 de fevereiro de 2013. Disponível em: http://mariano.delegadodepolicia.com/como-o-f-b-i-investiga-os-crimes-praticados-por-meios-eletronicos/

Council of Europe. **Convention on Cybercrime CETS No.: 185. Disponível em:** http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=9/2/2006&CL=ENG. Acessado em 21 de novembro de 2013.

CUNHA, M. A.V. C. da; **Administração dos Recursos de Informática Pública: Estudo de Caso do Modelo Paranaense.** Publicado em 1994 para obtenção do título de Mestre em Administração. Fundação Getúlio Vargas. São Paulo.

Delegado gaúcho troca experiências com policial italiano sobre cibercrimes. Disponível em: http://www.internetlegal.com.br/2010/01/delegado-gaucho-troca-experiencias-com-policial-italiano-sobre-cibercrimes/ Acessado em 14 de novembro de 2013.

Departamento de Investigações sobre Crime Organizado. Acessado em 26 de abril de 2012. Disponível em: http://www2.policiacivil.sp.gov.br/x2016/modules/mastop_publish/?tac=DEIC Sem data.

Descoberto vírus "que roubava documentos desde 2007" Disponível em: http://www.bbc.co.uk/portuguese/noticias/2013/01/130115_malware_red_october_rw.shtml. Atualizado em 15 de janeiro de 2013. Acessado em 01 de novembro de 2013.

DIAS, V. M. **A problemática da investigação do cibercrime**. Lisboa, novembro de 2010. Disponível em: http://www.verbojuridico.com/doutrina/2011/veradias_investigacaocibercrime.pdf

DINIZ, V., **A história do uso da tecnologia da informação na gestão pública brasileira através do CONIP – Congresso de Informática Pública.** Apresentado no X Congreso Internacional del CLAD sobre la Reforma del Estado y de la Administración Pública, Santiago, Chile, 18 - 21 Oct. 2005. Disponível em: https://attachment.fbsbx.com/file_download.php?id=435484769868394&eid=ASvrZiSIBURuUK5qrm6inlYNzDdBuugIxrTY06wOJh-f5tl9kOGs5sYGZCGvLhXd-1A&inline=1&ext=1368061319&hash=ASufM-r-8yX4GAOz e acessado em 10 de maio de 2013.

Diretor da Safernet diz que sigilo de dados pessoais ganhou importância com internet. Publicado em 02 de outubro de 2013. Disponível em: http://www2.camara.leg.br/camaranoticias/noticias/SEGURANCA/453576-DIRETOR-DA-SAFERNET-DIZ-QUE-SIGILO-DE-DADOS-PESSOAIS-GANHOU-IMPORTANCIA-COM-INTERNET.html. Acessado em 01 de janeiro de 2014.

EMBAIXADA AMERICANA - **Missão diplomática dos EUA no Brasil.** Disponível em: http://portuguese.brazil.usembassy.gov/pt/privacy2.html s/d. Acessado em 10 de fevereiro de 2013.

Entenda o Sopa e o Pipa, projetos de lei que motivam protestos de sites. 18 de janeiro de 2012. Acessado em 09 de fevereiro de 2013. Disponível em: http://g1.globo.com/tecnologia/noticia/2012/01/entenda-o-projeto-de-lei-dos-eua-que-motiva-protestos-de-sites.html

EUA: Senadora quer mudança em lei de fraude na internet após suicídio de Swartz. Publicado em 16 de janeiro de 2013. Acessado em 09 de fevereiro de 2013. Disponível em: http://canaltech.com.br/noticia/internet/Senadora-determina-mudanca-em-lei-de-fraude-na-internet-apos-a-morte-de-Swartz/#ixzz2KRRPyUet

FLORO, P. **Lei de crimes virtuais é o primeiro passo para legislação da web brasileira**. Publicado em 03 de fevereiro de 2013 e acessado na mesma data. Disponível em: http://blogs.ne10.uol.com.br/mundobit/2013/02/03/lei-de-crimes-virtuais-e-primeiro-passo-para-legislacao-da-web-brasileira/

FREITAS, *in* TOLENTINO, L., SILVA, W., e MELLO, P. A. M. S. **Perícia Forense Computacional.** Revista Tecnologias em Projeção, n. 2, v.2, p. 26-31. Brasília : Faculdade Projeção, 2011.

Fundação Getúlio Vargas. Centro de Tecnologia e Sociedade da Escola de Direito do Rio de Janeiro. **Relatório de políticas de Internet: Brasil 2011**. -- São Paulo : Comitê Gestor da Internet no Brasil, 2012.

G1. **Safernet lança site que reúne denúncias de crimes na internet - Pornografia infantil é crime que tem mais denúncias no Brasil. Domínios do Orkut têm 70% das denúncias entre sites.** São Paulo, 2012. Disponível em: http://g1.globo.com/tecnologia/noticia/2012/11/safernet-lanca-site-que-reune-denuncias-de-crimes-na-internet.html. Acessado em 24 de dezembro de 2013.

História dos computadores no Brasil. Apresentado no I CONIP - Congresso Nacional de Informática Pública, em São Paulo. *In* Museu do Computador – Universidade Estadual de Maringá. Disponível em: http://www.din.uem.br/museu/hist_nobrasil.htm. Acessado em 10 de abril de 2013.

LEMOS, M. **Novo Projeto de Lei vai regulamentar crimes virtuais: PL 2793/11.** Atualizado em 01 de novembro de 2012 e acessado em 01 de fevereiro de 2013. Disponível em: http://www.ferramentasblog.com/2012/05/novo-projeto-de-lei-regulamentar-crimes-virtuais-pl-2793-11.html

LOPES, V. PARNAÍBA, G. **Crimes cibernéticos disparam em BH**. Publicado em 03 de outubro de 2011. Acessado em 07 de março de 2013. Disponível em: http://www.em.com.br/app/noticia/gerais/2011/10/03/interna_gerais,253789/crimes-ciberneticos-disparam-em-bh.shtml

MAYUMI, B. **Delegacia de crimes eletrônicos registra mais de 270 casos este ano.** Publicado em 09 de setembro de 2007. Acessado em 08 de março de 2011. Disponível em: http://www.saopaulo.sp.gov.br/spnoticias/lenoticia.php?id=87572

MEDEIROS, E. **Rede de espionagem roubou dados em 70 países.** Publicado em 15 de janeiro de 2013. Acessado em 04 de setembro de 2013. Disponível em: http://jornalggn.com.br/blog/luisnassif/rede-de-espionagem-roubou-dados-em-70-paises

MINISTÉRIO DA JUSTIÇA (Portugal). **Ao Encontro dos Desafios do Cibercrime: Experiência, boas práticas e propostas para o aperfeiçoamento.** Apresentado

MONTEIRO, J. A. **Crimes informáticos: uma abordagem dinâmica ao direito penal informático.** Pensar, Fortaleza, v. 8, n. 8, p. 39-54, Fevereiro de 2003. Disponível em: http://hp.unifor.br/pdfs_notitia/1690.pdf

PIAUHYLINO, L. **PL 84/1999 – Projeto de Lei.** Disponível em: http://www.brdatanet.com.br/infocenter/biblioteca/pl8499.htm

PINHEIRO, R. C. **Os cybercrimes na esfera jurídica brasileira**. Agosto de 2000. Disponível em: http://www.egov.ufsc.br/portal/sites/default/files/anexos/19747-19748-1-PB.pdf Acessado em 35 de abril de 2013

Prevenção – Delegacias Cibercrimes. *In* SaferNet. Acessado em 07 de março de 2013. Disponível em: http://www.SaferNet.org.br/site/prevencao/orientacao/delegacias. Sem data.

Presidência da República – Casa Civil. Lei nº 12.737 de 30 de novembro de 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acessado em 31 de julho de 2013.

Primórdios do Imposto de Renda no Brasil. Disponível em: http://www.receita.fazenda.gov.br/Memoria/irpf/historia/histPriomordiosBrasil.asp Acessado em 12 de maio de 2013.

Quem somos? *In* SaferNet. Acessado em 07 de março de 2013. Disponível em: http://www.SaferNet.org.br/site/prevencao/orientacao/delegacias. Sem data.

Red October: Rússia e China podem estar por trás de operação de espionagem. Disponível em: http://canaltech.com.br/noticia/seguranca/Red-October-Russia-e-China-podem-estar-por-tras-de-operacao-de-espionagem/#ixzz2jhka3iwT. Acessado em 25 de setembro de 2013.

Relatório de Políticas de Internet. Observatório da internet.br. – observatório brasileiro de políticas digitais. Acessado em 02 de maio de 2013. Disponível em: http://www.cgi.br/publicacoes/livros/pdf/relatorio-politicas-internet-pt.pdf

REZENDE, P. A.D. **Cibercrime, Megalobby e *Sottogoverno***. *In* Observatório da Imprensa - Departamento de Ciência da Computação, Universidade de Brasília – Agosto de 2008. Disponível em: http://www.egov.ufsc.br/portal/conteudo/cibercrime-megalobby-e-sottogoverno

ROVER, T. **Lei sobre crimes na internet é positiva, mas redundante.** Publicado em 09 de dezembro de 2012 e acessado em 31 de janeiro de 2013. Disponível em: http://www.conjur.com.br/2012-dez-09/especialistas-lei-crimes-internet-positiva-redundante

SAFERNET BRASIL. **Safernet brasil vence prêmio de direitos humanos.** Brasília : 12 de dezembro de 2013. Disponível em: http://www.safernet.org.br/site/noticias/safernet-brasil-vence-pr%C3%AAmio-direitos-humanos. Acessado em 01 de janeiro de 2013.

SAFERNET BRASIL. **Educadores – prevenção.safernet.org.br. Cartilhas**. Disponível em: http://new.netica.org.br/educadores/cartilhas. Acessado em 29 de dezembro de 2013.

SANTOS, D. L. **Aplicação da Lei Penal no Espaço nos Crimes de Informática Transnacionais**. 2011. Disponível em: http://www3.pucrs.br/pucrs/files/uni/poa/direito/graduacao/tcc/tcc2/trabalhos2011_1/daniel_santos.pdf

SaferNet. **Institucional**, 2008. Disponível em: http://www.safernet.org.br/site/institucional. Acessado em 24 de maio de 2013.

SILVA, M. M. **Ação internacional no combate ao cibercrime e sua influência no ordenamento jurídico brasileiro**. 2012. 109 p. Dissertação de Mestrado em Direito Internacional Econômico da Universidade Católica de Brasília. Brasília : 2012.

STRICKLAND, J. **Como funcionam os hackers?** (Traduzido por HowStuffWorks Brasil). Sem data. Acessado em 09 de fevereiro de 2013. Disponível em: http://informatica.hsw.uol.com.br/hacker3.htm

SUPREMO TRIBUNAL DE JUSTIÇA. **Justiça usa Código Penal para combater crime virtual. Disponível em:** http://www.stj.gov.br/portal_stj/publicacao/engine.wsp?tmp.area=398&tmp.texto=90108. Acessado em 09 de fevereiro de 2013.

TRENDMICRO. **Brasil Desafios de Segurança Cibernética Enfrentados por uma Economia em Rápido Crescimento**. Agosto de 2013. Disponível em: http://www.trendmicro.com.br/cloud-content/br/pdfs/home/wp-brasil-final.pdf

VAZ, J.C. (2008). **O significado da prestação de serviços com foco no cidadão nas transformações da administração pública brasileira no período pós-redemocratização.** Disponível em: http://josecarlosvaz.pbworks.com/w/page/8531978/Foco%20no%20Cidadão%20nas%20Políticas%20Públicas. Acessado em 02 de janeiro de 2014.

VIANNA. Túlio Lima. **Hackers: um estudo criminológico da subcultura cyberpunk**. Disponível em: http://www.buscalegis.ufsc.br/revistas/files/anexos/29401-29419-1-PB.pdf