IV SINGEP
Simpósio Internacional de Gestão de Projetos, Inovação e Sustentabilidade
International Symposium on Project Management, Innovation and Sustainability
ISSN: 2317 - 8302

UM ESTUDO SOBRE CRIMES DIGITAIS: DETECÇÃO E PREVENÇÃO

ROBERTA RODRIGUES FAORO
Universidade de Caxias do Sul
roberta.faoro@ucs.br

BETINA RIBEIRO DE JESUS
Universidade de Caxias do Sul
betinarj@via-rs.net

MARCELO FAORO DE ABREU
Universidade de Caxias do Sul
marcelo.faoro@ucs.br

IV SINGEP
Simpósio Internacional de Gestão de Projetos, Inovação e Sustentabilidade
International Symposium on Project Management, Innovation and Sustainability
ISSN: 2317 - 8302

UM ESTUDO SOBRE CRIMES DIGITAIS: DETECÇÃO E PREVENÇÃO

Resumo

A Internet tem crescido além da imaginação e provido comunicação digital e interação para quase dois bilhões de usuários globais, o equivalente a aproximadamente um terço da população mundial. Associado a isso, a facilidade de acesso e o aumento do anonimato facilitados pela Internet permitem que os indivíduos sem escrúpulos interajam livremente com uma vasta comunidade global e comportem-se de forma que seria completamente inaceitável no mundo físico. Assim, o fenômeno da criminalidade da informática tornou-se uma ameaça constante quando se utiliza a Internet. Portanto, o objetivo deste estudo é identificar e caracterizar os principais crimes digitais para ajudar as pessoas que estão sendo ou possam ser vítimas de um crime digital. A pesquisa é de natureza qualitativa, de nível exploratório e a estratégia foi a pesquisa bibliográfica. Observou-se, que o problema dos crimes digitais tende a aumentar devido a fatores como a falta de cuidados dos usuários de tecnologias em geral, bem como, das técnicas utilizadas pelos cibercriminosos estarem se desenvolvendo cada vez mais. Conclui-se, que os crimes digitais geram grandes prejuízos à economia de diversos países e organizações e mais ainda, atingem a integridade das pessoas quando estas possuem seus dados acessados sem autorização e posteriormente violados.

Palavras-chave: Internet; Crimes Digitais; Prevenção.

Abstract

The internet has grown beyond imagination and provided digital communication and interaction to nearly two billion global users, equivalent to about one third of the world population. Associated with this, the ease of access and increased anonymity facilitated by the internet allow unscrupulous individuals freely interact with a wide global community and behave in a way that would be completely unacceptable in the physical world. Thus, the computer crime phenomenon has become a constant threat when using the internet. Therefore, the objective of this study is identify and characterize the main cybercrime to help people who are being or may be victims of cybercrime. The research is qualitative, exploratory level and the strategy was the literature. It was observed, the problem of computer crime tends to increase due to factors such as lack of care of users of technologies in general, as well as the techniques used by cybercriminals are developing more and more. It is concluded, that the cybercrime generate large losses to the economy of many countries and organizations and more, reach the integrity of the people when they have their data accessed without authorization and subsequently violated.

Keywords: Internet; Cybercrime; Prevention.

1 Introdução

Pessoas conectadas na Internet podem ser comparadas com pessoas caminhando em uma praça: estão vulneráveis e expostas a todos os tipos de pessoas e conteúdos. Sendo assim, é tão difícil assegurar que atos maliciosos não acontecerão com uma determinada pessoa que caminha na praça, quanto com as pessoas que acessam a Internet. Por isso, o acesso à rede mundial de computadores requer atenção e cuidados, a fim de que as possibilidades oferecidas sejam aproveitadas com mais segurança (Cunha & Nejm, 2012).

No contexto empresarial, as organizações dependem das ferramentas de tecnologias de informação e telecomunicações para o armazenamento de dados (Easttom, 2006). Adicionalmente, as empresas têm utilizado a Internet e outras tecnologias como meio de contato com clientes, parceiros e funcionários, independentemente da distância geográfica existente (Day, 2003). Como consequência da proliferação de atividades *on-line,* tem ocorrido o aumento no número de atividades criminosas cometidas, por meio ou no ambiente virtual. Deste modo, criando uma nova geração de cibercriminosos (Gupta & Hammond, 2005).

Segundo Ferreira (2005), crimes digitais são atos dirigidos contra um sistema de informática, tendo como subespécies atos contra o computador e atos contra os dados ou programas de computador. Complementando este conceito, podem ser considerados crimes digitais atos cometidos por intermédio de um sistema de informática e dentro deles incluídos infrações contra o patrimônio e/ou as infrações contra a liberdade individual e as infrações contra a propriedade imaterial. Para Pinheiro (2000), crimes digitais são todos os atos ilícitos praticados através da Internet que venham causar algum tipo de dano, seja ele patrimonial ou moral, ao ofendido.

Uma investigação sobre o *cyber-crime* realizada pela Symantec (2009) argumenta que o objetivo principal das atividades técnicas desenvolvidas pelos cibercriminosos é atacar os usuários finais para obter ganho financeiro. No entanto, o motivo por trás dos crimes digitais não está inteiramente relacionado ao ganho financeiro (Hunton, 2011). De acordo com Crespo (2011), algumas vezes este tipo de crime ocorre pelo mero gosto de superar desafios técnicos de segurança, pela vontade de invadir a privacidade alheia tendo acesso a informações sigilosas, ou, ainda, por se ter a intenção de manipular, defraudar e sabotar dados.

Os jovens são vulneráveis e também são alvo, sendo submetidos a crimes *on-line*, como aliciamento, *cyber-bullying*, pornografia e pedofilia. Uma pesquisa com adolescentes entre 11 e 18 anos de idade, realizada pela instituição de caridade *BeatBullying*, revelou que quase um terço das pessoas entrevistadas tinham experimentado algum tipo de *bullying on-line* (Beatbullying, 2009). Ainda, um estudo global aponta que 65% dos adultos usando a Internet já foram vítimas de *cyber-crime*, e mais de 50% haviam sido submetidos a um vírus de computador e ataques de *malware* (Norton, 2010).

Considerando o exposto, o tema de pesquisa deste estudo envolve a descrição dos riscos aos quais os internautas ficam expostos ao acessar domínios públicos na Internet e utilizar os demais serviços oferecidos através dos diversos dispositivos informáticos. Deste modo, o presente artigo apresenta uma revisão bibliográfica, concisa e acurada, de caráter pedagógico, a respeito de crimes digitais. Para isso, serão abordados os conceitos fundamentais sobre crimes digitais, sua evolução e características. Além disso, aborda uma compilação das principais ações que podem ser utilizadas como proteção contra os criminosos virtuais. Sendo assim, o objetivo deste artigo é identificar e caracterizar os principais crimes digitais e recomendar ações de prevenção para as pessoas que estão sendo ou possam ser vítimas de um crime digital.

2. Crimes digitais

Os crimes de informática são aqueles perpetrados através dos computadores, contra os mesmos, ou através deles. A maioria dos crimes é praticada através da Internet, e o meio usualmente utilizado é o computador (Castro, 2003). Por outro lado, os crimes digitais podem ser conceituados como sendo as condutas de acesso não autorizado a sistemas informáticos, ações destrutivas nesses sistemas, a interceptação de comunicações, modificações de dados, infrações a direitos de autor, incitação ao ódio e discriminação, escárnio religioso, difusão de pornografia infantil, terrorismo, entre outros (Pinheiro, 2010).

Também chamados de *cyber-crimes*, segundo Pinheiro (2000), estes são todos os atos ilícitos praticados através da Internet que venham a causar algum tipo de dano, seja ele patrimonial ou moral, ao ofendido. De outro ponto de vista, pode-se determinar crimes cibernéticos como sendo aqueles que têm por instrumento ou por objeto sistema de processamento eletrônico de dados, apresentando-se em múltiplas modalidades de execução e de lesão de bens jurídicos (Rocha, 1994). Já o Conselho da Europa vê o *Cyber-crime* como uma espécie de crime organizado que "é uma ameaça aos direitos humanos, democracia e ao estado de direito" (Coe Report, 2004).

> atos dirigidos contra um sistema de informática, tendo como subespécies atos contra o computador e atos contra os dados ou programas de computador. Atos cometidos por intermédio de um sistema de informática e dentro deles incluídos infrações contra o patrimônio; as infrações contra a liberdade individual e as infrações contra a propriedade imaterial (Ferreira, 2005, p. 261).

Segundo Hunton (2009, p. 106), "os termos *cyber-crime*, crime da Internet e *e-crime* são usados para descrever comportamento criminoso e indesejável ou prejudicial que é assistido ou habilitado pela tecnologia em rede e, mais especificamente, a Internet". Neste contexto, o termo *e-crime* é definido separadamente, como sendo o uso de computadores em rede ou tecnologia Internet para cometer ou facilitar o cometimento de crime (ACPO, 2009).

> como crime formal, a consumação da invasão de dispositivo informático ocorrerá com a efetiva violação indevida de mecanismo de segurança, e a consequente entrada sem autorização em dispositivo alheio, independente da ocorrência de qualquer outro resultado naturalístico (Siena, 2013, p. 2).

Para Hilbert (2013), *cyber-crime* é o uso de um computador ou de uma rede de computadores para conduzir um ato criminal, motivado por alguma forma de lucro, geralmente monetário, ou algum outro ganho. Isto inclui roubo de identidade, fraude, perseguição, extorsão *on-line*, *spam* e *phishing*. Assim sendo, a constatação de um crime informático e sua posterior classificação são tarefas difíceis, tendo em vista a evolução da tecnologia e as poucas conclusões a respeito deste assunto. Porém, são igualmente importantes e merecem especial atenção. De acordo com Crespo (2011), Tiedemann formulou em 1980 a seguinte classificação dos delitos informáticos:

a) Manipulações: podem afetar o *input* (entrada), o *output* (saída) ou mesmo o processamento de dados;
b) Espionagem: subtração de informações arquivadas abarcando-se, ainda, o furto ou emprego indevido de software;
c) Sabotagem: destruição total ou parcial de programas;
d) Furto de tempo: utilização indevida de instalações de computadores por empregados desleais ou estranhos (Crespo, 2011, p. 15).

Conforme abordado por Crespo (2011), em todas as classificações há distinções e pontos em comum a serem considerados: algumas posições atribuem os meios eletrônicos como objeto protegido (bem jurídico) e outras os atribuem como meio/instrumento de se lesionar outros bens. Esta última torna-se umas das mais oportunas, tendo em vista que abarca

mais opções acerca das práticas. Neste sentido, Hunton (2011) introduziu através de uma visão conceitual e lógica as principais características (Quadro 1), consideradas específicas na prática de crimes cibernéticos.

Característica	Descrição
Primeira	Intenção criminosa ou ilícita: leva a um comportamento criminoso específico.
Segunda	Identificação dos objetivos dos dados: permite o mapeamento e a investigação de atividades criminosas.
Terceira	Métodos de ataque: auxiliam na ocorrência dos crimes digitais.
Quarta	Tecnologia em rede: possui uma grande extensão que pode ser considerada uma arena para cometimento de crimes cibernéticos.
Quinta	Ocultação e evasão: envolve o aumento do anonimato e a dificuldade na apreensão dos cibercriminosos e recuperação de evidências voláteis.
Sexta	Ambiente globalizado: envolve o advento dos satélites e tecnologia de telefonia móvel, além da Internet, que oferecem aos cibercriminosos um vasto ambiente sobre o qual podem atuar e dificultam a aplicação da lei e recuperação de evidências.

Quadro 1. Características de Crimes Cibernéticos
Fonte: Adaptado de HUNTON, P. The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation. Journal Computer Law and Security Review, 2011.

Por fim, *cyber-crime* pode ser considerado como uma forma de desvio *on-line* utilizando tecnologia, seja em um computador ou telefones inteligentes. Seu desenvolvimento não foi um ato instantâneo, foi envolvido em mudanças evolutivas (Donner et al., 2014). Sendo assim, na próxima seção serão abordadas a evolução dos crimes cibernéticos e as suas gerações.

2.1 A evolução e as gerações do *cyber-crime*

Segundo Crespo (2011) pode-se dividir a evolução em três marcos: a sociedade da informação, a sociedade de riscos e o ambiente globalizado. Assim sendo, a sociedade da informação (Quadro 2) não surgiu repentinamente. Adveio de um longo processo de desenvolvimento, que pode ter o início vinculado à própria Revolução Industrial, que consistiu em um conjunto de mudanças tecnológicas com significativo reflexo na cadeia produtiva. A evolução pode ser didaticamente dividida em duas partes nos séculos XIX e XX, em que predominou a substituição da mão de obra humana e de animais por máquinas, e mais tarde, a partir do século XX, a substituição da atividade humana intelectual pelas máquinas. Diz-se que sociólogos economistas entendem esta segunda parte do desenvolvimento como uma "Segunda Revolução Industrial" (Crespo, 2011). Associado a isso, Del Canto (2002) discorre algumas linhas sobre a chamada "Segunda Revolução Industrial", já relacionando com a ocorrência de fatos ilícitos.

Década	Descrição
50	Os computadores passaram a ser empregados na indústria e, em pouco tempo, já se tinha notícias de ações ilícitas com o uso dos mesmos;
60	Com o processamento massivo de dados pessoais em bancos eletrônicos de dados, alguns países passaram a ter alguma preocupação com o armazenamento, transmissão e conexão de dados pessoais;
70	Nessa época, houve generalização do uso dos computadores e sistemas informáticos nas atividades comerciais e empresariais, bem como a implantação de redes abertas que, logo, foram alvo de acesso ilegal (ou *hacking*);
80	Com a expansão dos computadores ao uso pessoal, surgiu e disseminou-se a pirataria de programas informáticos. O aparecimento dos caixas eletrônicos foi alvo de fraude dos cartões magnéticos;

90	Aqui temos o auge da convergência entre informática e telecomunicações, a generalização e extensão dos computadores, Internet e serviços eletrônicos a quase todas as áreas da vida. Isso fez com que o uso passasse a ser feito não só por particulares, empresários, administrações, mas também por grupos racistas, neonazistas, criminosos econômicos e organizações criminosas, de tal forma que a inteligência informática começa a integrar não só a vida em geral, mas o crime em geral. A sociedade atribui mais importância aos bens materiais (depósitos em dinheiro, propriedades intelectuais, segredos comerciais) que não só adquirem outro valor, mas transformam-se em fator de poder.

Quadro 2. A "Segunda Revolução Industrial" na Sociedade da Informação
Fonte: Adaptado de DEL CANTO, E.R. Delincuencia Informática y Fraudes Informáticos. Granada: Comares, 2002.

Em seguida, Crespo (2011) comenta que o desenvolvimento tecnológico cresce em complexidade e rapidez, fazendo aparecerem novos riscos, com maiores impactos, sem que possam ser limitados no tempo ou espaço. São riscos que adquirem dimensão social, não se limitando aos indivíduos (Crespo, 2011). E, nesse sentido, a delinquência informática aparece configurada como um fenômeno social relacionado aos novos riscos, sendo, portanto, parte da "sociedade de risco". Além disso, a doutrina já é clara em apontar a criminalidade informática como forma de ilícito complexo, decorrente da sociedade de risco (Netto, 2006). Por fim, Crespo (2011) refere-se à significativa mudança da evolução social. Trata-se do progressivo contato dos cidadãos do mundo, que pode ser verificado em todos os âmbitos sociais. A base que estrutura este conceito é a de um mundo interligado, com estreitas relações econômicas, políticas e sociais, fruto da evolução das Tecnologias da Informação e da Comunicação, em especial da *World Wide Web*. Sendo assim, o Quadro 3, apresenta a relação entre crimes digitais e a sociedade.

Sociedade	**Crimes Digitais**
Sociedade da Informação	Teve seu início vinculado à Revolução Industrial e se estende por diversas décadas, podendo-se verificar a ocorrência de atos ilícitos já desde a década de 50. Na década de 70 destaca-se os computadores, sistemas de informações e redes abertas como alvos de *hackers*. Na década de 80 já ocorreram fraudes em caixas eletrônicos e cartões magnéticos. E, na década de 90 entramos no auge da convergência entre informática e telecomunicações e a generalização de serviços informáticos no cotidiano da sociedade.
Sociedade de Riscos	O desenvolvimento tecnológico é um dos fatores que faz surgir novos riscos, que adquirem dimensão social, com maiores impactos. Nesse sentido, a delinquência informática aparece configurada como um fenômeno social relacionado aos novos riscos. A criminalidade informática é apontada pela doutrina como ilícito complexo, decorrente da sociedade de risco.
Ambiente Globalizado	Este conceito é estruturado através da visão de um mundo interligado, com estreitas relações econômicas, políticas e sociais, fruto das Tecnologias da Informação e da Comunicação, em especial da *World Wide Web*.

Quadro 3. A Relação entre Crimes Digitais e a Sociedade
Fonte: Adaptado de NETTO, A. V. Tipicidade penal e sociedade de risco. São Paulo: Quartier Latin, 2006 e CRESPO, M. X. F. Crimes digitais. São Paulo: Saraiva, 2011.

Ainda assim, sobre a evolução do *cyber-crime*, existe a possibilidade de classificá-lo e dividi-lo em três gerações, de acordo com as táticas utilizadas pelos criminosos. Desta forma, a primeira geração do *cyber-crime* se caracteriza pela exploração ilegal de computadores *mainframe* e sistemas operacionais. Em geral, esses comportamentos envolvem crimes que já eram existentes antes da criação dos computadores e da Internet, mas essas inovações tecnológicas proporcionaram outra arena para cometê-los. Esses crimes têm a intenção de ganho financeiro ou destruição de informações restritas (Wall, 2010). Já, a segunda geração do *cyber-crime* usa as redes de computadores. Em outras palavras, é a criminalidade que já existe, mas expandida e adaptada através do uso da Internet (Katos & Bednar, 2008; WALL, 2010). *Hacking* e *cracking* são as formas mais comuns desta geração (Donner et al., 2014). Por último, a terceira geração do *cyber-crime* é identificada pela natureza da distribuição e foi exclusivamente desenvolvida pela criação da Internet. Esses crimes não existiriam se não

houvesse a Internet, que é o único lugar onde podem ocorrer. Disseminação de *malware*, tais como vírus ou cavalos de troia, são exemplos desta nova geração (Donner et al., 2014).

Considerando o exposto, é notável que o crescimento da tecnologia da informação foi o que introduziu uma nova forma de criminalidade para o sistema de justiça penal, bem como, trouxe novos meios para a ocorrência dos crimes cibernéticos. Portanto, em meio a grande variedade de crimes que podem ser cometidos atualmente em meio virtual, surge a necessidade de identificar quais são os crimes que de fato se enquadram como sendo digitais.

2.2 Principais crimes digitais

A respeito da classificação de crimes digitais, surgem diversas abordagens de diferentes autores. De acordo com Sieber (1998), um dos maiores estudiosos do tema, os ilícitos são classificados da seguinte forma: a) Violações à privacidade; b) Crimes econômicos (*Hacking*, espionagem, piratarias em geral (cópias não autorizadas), sabotagem e extorsão, fraude); c) Conteúdos ilegais e nocivos; d) Outros ilícitos (contra a vida, crime organizado e guerra eletrônica). Já Ferreira (2005) argumenta que uma classificação mais comum é a de separar os delitos em que a informática é meio, e em outras classificações, as demais condutas. Desta forma, é o que Briat (1985) propõe:

a) Manipulação de dados e/ou programas afim de cometer uma infração já prevista pelas incriminações tradicionais;
b) Falsificação de dados ou programas;
c) Deterioração de dados e de programas e entrave à sua utilização;
d) Divulgação, utilização ou reprodução ilícitas de dados e de programas;
e) Uso não autorizado de sistemas de informática;
f) Acesso não autorizado a sistemas de informática (Briat, 1985, p. 22).

Do ponto de vista de doutrinadores nacionais, destaca-se o proposto por Vianna (2003), que classifica os delitos como: a) delitos em que o computador foi instrumento para a execução do crime, mas que não provocou lesão ao bem jurídico, são denominados Delitos Informáticos Impróprios; b) delitos em que são afetados os dados, são denominados Delitos Informáticos Próprios; c) delitos complexos nos quais, além da inviolabilidade dos dados há outro bem jurídico lesado, são denominados Delitos Informáticos Mistos e; d) delitos informáticos próprios que atuem como crime-meio para a realização de crime-fim, são denominados Delitos Informáticos Mediatos ou Indiretos. Uma classificação menos complexa, todavia, mais plausível de ser adotada (Crespo, 2011), envolve: a) condutas perpetradas contra um sistema informático e; b) condutas perpetradas contra outros bens jurídicos (Ferreira, 2005; Greco Filho, 2000). Esta última será a abordagem adotada neste estudo, considerando que trata de dois tipos básicos de crimes: crimes digitais próprios, que correspondem às condutas perpetradas contra um sistema informático e crimes digitais impróprios que correspondem às condutas contra outros bens jurídicos.

Neste sentido, os Quadros 4 e 5 apresentam os crimes digitais próprios e os crimes digitais impróprios. Assim sendo, crimes digitais próprios (Quadro 4) envolvem delitos em que os dados são afetados (Vianna, 2003), e, além disso, envolvem delitos cujos bens jurídicos atingidos são primordialmente os sistemas informatizados ou de telecomunicações ou dados (Crespo, 2011).

Crime Digital Próprio	**Descrição**
Acesso não autorizado	Aquele que acessa de forma ilegítima um sistema computacional pode ter à sua disposição ferramentas, programas, bancos de dados, enfim, uma enormidade de informações e possibilidades de cometer ilícitos civis, administrativos e penais.
Obtenção e transferência ilegal de dados	Obtenção de dados através de meios como *spywares* (programas que rastreiam informações do usuário contidas em seu computador).

Dano informático	Há duas formas de danificar dados informáticos: com a destruição ou danificação da mídia que os arquiva ou com o uso da informática.
Dos vírus e sua disseminação	Vírus são segmentos de códigos de computação que se anexam a programas ou sistemas de modo a se propagar pelas máquinas e contaminar outros sistemas em contato com estas, através de *e-mails* e até mesmo por transmissão de dados maliciosos por outros métodos.
Divulgação ou utilização indevida de informações	Uso da técnica conhecida como *spam*, considerado uma das maiores pragas da Sociedade da Informação e também conhecido pela sigla UCE (*Unsolicited Commercial Email* ou Mensagem Comercial Não Solicitada).
Embaraçamento ao funcionamento de sistemas	Geralmente se dá pelos chamados Ataques de DoS – *Denial of Services*, ataques de negação de serviços. Nestes ataques, computadores são utilizados para tirar de operação um serviço ou outros computadores conectados à Internet.
Engenharia Social e *Phishing*	Engenharia social trata-se de todo método que mascara a realidade para explorar ou enganar a confiança de uma pessoa detentora de dados importantes a que se quer ter acesso, além disso, é o artifício intelectual para acessar informações sigilosas e que, portanto, não utiliza necessariamente tecnologia, mas sim qualquer meio de comunicação. Já o *phishing* trata-se de engenharia social que tem como finalidade obter informações relevantes, na modalidade fraude virtual, para a obtenção de dados valiosos dos particulares.

Quadro 4. Os Crimes Digitais Próprios
Fonte: Adaptado de CRESPO, M. X. F. Crimes digitais. São Paulo: Saraiva, 2011.

Já, os crimes digitais impróprios (Quadro 5) são aqueles tradicionalmente tipificados no ordenamento, mas atualmente praticados com o auxílio da tecnologia moderna. Desta forma, esta denominação apenas representa que os ilícitos penais podem ser cometidos por meio de novos modos. São exemplos desta modalidade crimes contra a honra, crimes de ameaça e até mesmo estelionato. Apesar disso, nada mais são do que os antigos crimes tipificados sob outra forma de cometimento (Crespo, 2011).

Crime Digital Impróprio	**Descrição**
Ameaça	Envio de e-mails ou publicações em redes sociais envolvendo frases de ameaça.
Participação em suicídio	Criação de comunidades e fóruns em redes sociais contendo dicas sobre como tirar a própria vida ou emprego de termos que "estimulem" o suicídio como "o mundo seria melhor sem você" e "se mate".
Incitação e apologia ao crime	Participantes de comunidades destinadas a veiculação de preconceito mediante agressões a outras pessoas e o consumo ou tráfico de drogas podem vir a ser responsabilizadas por este tipo de crime.
Falsa identidade e falsidade ideológica	No primeiro caso uma pessoa se faz passar por quem não é, utilizando dados e até mesmo senha de outra pessoa. Já no segundo caso, há inserção de dados falsos ou omissão de algo que deveria constar, em documentos públicos ou particulares, com intenção de prejudicar direito, criar obrigação ou alterar a verdade sobre fato juridicamente relevante.
Violação de direitos autorais, uso indevido de marcas e pirataria de *software*	A pirataria é o ato de copiar ou vender produto não autorizado pelo detentor dos direitos. É crime violar direitos de autor de programa de computador, bem como a venda, aquisição, exposição à venda, o depósito ou a ocultação, para fins de comércio, de original ou cópia de programa de computador, produzido com violação de direito autoral.
Pornografia infantil	É crime transmitir, publicar, distribuir, adquirir, possuir e armazenar vídeos, fotografias, imagens, envolvendo situações de pornografia com crianças e adolescentes.
Crimes contra a honra	Calúnia: atribuição de um fato criminoso a alguém, sabendo-se falsa tal acusação; difamação: atribuição de fato ofensivo à reputação de alguém, desacreditando-a publicamente; injúria: atribui características negativas sobre as qualidades físicas, morais ou intelectuais de cada um de nós; racismo e preconceito: disseminação de ideias que se referem à prática, indução ou incitação de discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional.

Quadro 5. Os Crimes Digitais Impróprios
Fonte: Adaptado de CRESPO, M. X. F. Crimes digitais. São Paulo: Saraiva, 2011.

Ainda assim, pode-se tratar das condutas mais comuns que podem resultar em crimes digitais, considerando o âmbito empresarial, que estão relacionadas no Quadro 6, de acordo com Crespo (2011):

Conduta	**Configuração de Crime**
Uso indevido de senha	Falsa identidade, falsidade ideológica e estelionato.
Vazamento de informações	Violação de sigilo e concorrência desleal
Cópia ilegal de dados e desvio de clientes	Concorrência desleal.
Uso não autorizado da marca	Violação de marcas, patentes e desenho industrial.
Mau uso do *e-mail* corporativo	Corresponsabilização por ilícitos praticados pelo funcionário.
Pirataria e *download* de *softwares* não homologados e *download* de músicas, imagens e vídeos	Violação de direitos autorais, uso indevido de marcas e pirataria de *software*
Existência de conteúdo inadequado nas máquinas, como mensagens preconceituosas, racistas ou de pornografia infantil	Crime contra a honra, de racismo e de pornografia infantil.
Contaminação por vírus e *trojans*	Crime de dano.
Falhas de segurança podem permitir que *hackers* modifiquem arquivos de modo a permitir que se obtenha acesso a contas de outras pessoas e efetuar transações fraudulentas, como compras e transferência de dinheiro	Interceptação ilegal de dados.
Manutenção de campos ocultos em *softwares* de comércio eletrônico, possibilitando alterar os preços e comprar produtos pagando menos, por exemplo	Interceptação ilegal de dados.
Ataques de negação de serviço, gerando prejuízo na prestação de serviços ou no fornecimento de mercadorias	Embaraçamento ao funcionamento de sistemas.
Acesso a informações sigilosas pela exploração de falhas de segurança e sabotagem de fluxo de dados, acessando arquivos de registros e o código-fonte de aplicativo	
Defacing ou "pichação de página *web*"	
Ocultação de comandos perigosos por meio de um "cavalo de troia" que libera código malicioso ou não autorizado, danificando o *site*	Dos vírus e sua disseminação.

Quadro 6. Condutas que podem resultar em crimes digitais
Fonte: Adaptado de CRESPO, M. X. F. Crimes digitais. São Paulo: Saraiva, 2011.

3. Recomendações de prevenções para os crimes digitais

Segundo Inellas (2004) a Internet é uma rede de computadores integrada por outras redes menores, comunicando-se entre si. Os computadores se comunicam através de um endereço lógico, chamado de endereço IP, onde uma gama de informações é trocada, surgindo neste ponto o problema: existe uma quantidade enorme de informações pessoais disponíveis na rede, ficando à disposição de milhares de pessoas que possuem acesso à Internet, e quando não disponíveis pelo próprio usuário, são procuradas por outros usuários que buscam na rede mundial de computadores o cometimento de crimes, os denominados crimes digitais.

Aliado a isso, os *cibercriminosos* se envolvem em ataques *on-line* que exploram vulnerabilidades e deficiências dentro das defesas cibernéticas de organizações (Szor, 2005) e, ressalta-se ainda que, por causa do tamanho, recursos e limitações de conhecimento, as pequenas empresas são muitas vezes mal preparadas para combater as ameaças emergentes do *cyber-crime* (Ryan, 2000). Portanto, nesta seção serão expostas algumas práticas que podem e que devem ser utilizadas, não apenas no ambiente organizacional, mas por qualquer pessoa que utiliza a Internet como ferramenta de trabalho, estudo ou até mesmo entretenimento.

Assim sendo, Awe (2004) declarou que não há uma medida que vai curar a ameaça do *cyber-crime*. Ainda afirmou que é a combinação de esforços em conjunto com sinceridade e

vigor que, quando forem implementadas e administradas servirão para reduzir os riscos de forma mais eficaz. Ajala (2007) sugere alguns questionamentos que dizem respeito ao combate dos crimes digitais:

> na luta contra a *cyber* criminalidade a pergunta a ser feita é: como a nação luta contra a mesma? O interessante é que há muito para se falar sobre o combate ao *cyber-crime*. Mas onde estão os esforços? E de que forma eles são eficazes? Uma vez que existe uma consciência da ameaça que representa para a sociedade, quais foram os esforços sinceros e significativos para combater o *cyber-crime*? Quanto foi investido em termos de tempo, educação, pessoal, etc? (Ajala, 2007, p. 27-28).

Segundo Ferrari (2014), atualmente, a economia digital está mais misturada à tradicional – e isso traz riscos, tanto na esfera pessoal quanto na profissional, muitas vezes negligenciados. Em entrevista concedida à revista Exame, o presidente da empresa de segurança Kaspersky, Eugene Kaspersky, diz que este é um fenômeno global, mas alguns povos estão mais vulneráveis do que outros. Nesse ponto, o especialista em segurança digital menciona que as empresas brasileiras têm perdas financeiras causadas por descuidos de seus funcionários bem acima da média mundial. Kaspersky ainda diz que "a solução, que parece piada, é ir morar na Floresta Amazônica ou na Sibéria, bem longe de uma conexão. Qualquer pessoa com um celular pode ser espionada". O mesmo ainda relata que apesar de todo o avanço na área de *softwares* para segurança digital, as pessoas estão deixando de se preocupar com segurança por saber que são vigiadas independentemente de sua vontade, clicam em *links* suspeitos e enviam *e-mails* com detalhes de projetos sigilosos e que cerca de 40% dos funcionários de grandes empresas não seguem as regras de segurança sugeridas pela área de tecnologia e, além disso, as técnicas dos criminosos estão cada vez mais sofisticadas.

Ainda assim, Goucher (2010) menciona que o *cyber-crime* é um termo interessante e propõe o seguinte questionamento: "como os usuários podem se defender contra um ataque que podem não reconhecer, proveniente de um atacante que não conhecem?". A autora ainda retrata o fato de que há um fator que não muda dos crimes tradicionais para os digitais: há uma vítima. No entanto, a diferença com a maior parte dos crimes que ocorrem na Internet é que as vítimas imaginam estar sem suporte. Elas não têm para onde ir, não há um número de emergência para discar e ninguém para conversar. Sendo assim, percebe-se a importância de noções básicas de segurança, prevenção e comportamentos no mundo virtual, além da obtenção de informações quanto à legislação e formas de denúncia, considerando que muitas vezes os *cibercriminosos* apenas encontram brechas devido à falta de conhecimento das vítimas.

Como pode ser visualizado no Quadro 7, de acordo com SaferNet (2012) existem alguns princípios para a governança e uso da Internet no Brasil e ainda, segundo Cunha e Nejm (2012) a Internet não mais se trata de uma terra sem lei e em algumas situações, para nos encontrarmos em segurança, devemos nos lembrar dos nossos deveres como internautas:

> fazer um uso responsável das ferramentas que a Internet oferece, prezando sempre pelo bem estar de todos; respeitar a diversidade de culturas, personalidades e opiniões; não disseminar na rede preconceitos de cor, gênero, religião, orientação sexual, de origem social ou de qualquer outro tipo; buscar fontes confiáveis de pesquisa; não reproduzir materiais que não foram feitos por você como se fossem de sua autoria; evitar encaminhar *e-mails* para todos os contatos - não praticar *spam* (Cunha & Nejm, 2012).

Princípio	Definição
Liberdade, privacidade e direitos humanos	O uso da Internet deve guiar-se pelos princípios de liberdade de expressão, de privacidade do indivíduo e de respeito aos direitos humanos, reconhecendo-os como fundamentais para a preservação de uma sociedade justa e democrática.

Governança democrática e colaborativa	A governança da Internet deve ser exercida de forma transparente, multilateral e democrática, com a participação dos vários setores da sociedade, preservando e estimulando o seu caráter de criação coletiva.
Universalidade	O acesso à Internet deve ser universal para que ela seja um meio para o desenvolvimento social e humano, contribuindo para a construção de uma sociedade inclusiva e não discriminatória em benefício de todos.
Diversidade	A diversidade cultural deve ser respeitada e preservada e sua expressão deve ser estimulada, sem a imposição de crenças, costumes ou valores.
Inovação	A governança da Internet deve promover a contínua evolução e ampla difusão de novas tecnologias e modelos de uso e acesso.
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.
Imputabilidade 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.
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.
Padronização e interoperabilidade	A Internet deve basear-se em padrões abertos que permitam a interoperabilidade e a participação de todos em seu desenvolvimento.
Ambiente legal e regulatório	O ambiente legal e regulatório deve preservar a dinâmica da Internet como espaço de colaboração.

Quadro 7. Os dez princípios para a governança e uso da Internet no Brasil
Fonte: SAFERNET BRASIL. Saferdicas: Brincar, estudar e... Navegar com segurança na Internet! 5. ed. Salvador: SaferNet Brasil, 2013

O uso seguro da Internet envolve algumas atitudes como: nunca divulgar senhas, nome completo, endereços, números de telefone ou fotos íntimas, comunicar-se com educação, evitar gravar senhas e *login* no computador para não facilitar roubos, ter cuidado ao baixar arquivos pois estes podem conter vírus, materiais impróprios ou ser ilegais (antivírus e filtros podem ajudar a proteger), nunca aceitar que *sites* instalem programas no computador e não fazer *download* de algo que não se conhece o que é e sua origem e, por fim, buscar provedores e serviços que ofereçam recursos de segurança e sejam éticos e responsáveis (Safernet, 2013).

Ainda no contexto da Internet em geral, existem os navegadores, também conhecidos como *browsers*, que são programas que permitem visualizar os conteúdos e explorar as páginas na Internet. Para que o usuário se mantenha seguro nessas ferramentas, é importante que: leia com atenção as mensagens exibidas pelo navegador, pois elas podem ajudar a identificar um programa malicioso; utilize o bloqueio de *pop-up* em seu navegador; e que, ao realizar transações financeiras, confira se aparece o desenho de um cadeado fechado no rodapé da página e se o endereço começa com "*https*", ao invés de "*http*" (Safernet, 2013).

Quanto aos *sites* de busca, que são páginas que oferecem o serviço de busca de conteúdos disponíveis em outros *sites* na Internet a partir de expressões ou palavras-chave, é importante: não confiar em todas as informações de seu conteúdo, já que podem apresentar incorreções; colocar as palavras entre aspas para evitar resultados muito amplos; utilizar o serviço de pesquisa segura dos buscadores; e procurar em preferências e ativar a filtragem de páginas com conteúdo sexual explícito, impedindo que elas apareçam nos resultados da pesquisa. Ao utilizar o servidor de *e-mail* o usuário pode se proteger da seguinte forma: configurar a conta para bloquear contatos indesejados, evitar senhas com informações óbvias, não aceitar nem abrir *e-mail* de desconhecidos, procurar saber a origem da informação e se o responsável é de confiança ou conhecido, ter muito cuidado com cartões virtuais e não abrir arquivos cujo nome possui ".exe" no final, atualizar o antivírus e usar *anti-spam*, jamais acreditar em pedidos de pagamento, correção de senhas ou solicitação de qualquer dado

pessoal por *e-mail* e no caso de recebimento de *spam*, denunciar ao próprio servidor de *e-mail* (Safernet, 2013).

No que diz respeito ao comportamento em redes sociais, Cunha e Nejm (2012) sugerem que, primeiramente, os usuários pensem bem nos tipos de informação que irão publicar em seu perfil. Também é importante controlar o quê e para quem essas informações serão publicadas, perceber que qualidade prevalece sobre quantidade pois deve-se ter cuidado com estranhos, não compartilhar senhas, evitar dar endereços de lugares como moradia, trabalho e escola. Além disso, um item muito importante trata-se de criar uma senha forte, mesclando números, letras e outros caracteres. De acordo com a instituição Childhood (2012) não devem ser usadas fotos em alta resolução na construção de perfis em redes sociais, pois o risco delas serem usadas em montagens é maior do que se as fotos forem menores em tamanho e qualidade. Já de acordo com SaferNet (2013) deve-se evitar aceitar encontro presencial com desconhecidos, trocar a senha de acesso periodicamente e configurar a conta para bloquear os contatos indesejados. O Quadro 8 apresenta recomendações na utilização de redes sociais *Twitter* e *Facebook*, ambas utilizadas globalmente.

Rede Social	Recomendações gerais	Recomendações na criação da conta
Twitter	Se você usou a opção "proteger meus *tweets*" ao configurar seu perfil no Twitter, cada pessoa que quiser segui-lo terá que pedir sua permissão. Ao receber solicitações verifique se reconhece a pessoa que a enviou. Perfis com milhares de seguidores podem indicar perfis falsos ou de spam.	- Se possível, não utilize seu nome completo; - Defina uma senha forte; - Para concluir a configuração mais segura de sua conta seleciona a opção "Settings" – em português, configurações – no canto direito superior da tela. Dentro destas opções: seja genérico na descrição sobre você, no campo "local onde você mora" preencha apenas país ou estado, selecione a opção "protect my tweets" – proteger meus tweets – para que as pessoas tenham permissão para ter acesso à sua conta.
Facebook	Substitua seu sobrenome pela abreviatura depois da criação da conta.	- Para configurações adicionais e mais segurança, após a criação da conta, selecione a opção "Configurações", no canto superior direito da tela. - Pergunta de segurança: escolha uma pergunta da lista apresentada e defina uma resposta. É muito importante não responder a esta pergunta com a resposta correta, pois é possível investigar a partir de buscar na Internet e em redes sociais e obter as respostas. Defina uma resposta e anote-a. Este conjunto será utilizado no processo de recuperação da senha da conta. - Privacidade: esta opção permite controlar o acesso de outros perfis às informações, fotos e outros recursos do perfil. - Perfil: definir qual será o nível de acesso ao conteúdo. O nível mais restritivo é "apenas amigos". Daí a importância de não aceitar solicitações de desconhecidos.

Quadro 8. Recomendações na utilização de redes sociais
Fonte: RNEP - Rede Nacional de Ensino e Pesquisa. Segurança em Redes Sociais: recomendações gerais. CAIS/RNP, Rio de Janeiro, set. 2011.

Lan houses e infocentros são centros públicos de acesso à Internet com vários computadores em rede. Os Infocentros e Telecentros são espaços criados e apoiados pelos governos para ampliar o acesso gratuito à Internet no país. A diferença entre eles e as *Lan Houses* é que estas últimas são comerciais e cobram pelo acesso. No Brasil, em 2008, cerca de 48% dos internautas acessaram a Internet por meio de uma *Lan House*. Daí percebe-se a necessidade de esclarecer a melhor forma de comportar-se nestes ambientes de uso comum, de forma segura e sem correr riscos: lembrar sempre de clicar em "sair" antes de fechar as páginas e os programas, não deixar senhas gravadas, não aceitar ajuda de estranhos,

chamando sempre o responsável pelo estabelecimento em caso de dúvida e evitar acessar *sites* de bancos e fazer compras em *Lan Houses* e Infocentros (Safernet, 2013).

O Quadro 9 apresenta algumas situações que podem ser encontradas na Internet e algumas dicas sobre como os usuários devem se comportar para evitar que situações como estas aconteçam ou como tratá-las depois de ocorridas.

Situação	**O que é e como ocorre?**	**Dicas**
Cyber-crime	Uso das novas tecnologias para ações ilícitas como roubo, chantagem, calúnia, difamação e violação aos Direitos Humanos fundamentais. O ciberespaço é um ambiente público que reflete a diversidade e complexidade da sociedade, tanto nas qualidades como nas práticas ilegais. Como todo crime, prejudica as pessoas moralmente ou financeiramente. Quem pratica crimes pela Internet se aproveita da falsa sensação de anonimato e impunidade.	- Divulgar o mínimo de informações pessoais na Internet; - Trocar senhas com frequência, evitar utilizar informações óbvias ao criá-las e não compartilhar suas senhas; - Não deixar conta de *e-mail* ou rede social conectada quando não estiver usando o computador; - Não gravar arquivos confidenciais ou dados pessoais em computadores de *Lan Houses*; - Comunicar imediatamente ao banco quando perceber alguma irregularidade no extrato bancário ou cartão de crédito; - Nas compras pela Internet, dar preferência para pagamento com cartão de crédito ou boleto bancário e sempre procurar empresas conhecidas e respeitadas.
Ciberbullying	Trata-se de *bullying* virtual e é considerado uma forma de violência. Ocorre quando pessoas divulgam conteúdos que ofendem, humilham e ameaçam outra pessoa, com fotos, vídeos ou comentários violentos, causando vergonha e intimidação, deixando-a com medo.	- Relatar o caso a algum adulto de confiança; - Não responder e gravar todas as mensagens e/ou imagens; - Pais e escola devem ajudar ou podem ser responsabilizados por não terem ajudado; - Quando não há espaço para resolver o problema com diálogo, o caso pode ser relatado ao Conselho Tutelar, Ministério Público ou Delegacia de Polícia mais próxima.
Sexting	É quando adolescentes e jovens trocam imagens de si mesmos (com pouca roupa ou nus) e mensagens de texto eróticas, com convites e brincadeiras sensuais entre namorados(as), pretendentes e/ou amigos(as). Ocorre quando fotos e vídeos são feitos com o uso de tecnologias (câmeras fotográficas, *webcam*, etc) e trocados através da Internet e de seus aparelhos celulares. O problema principal é que perde-se o controle de onde estes dados podem chegar, podendo até mesmo parar em *sites* no exterior, tornando muito difícil removê-los.	- Não se deixar levar pelos outros para produzir ou publicar imagens sensuais; - Preservar sua privacidade (nem tudo é para ser colocado na rede, pois nunca sabemos quem pode ter acesso e o que pode ser feito com o que publicamos); - Lembrar do fato de que se enviar uma foto íntima para alguém, ela pode parar nas mãos de estranhos;

Aliciamento de crianças e adolescentes	É quando uma pessoa adulta tenta seduzir, convencer e chantagear crianças ou adolescentes com o objetivo de marcar encontros, produzir imagens eróticas, sexuais e cometer abuso sexual infanto-juvenil *on-line* ou *off-line*. Ocorre quando adultos fingem ser crianças ou adolescentes, falando a mesma linguagem e dizendo coisas que interessam a garotos e garotas dessas faixas etárias.	- Não confiar: nunca se tem certeza de quem está por trás de um perfil, de um *e-mail* ou apelido; - Aliciadores são pessoas que fingem ser amáveis e fazem muitos elogios, para ganhar confiança e pedir informações que podem ser usadas contra você, portanto, não passar informações a estranhos; - Evitar usar a *webcam* com estranhos; - Não responder mensagens e convites de desconhecidos e gravar quando houver ameaça ou imagens violentas; - Bloquear o contato dos agressores no celular, *chat*, *e-mail* e redes sociais; - Jamais aceitar convite para encontrar presencialmente um amigo virtual sem autorização; - Pedir ajuda a um adulto de confiança para interromper este tipo de violência.
Roubo de dados e invasão	Utilizar de dados pessoais como senha, perfil, comunidade, personagem ou *e-mail* de um usuário sem a autorização ou consentimento para qualquer fim pode ser considerado crime. Se passar por outra pessoa na Internet para ofender e humilhar também é crime.	- Nunca abrir arquivos anexos de remetentes desconhecidos; - Não instalar programas que sejam enviados por desconhecidos; - Manter antivírus e *firewall* sempre atualizados; - Não acreditar em todas as informações que receber; - Não adicionar pessoas desconhecidas; - Denunciar ao próprio *site* quando houver perfis falsos e páginas que agridam outros usuários.

Quadro 9. Situações que podem ser encontradas na Internet
Fonte: Adaptado de CUNHA, J. & NEJM, R. Preocupado com o que acontece na internet: quer conversar? 2. ed. Salvador: SaferNet Brasil, 2012 e SAFERNET BRASIL. Saferdicas: Brincar, estudar e... Navegar com segurança na Internet! 5. ed. Salvador: SaferNet Brasil, 2013.

Além do que foi apresentado, outra ferramenta importante e à qual sempre pode-se recorrer, virtualmente ou não, é a denúncia. A denúncia é a principal arma para frear as atividades ilegais. Mesmo que as pessoas tenham dúvidas, devem procurar pessoas e organizações competentes que se incumbirão de fazer a devida apuração. Na Internet podem ser acessados os sites da Central de Denúncias de Crimes Cibernéticos www.denunciar.org.br e o do Ministério da Justiça www.mj.gov.br, que também aceita denúncias mediante envio de e-mail para *crime.Internet@dpf.gov.br* (Childhood, 2012).

Por fim, de acordo com o exposto nesta seção, conclui-se que além das medidas de segurança que os usuários devem utilizar, se faz necessário que os mesmos saibam comportar-se de maneira adequada virtualmente, considerando o fato de que estão tão e talvez até mais expostos a riscos do que no mundo real. Sendo assim, a melhor forma de proteção é uma combinação de fatores que foram apresentados ao longo deste trabalho: o conhecimento mínimo sobre o que são crimes digitais, de que forma acontecem e como a lei brasileira auxilia no caso da ocorrência dos mesmos, a utilização das boas técnicas de uso da Internet e demais dispositivos informáticos e a prática diária dos deveres que lhe são incumbidos.

4. Considerações finais

Segundo o historiador Rovira Del Canto, o conceito de crimes digitais já pôde ser percebido na década de 50, época denominada pelo mesmo de "Segunda Revolução Industrial", quando os computadores passaram a ser empregados na indústria e, em pouco tempo, já se tinha notícias de ações ilícitas com o uso dos mesmos. Assim, o *cyber* criminoso

está desde então aproveitando a oportunidade para o uso indevido do computador e utilizando uma ampla variedade de técnicas (HUNTON, 2011), que vêm sendo aprimoradas ao longo dos anos, também facilitadas pelo alto nível alcançado na tecnologia moderna.

Com os resultados obtidos é possível constatar que o problema dos crimes digitais tende a aumentar devido a fatores como a falta de cuidados dos usuários de tecnologias em geral, bem como, das técnicas utilizadas pelos cibercriminosos estarem se desenvolvendo cada vez mais. Além disso, ao longo do trabalho ficou claro que os crimes digitais geram grandes prejuízos na economia de diversos países e organizações e mais ainda, atingem a integridade das pessoas quando estas possuem seus dados acessados sem autorização e posteriormente violados. Por isso, a importância da segurança digital jamais deve ser questionada, e, além disso, esta deve ser considerada uma forte aliada no combate ao crime cibernético. Logicamente, o combate a esse tipo de crime é realizado conjuntamente através do uso das boas práticas, a legislação e à denúncia quando estes casos ocorrem.

Ainda, percebeu-se que a maior parte das ferramentas de segurança, segundo diversos autores pesquisados, não se faz eficaz quando os usuários das diversas tecnologias não fazem uso correto das mesmas, ou, até mesmo, nenhum uso. Por isso, além da disponibilidade de meios para proteção, é necessário que as pessoas se conscientizem da importância do uso diário destes meios. Aqui fica em evidência novamente a frase do famoso *hacker* Kevin Mitnick: "o ser humano é o elo mais fraco da segurança" e a colocação de Veloso (2012): *firewalls* de nova geração, criptografia, etc., são tecnologias que se tornam ineficazes quando um usuário mantém sua senha anotada embaixo do teclado, por exemplo.

Por fim, recomenda-se que este estudo tenha continuidade, considerando a amplitude do tema e, portanto, a dificuldade em completar uma série de lacunas. Além disso, o que também motiva o aprofundamento deste trabalho é a existência de uma preocupação generalizada referente aos crimes digitais. Esta preocupação se dá devido aos danos organizacionais, econômicos e morais que estes crimes causam quando ocorrem e aos quais todos que possuem contato com ambientes virtuais estão sujeitos.

Referências

ACPO. (2009). The Association of Chief Police Officers of England, Wales and Northern Ireland. A Estratégia de E-Crime.

AJALA, E. (2007). Cybercafes, Cybercrime Detection and Prevention. Library Hi Tech News, 7, 26-29.

AWE, J. (2004). Fighting cyber crime in nigeria, Guest Commentaries in the Nigerian Village. Square Forum.

BEATBULLYING. (2009). Virtual violence: protecting children from cyberbullying.

BRIAT, M. (1985). La fraude informatique: une approche de droit compare. Bruxelas, 4.

CASTRO, C. R. A. (2003). Crimes de Informática e seus Aspectos Processuais. 2. ed. Rio de Janeiro: Lumen Juris.

CHILDHOOD, Instituto. (2012). Navegar com segurança: por uma infância conectada e livre de violência sexual. 3. ed. São Paulo: CENPEC: WCF Brasil.

COUNCIL OF EUROPE. (2004). Summary of the Organized Crime Situation Report: Focus on the threat of Cybercrime [CoE Report, 2004].

CRESPO, M. X. F. (2011). Crimes digitais. São Paulo: Saraiva.

CUNHA, J. & NEJM, R. (2012) Preocupado com o que acontece na internet: quer conversar? 2. ed. Salvador: SaferNet Brasil.

DAY, K. (2003). Inside the Security Mind: Making Tough Decisions, Prentice-Hall, Upper Saddle River, NJ.

DEL CANTO, E.R. (2002). Delincuencia Informática y Fraudes Informáticos. Granada: Comares.

DONNER et. al. (2014). Low self-control and cybercrime: Exploring the utility of the general theory of crime beyond digital piracy. Journal Computers in Human Behavior.

EASTTOM, C. (2006). Computer Security Fundamentals, Prentice-Hall, Upper Saddle River, NJ.

FERRARI, B. (2013). A guerra está só no começo. Revista Exame, p. 127.

_____. (2013). No Brasil é fácil roubar dados. Revista Exame, p. 106, 19 de março de 2014.

FERREIRA, I. S. (2005). Direito & Internet: aspectos jurídicos relevantes. 2 ed. São Paulo: Quartier Latin.

GOUCHER, W. (2010). Being a cybercrime victim. Computer fraud and security.

GRECO FILHO, V. (2000). Algumas observações sobre o direito penal e a internet. Boletim do IBCCrim, São Paulo, ano 8, n. 95.

GUPTA, A. & HAMMOND, R. (2005). Information systems security issues and decisions for small businesses: an empirical examination. Information Management & Computer Security, v. 13, n. 4.

HILBERT, E.J. (2013). Living With Cybercrime. Journal Network Security.

HUNTON, P. (2009). The growing phenomenon of crime and the internet: a cybercrime execution and analysis model. Journal Computer Law & Security Review.

_____. (2011). A rigorous approach to formalising the technical investigation stages of cybercrime and criminality within a UK law enforcement environment. Journal Digital Investigation.

_____. (2011). The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation. Journal Computer Law and Security Review.

_____. (2012). Data attack of the cybercriminal: Investigating the digital currency of cybercrime. Journal Computer Law and Security Review.

INELLAS, G. C. Z. (2004). Crimes na Internet. São Paulo: Editora Juarez de Oliveira.

KATOS, V. & BENDAR, P. M. (2008). A cybercrime investigation framework. Journal Computer Standards and Interfaces, 30 (4), 223–228.

NETTO, A. V. (2006). Tipicidade penal e sociedade de risco. São Paulo: Quartier Latin.

NORTON-SYMANTEC. (2011). Cybercrime Report: The Human Impact.

PINHEIRO, R. C. (2000). Os cybercrimes na esfera jurídica brasileira. Jus Navigandi, Teresina, ano 5, n. 44, 1 ago. 2000. Disponível em: <http://jus.com.br/artigos/1830>. Acesso em: 16 abr. 2014.

PINHEIRO, P. P. (2010). Direito Digital. 4. ed. São Paulo: Saraiva.

RNEP. Segurança em Redes Sociais: recomendações gerais. (2011). CAIS/RNP, Rio de Janeiro, set. 2011. Disponível em <http://www.rnp.br/_arquivo/cais/Seguranca_em_Redes_Sociais.pdf>. Acesso em: 12 nov. 2014.

ROCHA, M. L. (1994). Direito da informática legislação e deontologia – Lisboa: ed. Cosmos.

RYAN, J.J.C.H. (2000). Information Security Practices and Experiences in Small Businesses, The George Washington University, Columbia, CA.

SAFERNET BRASIL. (2013). Saferdicas: Brincar, estudar e... Navegar com segurança na Internet! 5. ed. Salvador: SaferNet Brasil.

SIEBER, U. (1998). Legal aspects of computer-related crime in the information society – Comcrime Study. União Européia, Universidade de Wüerzburg.

SIENA, D. P. B. (2013). **Lei Carolina Dieckmann e a definição de "crimes virtuais"**. Jus Navigandi**,** Teresina, ano 18, n. 3652, 1 jul. 2013. Disponível em: <http://jus.com.br/artigos/24406>. Acesso em: 7 jan. 2015.

SYMANTEC. (2008). Symantec report on the underground economy. July 07 e June 08, Published November 2008. Symantec Corporation; 2008.
_____. (2009). Symantec global internet security threat report, trends for 2008, vol. XIV. Symantec Corporation; 2009. Published April 2009.
_____. (2010). State of enterprise security 2010. Symantec Corporation; 2010.

SZOR, P. (2005). The Art of Computer Virus Research and Defense, Symantec Press, Upper Saddle River, NJ.

VELOSO, M. (2012). Campanha de Conscientização. Revista Segurança Digital, ed. 009, p. 32-33.

VIANNA, T. L. (2003). Fundamentos de direito penal informático. Rio de Janeiro: Forense.

WALL, D.A. (2010). The internet as a conduit for criminal activity, In: Pattavina A., (Ed.), Information technology and the criminal justice system, sage; Thousand Oaks, CA, p. 77–98.