FACULDADES INTEGRADAS DE PONTA PORÃ

KAIC AUGUSTO ALVES BARBI

INVASÃO CIBERNÉTICA E PROCEDIMENTOS DE SEGURANÇA:

Lei 12.737/2012

Ponta Porã-MS
2017

KAIC AUGUSTO ALVES BARBI

INVASÃO CIBERNÉTICA E PROCEDIMENTOS DE SEGURANÇA:
Lei 12.737/2012

Trabalho de Conclusão apresentado à Banca Examinadora das Faculdades Integradas de Ponta Porã, como exigência parcial para obtenção do título de Bacharel emDireito.

Orientadora: Prof.ª MªDanyelle Bezerra Terhorst.

Ponta Porã-MS
2017

KAIC AUGUSTO ALVES BARBI

INVASÃO CIBERNÉTICA E PROCEDIMENTOS DE SEGURANÇA: Lei 12.737/2012

Trabalho de Conclusão apresentado à Banca Examinadora das Faculdades Integradas de Ponta Porã, como exigência parcial para obtenção do título de BacharelemDireito.

BANCA EXAMINADORA

_____

Orientadora: Prof.ª Mª Danyelle Bezerra Terhorst.
Faculdades Integradas de Ponta Porã

_____

Examinadora: Prof.ª MªLarissa SatieFuzishimaKomuro.
Faculdades Integradas de Ponta Porã

Ponta Porã, 11dedezembrode 2017.

Dedico este trabalho à minha família, por entender necessário todos os momentos que precisei me isolar para alcançar meus objetivos.

AGRADECIMENTOS

Agradeço primeiramente a Deus, por sempre estar ao meu lado, dando-me forças para continuar o meu percurso, bem como meaconselhando nas decisões que já tomei.

É com muita gratidão que tenho o orgulho de parabenizar a professora, orientadora e amigaDanyelle Bezerra Terhorst. Obrigado por confiar no meu trabalho e, principalmente, pelo apoio empenhado nos momentos que precisei.

Por fim, quero constar o reconhecimento que tenho pela instituição e pelos demais professores, pois foram imprescindíveis para a formação do meu aprendizado acadêmico.

ALVES, Kaic Augusto Barbi. **INVASÃO CIBERNÉTICA E PROCEDIMENTOS DE SEGURANÇA:** Lei nº 12.737/12. 48. Trabalho de Conclusão (Graduação em Direito) – Faculdades Integradas de Ponta Porã, Ponta Porã-MS, 2017.

RESUMO

Este trabalho tem como objetivo o estudo na interligação entre a ciência do direito e a do ramo informático, com enfoque nos casos de invasão cibernética, amparada pela Lei nº 12.737/12. Visa-se conscientizar o leitor das possibilidades violadoras que possam ocorrer no usocotidiano do maquinário, dando-lhes o entendimento simples e necessário quanto ao modo correto de manusear os dispositivos eletrônicos, maneiras de evitar agressões de terceiros nessa área, bem como os procedimentos adequados a serem realizados caso se torne vítima. O critério qualitativo foi aplicado para buscar uma compreensão mais pormenorizada do que vem a ser os crimes cibernéticos, dando sua descrição e relevância para a atualidade. Ainda assim, a característica bibliográfica foi escolhida para colher informações já desenvolvidas em fontes variadas, como doutrinas, leis, revistas e informações hospedadas na Internet, com o fim de alcançar a produção adequada de dados para a realização da presente pesquisa.

Palavras-chave: Crimes Cibernéticos. Cibercrimes.Crimes Informáticos. Crimes Eletrônicos. Invasão Cibernética.

ALVES, KaicAugusto Barbi. **INVASIÓN CIBERNÉTICA Y PROCEDIMIENTOS DE SEGURIDAD:** Lei nº 12.737/12. 48. Trabalho de Conclusão (Graduação em Direito) – Faculdades Integradas de Ponta Porã, Ponta Porã-MS, 2017.

RESUMEN

Este trabajotiene como objetivo elestudioenlainterconexión entre lacienciadelderecho y ladel ramo informático, con enfoque enlos casos de invasión cibernética, amparada por laLey nº 12.737/12. Se pretende concientizar al lector de lasposibilidades violadoras que puedanocurrirenel uso cotidiano de la maquinaria, dándoleselentendimientosimple y necesarioencuanto al modo correcto de manejar los dispositivos electrónicos, maneras de evitar agresiones de tercerosenesa área, así como losprocedimientosadecuados a ser realizados en caso de ser víctima. El criteriocualitativofue aplicado para buscar una comprensión más detallada de lo que viene a ser loscrímenes cibernéticos, dando sudescripción y relevancia para laactualidad. Sin embargo, la característica bibliográfica fue elegida para recogerinformacionesyadesarrolladasenfuentes variadas, como doctrinas, leyes, revistas e informaciones hospedadas en Internet, conelfin de alcanzarlaproducciónadecuada de datos para larealización de la presente investigación.

Palabras-clave: Crímenes Cibernéticos. Cibercrimes. Crímenes Informáticos. Crímenes Electrónicos. Invasión Cibernética.

SUMÁRIO

INTRODUÇÃO

Indiscutível que atualmente a Internet é conhecida como um dos maiores meios para obter informações, assim como forma de contato virtual, dada sua praticidade e acessibilidade que possui, cuja finalidade abrange diversas funções, sendo usada, pela maioria, tanto no trabalho, estudos e relacionamentos em geral. Em consequência disso, a utilização descontrolada gera um amplo risco à privacidade dos usuários, podendo se tornar vítimas das mais variadas possibilidades de violações.

Além disso, percebe-se que os estudos de riscos no uso do campo cibernético vêm crescendo com o passar dos dias e isso pode-se notar com a demanda de ações visando o amparo frente a algum dano causado por terceiros, como é o caso daqueles que foram prejudicados por algum invasor. Ainda assim, mesmo com números elevados de ocorrências sobre o assunto, a legislação vigente e também as ferramentas existentes ainda não conseguiram acompanhar a evolução dos agentes maléficos.

Desde logo, justifica-se a necessidade de harmonizarmos com a evolução informática para não sermos reféns de todos os tipos de arquivos e programas que possuam a finalidade de acessar indevidamente nossos dados ou de outrem. Portanto, o presente trabalho proporcionará o amparo jurídico e informático sobre os delitos virtuais, abrangendo de forma clara e simples, para que, independente de qual for o grau de ensino do leitor, o entendimento seja alcançado.

A essência deste trabalho visa, como objetivo,demonstrar à sociedade, usuária dos meios informáticos, os riscos que as invasões cibernéticas podem causar, bem como indicar maneiras de prevenções a esses ataques. Importante frisar que, para que tal conhecimento seja obtido, necessário se faz o aprendizado quanto a origem dos crimes cibernéticos, analisando sua abordagem frente a legislação brasileira e ilustrando a impactante impunidade diante da dificuldade de identificar a autoria delitiva, possuindo como um dos meios, a abordagem de prevenções a essas manobras virtuais.

Para que tal fim almejado seja atingido, como metodologia adotada, serão extraídas informações de doutrinas, revistas, artigos e periódicos científicos, como fontes para embasamento. Ademais, imprescindível a menção das principais

legislações vigentes que abordam os crimes informáticos, para que possa ser colhido dados com a maior riqueza de detalhes possíveis.

O trabalho foi desenvolvido em quatro capítulos, em busca de descrever o surgimento dos crimes cibernéticos, seus riscos e formas de repreensão. Será mencionado com maior enfoque os delitos que caracterizam pela violação de dados, como é o caso do amparo legislativo conforme a Lei nº 12.737/2012.

No primeiro capítulo será apresentado a origem dos crimes cibernéticos, desde as primeiras utilizações do computador, como também o surgimento da Internet como forma de acelerar as atividades exercidas nesta máquina. Também trará diferenciações do que vem a ser “*hardware*” e “*software*”, principais *softwares* maliciosos, em que provocaram os legisladores, mencionando, ainda, acerca dos arquivos que são salvos em rede computacional.

Em sequência, o segundo capítulo abordará as principais legislações pátrias acerca da invasão indevida de dados, mostrando ao leitor o atual apoio estatal.

Já o terceiro capítulo alertará a impunidade frequente, em razão da dificuldade em identificar o autor do delito ocasionado, dada a falta de mecanismos adequados para combater tais condutas.

Por fim, o quarto tópico acobertará ensinos quanto aos modos corretos de uso dos aparelhos eletrônicos, visando facilitar ao máximo, de forma simplificada, a leitura dos itens que serão aqui transcorridos.

CAPÍTULO I

1.ORIGEM DOS CRIMES CIBERNÉTICOS E A INFORMÁTICA

1.1 ORIGEM E RELAÇÃO DO MEIO INFORMÁTICO COM A INTERNET

Antigamente o acesso a informática era algo restrito a determinadas classes de pessoas, visto que o seu uso só ganhou destaque no início da segunda grande guerra mundial, em que a tecnologia era utilizada para facilitar o modo operacional dos militares, tanto em campo de batalha, como também para prevenir possíveis ataques. Nessa época foi o momento em que as máquinas ganharam grande evolução e marco histórico, sendo um período impulsor para novas buscas em instigar o crescimento tecnológico (CAZELATTO; SEGATTO, 2014, p. 390).

Por sua vez, ao passo que as evoluções das máquinas cresciam, surgiu a necessidade de uma interligação entre elas para facilitar a troca de informações visando oalcance de poder, conhecimento e campos de pesquisas. Isso fez com que o homem buscasse meios para facilitar ainda mais suas atividades, dando-se a ideia da criação da Internet (CAZELATTO; SEGATTO, 2014, p. 391).

Foi em 1962, com a Guerra Fria, que ao se depararem com os ataques em seus sistemas de dados, o governo norte-americano deu origem ao que chamamos hoje de Internet. Com isso, buscou-se também as primeiras ferramentas de amparo ao meio informático, dado que até então não se tinham alternativas para garantir o acesso seguro a informações.

David Augusto Fernandes nesse mesmo sentido esclarece que:

> No período da guerra fria, mais especificamente durante o ano de 1962, pesquisadores americanos começaram a imaginar um sistema imune a ataques aéreos, que fosse capaz de interligar muitos computadores, permitindo o compartilhamento de dados entre eles. Passados sete anos, a primeira versão desse sistema ficou pronta, recebendo a denominação de AdvancedResearchProjectsAgency ou Agência de Projetos de Pesquisa Avançada (ARPAnet). Sua principal característica era não possuir um comando central, de modo que, em caso de destruição de um ou mais computadores, todos os outros equipamentos ligados ao sistema continuariam operando (FERNANDES,2013, p. 140).

Já em 1969, estabeleceram o denominado padrão TCP/IP, criado pela ARPANET, que caracteriza a Internet como sendo o aglomerado de redes que se interligam, que diante dessa situação trocam e acessam dados e até mesmo a utilizam como forma de facilitar o modo de comunicação, independente do país em que o usuário se encontre (MADALENA, 2013, p. 103).

Apesar de conversas a respeito do assunto já circularem pelos estudiosos, precisamente a Internet só veio a nascer nos anos de 1980, o qual a definiram como sendo vários computadores que se comunicam pelo mundo inteiro, possuindo protocolos de identificação e até mesmo serviços. Conceito este que foi se aperfeiçoando com o decorrer do tempo(FERNANDES, 2013, p. 142).

Oportuno destacar que, desde os primórdios de sua implantação, a informática cada vez mais vem ganhando espaço no cotidiano da sociedade em comum, tornando-se, atualmente, um dos maiores meios de comunicação, dada a sua praticidade e agilidade em seu manuseio, cuja finalidade abrange diversas funções, sendo usada, pela maioria, tanto no trabalho, estudos e relacionamentos em geral. Em contrapartida, a utilização descontrolada gera um amplo risco para a proteção da privacidade dos usuários, podendo se tornar vítimas das mais variadas possibilidades de violações.

No decorrer dos anos, com a evolução informática, o conjunto dessas ideias passaram a serem usadas no meio dos centros universitários, tal como na América do Norte e, posteriormente, para o restante dos países. Destaca-se que no período de 1990 foi que se deu o conhecimento do desenvolvimento de redes, dada a criação da *worlwide web* conhecida por nós como as iniciais de um site – www, sendo uma considerável reunião de informações, na identificação de mídia ou mesmo na forma de texto, vale dizer, arquivos de texto, fotos, imagens, bem como vídeos, estrategicamente explorados com a intenção de que o usuário consiga “navegar” dentro da página desejada, através dos denominados URL, isto é, localização universal de registro ou até mesmo por numerações de endereços de IP – *Internet Protocol*, o que exigirá um pouco mais de conhecimento daquele que acessa o site desejado (FERNANDES, 2013, p. 141).

Foi no ano de 1995, com a autorização do Ministério de Comunicações e de Ciência e Tecnologia, que foi liberado o comércio, por meio da participação da

RNP – Rede Nacional de Ensino e Pesquisa[1], bem como, mais a diante, com a intervenção também da Embratel. Já a parte burocrática, propriamente dita, foi realizada pelo Comitê Gestor da Internet, o qual deu iniciativa a uma Portaria Interministerial, buscando iniciativas no trabalho brasileiro interligado a Internet para agregar as inovações tecnológicas do país.

Com o acesso facilitado à população, grandes ideias passaram a surgir, possibilitando o controle estatal, divulgações de informações que antes não eram possíveis de maneira imediata e até mesmo a fiscalização no que diz respeito à política de cada país. Isso preocupou de forma significativa àqueles que antes infringiam a moral da sociedade, pois, após esse momento, o que antes era feito "por baixo dos tapetes", passou a ser rigorosamente visto por outros, causando um pressionamento para evitar condutas imorais.

Variados meios possibilitaram a troca de dados entre os usuários, como, por exemplo, os correios eletrônicos (conhecidos como e-mail) e as redes sociais. Tudo no começo parecia uma maravilha, porém, como para a existência do bem, também se tem o mal, aqui não seria diferente, visto que, com o uso descontrolado desses meios, pessoas com intenções malévolas passaram a estudar e acompanhar o assunto, visando sempre um proveito indevido próprio ou mesmo apenas para prejudicar outrem.

> Antes da popularização da internet as práticas consistiam em telefonemas, cartas, visitas indesejáveis, entre outras atitudes mais físicas. Ocorre que quando a internet eclodiu no cotidiano tudo ficou mais fácil para os perseguidores, já que poderiam acompanhar a vida da vítima na hora que bem entendessem e sem se preocupar em sua identidade ser descoberta (PACHECO, 2016, p. 243).

Foi assim que, com a evolução da informática e da Internet, obrigou-se também o desenvolvimento protetivo dos usuários, pois não bastava disponibilizar o acesso às benesses tecnológicas, também era preciso garantir que esse acesso fosse seguro, impossibilitando a violação de dados por terceiros.

Percebe-se, com isso, que o meio em estudo transgrediu para uma análise mais individualizada, conforme passou a buscar a satisfação de interesses pessoais e não mais apenas coletivos. Dessa forma, tanto os aparelhos

[1]RPN REDE NACIONAL DE ENSINO E PESQUISA. Nossa história. Disponível em: < https://www.rnp.br/institucional/nossa-historia >. Acesso em: 15 nov. 2017.

informáticos, bem como os meios de manuseá-los virtualmente passaram a serem mais especificados para cada fim que o usuário quisesse cumprir.

Com a entrada do ano 2000, o que antes era manuseado apenas por aparelhos de mesa, passou a ser executada tarefas por ferramentas diversas, com dimensão física menor, mas, em compensação, sua velocidade de transformar dados em material lógico passou a ser incrivelmente muito maior, porque é neste século que o investimento nessa seara passou a ser ainda mais aplicado. Pode-se constatar com a presença de tablets, celulares, os quais possuem variadas utilidades.

1.2DEFINIÇÃO DE HARDWARE E SOFTWARE

Antes mesmo de apresentar conceitos e definições do que vem a ser o estudo em tela, necessário saber como é que tudo começou para que seja adquirida uma melhor compreensão do assunto. Dessa forma, aprender o porquê de as coisas funcionarem do jeito que estão é uma tarefa imprescindível.

Em um primeiro momento, o estudo sobre máquinas era investido pelo Estado para melhorias nos fins de evolução acadêmica de seu país, assim como para melhor equipar os serviços prestados pelas forças armadas. Tal período ficou registrado pela presença de computadores com enormes dimensões, que em alguns casos ocupavam até uma sala inteira e seu uso apenas era possível por especialistas na área, dada a dificuldade de entender como os procedimentos de manuseio naquela época era realizado (CAZELATTO; SEGATTO, 2014, p. 390).

Como se não bastasse a problemática diante do tamanho e dificuldade de uso, outro aspecto era o valor cobrado por tais aparelhos, os quais tinham um preço absurdo, restringindo a aquisição pela maioria da população. Em 1969 o sistema utilizado era, em destaque, o UNIX, o qual fora aprimorado pela *AT&T Corporation – American TelephoneandTelegraph*[2], conhecida por ser uma das mais antigas companhias de telecomunicação, cuja sede é localizada em Dallas, nos Estados Unidos da América.

[2]The New York Times. AT&T’s History of Invention and Breakups. Disponível em: < https://www.nytimes.com/interactive/2016/02/12/technology/att-history.html >. Acesso em: 15 nov. 2017.

Para solucionar a barreira que estava levantada, foi-se necessário a criação de dispositivos que possibilitassem o uso pela sociedade que não detinha especialização na área eletrônica, pois o intuito principal de *marketing* era a comercialização para a maior quantidade possível de pessoas e, para que isso acontecesse, mister se faz o acesso facilitado, prático e rápido por qualquer que seja aquele que está manuseando. O êxito para essa ideologia se deu quando dois jovens estudiosos se empenharam, em torno de 1970, no desenvolvimento tecnológico, sejam eles Steve Jobs e Steve Wozniak, dois grandes nomes marcados nesse ramo, em que depois deram criação à máquina que ficou conhecida como Apple (CAPELAS, 2014).

O computador Apple era integrado por *hardware* e *software*, cuja influência se deu pelo sistema UNIX, já mencionado. Seu intuito era proporcionar segurança, velocidade e praticidade em seu uso, caracterizando não apenas como meio de trabalho, mas também como uso doméstico (MORIMOTO, 2009).

Questiona-se, então, o que de fato vem a ser *software* ou*hardware*, tais palavras acabam pouco sendo usadas nas conversas diárias da sociedade em comum, tendo em vista o desconhecimento do seu real significado. Ora, a definição dessas nomenclaturas, pelo contrário do que muitos imaginam, é mais simples do que aparenta.

As máquinas, os aparelhos, os equipamentose os dispositivos são exemplos de *hardware*, e, se formos caracterizar de forma simples e didática, todo compartimento tocável, físico, cuja finalidade destina-se a desempenhar atividades tecnológicas poderão ter a mesma consideração, via de regra. Dessa forma, um computador é considerado um *hardware*, mas, para que ele tenha efetivo funcionamento, é necessário que seja integrado sistemas lógicos, pois o aparelho é apenas uma ferramenta, o qual sem um *software* adequado acaba perdendo variadas utilidades que poderá ter como desempenho (BRAGA; ALECRIM, 2010).

Entende-se por *software* a parte lógica que está sendo usada em um aparelho informático, sendo um meio inteligente de conduzir as intenções que pretendemos atingir (BRAGA; ALECRIM, 2010).Isso pode ser bem visto ao lembrarmos dos sistemas operacionais e dos programasque usamos em *smartphones*, máquinas fotográficas e até mesmo a parte eletrônica do painel de um veículo.

Consequentemente outras empresas começaram a fabricar computadores, dada a clientela que cada vez mais vinha a crescer. Todavia, diferentemente da Apple que já continha um aparelho completo (*hardware* e *software)*, precisaram providenciar um sistema operacional para fazer parte de suas máquinas e estas funcionarem.

Oportunidade na qual Bill Gates e Paul Allen ganharam destaque ao fornecerem um *software* para “dar vida” aos computadores que seriam fabricados por empresas diversas da Apple. Portanto, criaram a empresa Microsoft Corporation, em que sua maior intenção era dominar o setor de vendas de todos os computadores do mercado com o seu sistema operacional (PERON, 2009).

Com o passar dos anos, os usuários perceberam que uma exigência os seguiam, isto é, para que pudessem adquirir computadores e executar atividades de desempenho, necessariamente precisavam comprar o sistema operacional da Microsoft, como se fosse uma compra em conjunto, caso não preferissem obter os disponíveis da Apple. Foi a partir desse momento que começaram a serem desenvolvidos os *softwares* livres, cuja aquisição independeria de pagamento, visto que os usuários poderiam não apenas usufruir de seus benefícios sem precisar pagar nada, mas também teriam o poderio de distribuir cópias desse sistema operacional para terceiros interessados e até mesmo modificar suas funcionalidades, adequando ao gosto do freguês ou mesmo às suas necessidades (CAMPOS, 2006).

Marcado maior relevância no começo do ano de 1980, Richard Matthew Stallman (apelidado por rms) foi o grande incentivador e impulsor do movimento que garantia acesso gratuito a sistemas operacionais, o então denominado General PublicLicense, muito conhecido também pelas siglas GNU e GPL, tratando-se da licença gratuita que passou a ser a mais utilizada pelos usuários. Dessa forma, surgiu uma distinção de sistemas operacionais, em que os com código fonte privado foram classificados como *copyright*, enquanto que os com código fonte livre identificados como *copyleft*(KUSZKA, 2013).

Em 1991, um estudioso chamado Linus Torvalds percebeu que o GNU poderia ser aperfeiçoado, instante em que resolveu realizar mudanças nesse sistema operacional, já que sua fonte é livre e possui permissão para alterá-lo. Instante no qual percebeu que o programa possui como se fosse um núcleo,

imutável, chamado de *Kernel* e o utilizou para criar o nomeado Linux (GNU/Linux), desenvolvido com vestígios do antigo GNU (SALES, 2016).

Atualmente o mercado é dominado pela empresa Microsoft, a qual possui o sistema operacional chamado Windows – código fonte fechado, mas também há parcela numerosa quanto ao sistema operacional macOS, que é desenvolvido pela Apple e seu uso é maior percebido no comércio de *smartphone* (celular com funções superior aos comuns), iPod, iPad e o famoso iPhone. Já quanto ao GNU/Linux, apesar de embarcar uma porcentagem muito menor de clientes do que o Windows, seu uso vem ganhando espaço cada vez mais, dado o acesso livre, em que o usuário pode acessá-lo sem se preocupar com a cobrança para o seu manuseio, bem como pelo modo de visão que se tem sobre seu sistema, permitindo aprimoramentos para adequar o modo de operação de cada usufruidor (NASCIMENTO, 2015).

1.3SOFTWARES MALICIOSOS E OS CRIMES CIBERNÉTICOS

Identificado como sendo uma situação que está ganhando espaço nesteséculo, é necessário realizar uma compreensão pormenorizada do que vem a ser os crimes cibernéticos, dando sua descrição, relevância e aplicação no cotidiano comum de toda a sociedade usuária dos meios informáticos. Com isso, o levantamento acerca dos fatos já conhecidos visa aprimorar pesquisas com o reconhecimento do problema presente, seja pela impunidade dos infratores neste campo, seja pela falta de investimento em tal área.

Observa-se que, por se tratar de um caso classificado como complexo pela maioria das pessoas, o funcionamento adequado dos meios tecnológicos proporcionará não só a agilidade das tarefas neles empenhadas, mas também a garantia da integridade do conteúdo que ali está sendo trabalhado.

Sabe-se que crimes, tanto no meio comum, quanto os virtuais, são ações reprováveis, o que se questiona por alguns é qual seria o objeto violado nos casos mais diários acontecidos no meio eletrônico. Em suma, quatro critérios da segurança da informação podem serem violados, quais sejam: a) autenticidade - confirmação de identidade inapropriada por outrem; b) integralidade -dados de determinado arquivo alterado por terceiro não autorizado; c) disponibilidade -neste item o ataque se dá pela quebra de acesso ao conteúdo que estava disponível; e, por fim, o critério

d) confidencialidade -visto como sendo o segredo vasado, pois o que antes era restrito, passa a tornar público indevidamente (FREITAS, 2017).

Os meios atacados acima mencionados não são empenhados por *hackers*, mas sim por *crackers*, sendo a denominação correta e que deve ser utilizada. Isso é diferenciado, pois, ao contrário do que muitos pensam, o *hacker* é o sujeito que tem autorização para percorrer o meio virtual (muito comum em empresas que testam sua área de segurança com ataques intencionais), enquanto que o *cracker* não, agindo sorrateiramente, sem permissão de uso (facilmente identificado nos casos de furto de senhas, cartões de crédito ou mesmo em situações de espionagem) (ARIMURA, 2016).

Os crimes informáticos podem ocorrer por meio de engenharia social, bem como por força bruta. Esta é percebida pela presença da efetiva força humana, em que certa pessoa obtém o acesso a algum conteúdo por meio de, geralmente, um crime - como é o caso de um furto de celular, enquanto que aquele é o mais extenso, visto que se logra mediante o meio virtual, o qual com o passar dos anos a criação de espécies maliciosas (*malwares*) vem crescendo cada vez mais.

Pois bem. Conveniente tecer sobre uma categoria comumente presente nos dias atuais, que é o *Spam*, caracterizado como sendo um conteúdo indesejado que é enviado no e-mail do destinatário, sobrecarregando a caixa de mensagens do usuário, cujo fim se destina a prolatar anúncios, ora comerciais, industriais, gerenciais, ora imorais, como também conteúdos pornográficos ou até mesmo fraudulentos. Sua identificação se dá por ser algo que o destinatário sequer solicitou, mas mesmo assim o recebe em seu correio eletrônico determinada mensagem que muitas das vezes pode causar algum dano patrimonial ou até mesmo moral (WENDT, 2011, p. 36).

Outra modalidade de *software* malicioso é o *Phishing*, palavra socialmente conhecida como sendo uma “pescaria”, dado que ilude o usuário a realizar procedimentos que acreditava estarem corretos, como no caso de acesso de uma página famosa, mas que, por sua vez, não passava de um “clone”, uma falsa máscara para enganar pessoas desatentas. A vítima, acreditando que está usando de um site seguro, acaba preenchendo seus dados pessoais, causando ulterior dano e beneficiando o autor do delito (COLLI, 2010, p. 69).

Há também o invasor que usa programas interativos como meio de crimes, como no caso de jogos, em que o infrator agrega a um arquivo lícito algum

outro conteúdo ilícito, infectando o computador do usuário vulnerável. Esse é famoso *Trojan Horse*, traduzido pela língua brasileira como Cavalo de Tróia, pois é um falso presente, cujo interior é “recheado de surpresas mal-intencionadas” (VIANNA; MACHADO, 2013, p. 66).

Outra hipótese é o *Spyware*, muito exemplificado nos cinemas norte-americanos, tratando-se de um arquivo espião controlado por outrem que atua em segundo plano para descobrir quais atividades o usuário fim está executando, conseguindo, assim, senhas e informações que, em um primeiro momento, eram sigilosas. Diferencia-se do *malware* anterior por não ser visível, já o *Trojan Horse*, mesmo sendo um poderoso ataque, pode ser perceptível pelo usuário que está sendo atacado (XAVIER, 2008).

Ótimo momento para já descrever uma subcategoria de *Trojan Horse*, que é o *Ransomware*, espécie de *software* malicioso que vem ganhando destaque nos dias hodiernos, pois é um sequestrador virtual que viola dispositivos eletrônicos e obtém arquivos de vítimas, com o intento de cobrá-las algum proveito, seja dinheiro ou mesmo favores. A categoria em questão é destacada, porque o seu uso cada vez mais está interessando os criminosos, sendo uma forma de apanhar ilegalmente quantias consideráveis de vantagens ilícitas (ALECRIM, 2016).

O Vírus, em rumo diverso do que a maioria imagina, não é todo arquivo malicioso, e sim caracterizada como sendo uma espécie de *malware*, por isso que não podemos dizer que sempre que nosso computador está infectado é em razão de Vírus, sendo apenas uma das variadas modalidades de delito virtual (VIANNA; MACHADO, 2013, p. 34). Ainda assim, mesmo sendo uma espécie de *software* malicioso, também possui seus desmembramentos, podendo ser identificado por diversas ocorrências, como são, dentre outras, as hipóteses de Vírus que atacam em datas específicas, geralmente comemorativas, e o Vírus de *Boot*, marcados pelas agressões provocadas logo no início do funcionamento da máquina.

Chega a ser surpreendente a criatividade maliciosa atual, pois como se não fosse suficiente os casos explanados, surge o *BlendedThreats*, ataques simultâneos altamente massivos, integrado pela junção dos *malwaresTrojan Hourse, Spyware* e Vírus de aplicativo. Seu modo de atuação é presenciado pela a execução de um primeiro programa comum, em que ações escondidas são ativadas e, em “efeito dominó”, ativam as outras ilícitas, causando danos maiores do que um simples aplicativo malicioso poderia acarretar.

É evidente que existem inúmeros outros casos de arquivos mal-intencionados, até porquê a cada dia o trabalho ilegal vem ganhando destaque, aperfeiçoando-se. O objetivo deste tópico foi apresentar os casos mais comuns, que a maioria das pessoas ao menos já em algum momento ouviram falar, pois, caso fosse discorrer sobre a maioria dos *malwares*, seria necessário a edição de um livro específico a respeito do assunto, dado o volume de hipóteses e em razão da engenhosidade criminosa que cresce com o passar dos anos. Assim, como meio educacional, bastam os exemplos acima expostos, não impedindo o leitor de ganhar conhecimentos buscando novas áreas do saber.

CAPÍTULO II

2 - ABORDAGENS NA LEGISLAÇÃO BRASILEIRA ACERCA DA INVASÃO INDEVIDA DE DADOS

2.1 LEI DE CRIMES CIBERNÉTICOS - 12.737/2012

Como a publicidade possui enorme força quando ligada a Internet, fica fácil identificar casos em que pessoas que utilizam tais recursos acabam se tornando vítimas, ora pela falta de informação quanto aos meios de prevenções, ora pelo descuido ao acreditar que jamais serão atacadas.

O acesso informático possibilita, ainda, meios mais solenes de colher informações quanto as hipóteses verídicas de crimes cibernéticos já ocorridos. Percebe-se nas hipóteses de comunicações às delegacias, em que são gerados boletins de ocorrências quando vítimas acabam sendo atingidas de forma significativa, perdendo parte de seu patrimônio ou até mesmo tendo sua privacidade violada.

Caso semelhante foi o da atriz Carolina Dieckmann, em que a partir de tal fato o legislador foi provocado a criar a Lei nº. 12.737/12[3], passando a amparar, ainda que de forma substancial, parcela dos crimes que ocorrem no meio virtual.

Carolina foi vítima de ataques de *Crackers*, sendo quatro suspeitos responsáveis pela conduta delitiva, em que estes alegaram que invadiram seu correio eletrônico. Sabe-se, ainda, que foi enviado um *software* mal-intencionado para a conta de e-mail de Carolina. Momento em que ela clicou no e-mail malicioso, infectando sua máquina e possibilitando que os meliantes obtivessem seus dados particulares (LISBOA, 2013).

A autoria criminosa, no caso em comento, foi encontrada por meio do número de identidade da máquina dos violadores, o qual, em termos técnicos, é chamado de IP – *Internet Protocol*. Foi graças a esse meio que os agentes policiais lograram êxito no encalço delitivo, dado que os crimes informáticos, em regra,

[3] _____.Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm> Acesso em nov. de 2017.

deixam rastros, vestígios de todas as atividades executadas pelo usuário do dispositivo (CANDIDO, 2012).

Diante do receio ao utilizar a informática, em razão dos ataques maliciosos provocados por terceiros, foi-se necessário a criação de determinadas legislações específicas acerca do tema com o intuito de quebrar a sensação de impunidade que estava sendo estabelecida.

Ainda assim, apesar de existirem pouquíssimas normas com o intuito de combater o acesso indevido de dados, estamos diante de uma mora legislativa, dado que, pela criação de novos tipos de arquivos maléficos crescendo cada vez mais, não há o acompanhamento na elaboração de novas leis visando combater tais delitos, o que acaba surgindo a oportunidade de burlar a rede de dados dos servidores computacionais.

Com a entrada em vigor da Lei nº 12.737/2012 ocorreu a mutação no atual Código Penal Brasileiro, acrescendo dois artigos que trouxe, como ponto inicial, a legislação diante dos crimes cibernéticos. São eles os artigos 154-A e 154-B, os quais dispõem o seguinte:

> **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 obtidos.
> § 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.
> **Ação penal**
> Art. 154-B. Nos crimes definidos no art. 154-A, **somente se procede mediante representação**, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.[4](Grifei)

O objeto protegido pela norma em análise são tanto os arquivos armazenados em determinado dispositivo, bem como a forma de garantir a sua proteção, evitando que seja implantada alguma espécie de programa julgado como prejudicial ou mesmo que tenha funcionalidade parasita.

Além disso, essa inovação se deu com respaldo no artigo 5º, inciso X, da atual Carta Magna[5], que protege os direitos imprescindíveis quanto a intimidade, visão moral social sobre as pessoas, merecimento e, se porventura for violado, amparará a vítima mediante indenização. Por essa razão que a essa Constituição, ao mesmo tempo que libera o direito de qualquer indivíduo se expressar, também o obriga a se identificar, posto que assim poderá amparar eventual dano causado.

Antes mesmo de analisar os sujeitos delitivos, precioso ilustrar os conceitos destes para que àqueles que não são da área jurídica possam entender do que se está falando. Sendo assim, vejamos:

> **Sujeito ativo** do crime é a pessoa que pratica a infração penal. Qualquer pessoa física capaz e com 18 (dezoito) anos completos pode ser sujeito ativo de crime (p. 153)
> O **sujeito passivo** é a pessoa ou ente que sofre as consequências da infração penal. Pode figurar como sujeito passivo qualquer pessoa física ou jurídica, ou mesmo ente indeterminado, destituído de personalidade jurídica (ex: coletividade, família, etc.), caso em que o crime é chamado pela doutrina de vago (CUNHA, 2016).

---

[4] _____. Código Penal - Decreto-lei 2848/40 | Decreto-lei no 2.848, de 7 de dezembro de 1940. Disponível em: <http://www2.camara.leg.br/legin/fed/declei/1940-1949/decreto-lei-2848-7-dezembro-1940-412868-publicacaooriginal-1-pe.html> acessado em nov. 2017.

[5] BRASIL, Constituição da República Federativa do Brasil (1988). Disponível em <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm> Acesso em nov. de 2017.

Nesse delito, o sujeito ativo é comum, vale dizer, qualquer pessoa pode ser um violador de dados, não necessitando de nenhuma característica especial. Logicamente, o proprietário dos arquivos fica obstado de se enquadrar como sujeito ativo, dado que ele tem permissão para acessar os conteúdos hospedados, por se tratar de material que lhe pertence.

Túlio Vianna e Felipe Machado (2013, p. 95)ensinam ainda que haverá sim a possibilidade da esposa ou mesmo o marido configurarem como sujeitos ativos do delito em questão quando um acessar qualquer aparelho informático do outro sem permissão anterior, pois o casamento não dá,de forma implícita, o direito de nenhuma das partes revirar as informações do seu cônjuge. Assim, independentemente de realizado ou não o casamento, os direitos de qualquer cidadão devem ser respeitados.

Em outro ângulo, identifica-se que o sujeito passivo, isto é, a vítima, poderá ser também qualquer indivíduo - pessoa física - ou até mesmo jurídica, detentora de propriedades intelectuais e virtuais.

As condutas incriminadoras da lei em estudo são identificadas pela quebra da uma barreira a qual tinha a função de proteger as informações da vítima, obtendo indevidamente seus dados, pois em momento algum possuía autorização para manuseá-los. Outrossim, poderá, também, ser identificada pela implantação, pelo sujeito ativo, de vulnerabilidades na máquina do sujeito passivo, ou seja, aquele que detém algum dispositivo eletrônico.

Vale salientar que o artigo 154-A, do Código Penal Brasileiro deixa claro que não importa se o aparelho afetado estava ou não conectado a uma rede, seja ela interna ou mesmo externa, pois o que é visado na norma é a proteção do conteúdo privado, sendo esses pontos irrelevantes para a configuração do delito. Dessa forma, caso ocorra condutas como essas mencionadas, o delito estará, em regra, completo.

Identifica-se, ainda, que há falha na Lei nº 12.737/2012 ao exigir, em seu artigo 154-A, *caput*, acrescentado no Código Penal, como requisito obrigatório que para a configuração do delito previsto é preciso que o dispositivo contenha um mecanismo de segurança, sendo que estaproteçãodeverá ser violada pelo infrator. Vale dizer, é elementar do tipo que no meio de execução seja vencido o meio de segurança do aparelho informático. Ora, a legislação é retrocedente nesse aspecto, dado que ninguém pode obter informações sigilosas ou mesmo

particulares(pertences tecnológicos) sem antes possuir a permissão do dono, independentemente se nele conter ou não programas de segurança.

Em regra, a configuração do artigo 154-A, *caput,* só terá seguimento mediante uma condição de procedibilidade, que é a representação da vítima, dada a previsão legal no artigo 154-B. Já o parágrafo primeiro, da mesma norma, pune quem comercializa os programas que tem como finalidade a obtenção indevida de dados de outrem, isto é, *softwares* maliciosos que são criados para acessar outra máquina.

Contudo, indaga-se quem seria a vítima desse parágrafo primeiro, pois, ao contrário do ilustrado no *caput*do artigo 154-A, em que a vítima é quem está sofrendo a agressão cibernética, no seu parágrafo primeiro não se tem vítima se não for violado direito de terceiros. Percebe-se, então, a falha na legislação, visto que o parágrafo em questão está caracterizado como vítima indeterminada, pois, se não existe vítima certa ficará inviável sua representação e procedibilidade da ação.

Os demais parágrafos do artigo 154-A tratam de situações mais graves, em que será aplicado a agravante prevista ou mesmo modalidade de aumento de pena, a depender do caso.

Apesar da fabricação dos artigos comentados, suas aplicabilidades não abordam boa parte dos delitos atualmente existentes, que,por sua vez, acabam ocasionando os mais diversos prejuízos àqueles que são afetados. Desde logo a situação do meio virtual é visualizada como crítica, pois não basta garantir que toda a população tenha acesso à tecnologia, mister também que a seja segura.

2.2PREVISÃO DOS CRIMES CIBERNÉTICOS NO CÓDIGO PENAL BRASILEIRO

Ressalta-se que nosso ordenamento jurídico pátrio pouco aborda quanto ao assunto cibernético, pois ainda nosso Código Penal é antigo e suas alterações são morosas. Dessa forma, poucas são as leis que resguardam o direito informático, deixando crítica a situação dos usuários deste meio. Observemos algumas delas.

Em grande parte dos casos o nosso atual Código Penal Brasileiro pode ser usado, de forma equiparada, no meio virtual. É o que ocorre no § 1º-A, do artigo 153, que diz:

> Art. 153 - Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem:
> Pena - detenção, de um a seis meses, ou multa.
> § 1º Somente se procede mediante representação.
> § 1º-A. Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública:
> Pena – detenção, de 1 (um) a 4 (quatro) anos, e multa.
> § 2º Quando resultar prejuízo para a Administração Pública, a ação penal será incondicionada.[6]

Observa-se que o parágrafo em comento visa dar um amparo ao segredo da informação da Administração Pública, ou seja, o que é protegido aqui é o conteúdo guardado pelo Estado, em que este poderá se tornar vítima, caso venha a ser atingido por tais violações. Além disso, qualquer pessoa pode ser sujeito ativo desta ação penal, ao passo que basta o intuito de um indivíduo comum querer divulgar o conteúdo protegido da Administração Pública, pouco importando se estava alocado em seus bancos de dados ou que venha a causar danos a outrem, sendo necessário apenas a execução da prática prevista, qual seja a divulgação da informação.

Segundo Juliano Madalena, existe a necessidade de uma complementação entrea lei e a ciência técnica, pois a Internet está sendo considerada uma extensão do homem, assim como é tratado o direito. Logo, o caminhar conjunto entre esses elementos éreconhecido (2016, p. 91-92).

Em continuidade, há também o caso do apelidado peculato eletrônico, o qual foi advindo da Lei nº 9.983/2000[7] – assim como o artigo anteriormente comentado - e acrescentado pelos artigos 313-A e 313-B do Código Penal Brasileiro. Muito embora esses artigos tenham ganhado a alcunha de peculato, sua definição é bem diversa.

Pois então vejamos o que diz a legislação sobre o assunto:

> Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos

---

[6] _____. Código Penal - Decreto-lei 2848/40 | Decreto-lei no 2.848, de 7 de dezembro de 1940. Disponível em: <http://www2.camara.leg.br/legin/fed/declei/1940-1949/decreto-lei-2848-7-dezembro-1940-412868-publicacaooriginal-1-pe.html> acessado em nov. 2017.

[7] BRASIL,Lei nº 9.983, de 14 de julho de 2000. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/L9983.htm#art2> acessado em nov. 2017.

> sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano: (Incluído pela Lei nº 9.983, de 2000)
> Pena – reclusão, de 2 (dois) a 12 (doze) anos, e multa.[8]

Com uma breve análise já é possível averiguar que se trata de uma inserção ou mesmo disposição de ajuda para que outro inclua conteúdo falso nos sistemas eletrônicos da Administração Pública, com o almejo de lograr ganho indevido para si ou mesmo para terceiros. Destaca o artigo acima que para a prática deste delito é necessário que o agente, executor do verbo penal, seja funcionário que possua permissão, isto é, autorizado, o qual acrescentará os dados ilegais ou mesmo auxiliará que outrem o faça.

Importante mencionar que o mesmo diploma legal incriminador leciona, em seu artigo 327, que, para fins penais, a descrição de funcionário público é mais ampla, pois basta que exerça função pública, emprego ou mesmo um cargo público, seja ele com ou sem ganho de remuneração, tampouco necessitando que seja estável, permanente. Assim, o que o artigo ressalta é que o sujeito exerça uma atividade pública e que nesta pratique o crime.

No mesmo caminhar, o artigo 313-B, também acrescentado pela Lei nº 9.983/2000, traz amparo ao meio informático, ao trabalhar quanto aos assuntos sobre a mudança, não permitida, de sistemas de informação.

Vejamos:

> Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente:
> Pena – detenção, de 3 (três) meses a 2 (dois) anos, e multa.
> Parágrafo único. As penas são aumentadas de um terço até a metade se da modificação ou alteração resulta dano para a Administração Pública ou para o administrado.[9]

Note-se que bastante se assemelha ao artigo 313-A, mas seu diferencial está no ponto que menciona a mera conduta do funcionário público modificar os

---

[8] _____. Código Penal - Decreto-lei 2848/40 | Decreto-lei no 2.848, de 7 de dezembro de 1940. Disponível em: <http://www2.camara.leg.br/legin/fed/declei/1940-1949/decreto-lei-2848-7-dezembro-1940-412868-publicacaooriginal-1-pe.html> acessado em nov. 2017.

[9] _____. Código Penal - Decreto-lei 2848/40 | Decreto-lei no 2.848, de 7 de dezembro de 1940. Disponível em: <http://www2.camara.leg.br/legin/fed/declei/1940-1949/decreto-lei-2848-7-dezembro-1940-412868-publicacaooriginal-1-pe.html> acessado em nov. 2017.

sistemas informáticos sem prévia autorização ou mando do agente competente, sendo este, na maioria dos casos, o seu superior hierárquico da instituição o qual integra. Para o caso em comento também terá como sujeito lesado o Estado, visto que a própria Administração Pública sofrerá com eventuais mudanças não autorizadas.

Dessa maneira, o artigo em apreço, que fora acrescentado pela Lei nº 9.983/2000se distingue do outro também acrescentado pela mesma legislação, pois "enquanto no dispositivo anterior protegem-se os dados componentes de um sistema, busca-se, agora, tutelar o próprio sistema de informações ou programa de informática" (CUNHA, 2016, p. 749).

Tempestivo e gratificante levantar outro ponto que a Lei nº 12.737/2012 modificou no Código Penal Brasileiro, qual seja o acréscimo do § 1º no artigo 266, mencionando que também serão sancionadas as condutas de obstar serviços telemáticos ou de conteúdo que interesse o coletivo. Para tal delito a pena será de um a três anos, somados com multa, destacando-se que sua aplicação em dobro quando se tratar de situação em que houver calamidade pública.

Ademais, a Lei nº 12.737/2012 também trouxe amparo maior para o artigo 298[10] do Código Penal Pátrio ao incluir, em seu novo parágrafo primeiro, a conduta equiparada da falsificação de documento particular, abarcando nos casos de cartão de crédito ou débito. Nada mais do que justo, dado que a falsificação desses pertences prejudica a vítima, tanto quanto os documentos impressos.

> Se a falsificação for grosseira e visualmente for incapaz de enganar alguém, o crime será impossível, devendo ser aplicado o art. 17 do CPB, por absoluta impropriedade do objeto. Se, apesar de visualmente ser incapaz de enganar um ser humano, o chip for reconhecido pelos caixas eletrônicos como válido, ainda assim o crime do art. 298 do CPB será impossível, podendo o agente, nesse caso, ser punido pelo crime do art. 154-A, também do CPB (VIANNA; MACHADO, 2013, p. 106).

[10] _____. Código Penal - Decreto-lei 2848/40 | Decreto-lei no 2.848, de 7 de dezembro de 1940. Disponível em: <http://www2.camara.leg.br/legin/fed/declei/1940-1949/decreto-lei-2848-7-dezembro-1940-412868-publicacaooriginal-1-pe.html> acessado em nov. 2017.

2.3RESPONSABILIDADE CIVIL FRENTE A VIOLAÇÃO DE PRIVACIDADE

Todo aquele que provocar indevidamente um dano a outrem estará incumbido de indenizá-lo para que a lesão seja ao menos minimizada, como é no caso da obrigação de pagar multa diante do cometimento de crimes. Assertiva essa postura, até porquê condutas reprováveis andam na contramão da moral social.

Como é o caso do artigo 186, do Código Civil[11]:

> Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito.

No mesmo sentido aduz o artigo 927, do mesmo diploma legal:

> Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo.
> Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem.

No dia a dia inúmeros casos de responsabilidade civil são questionados, no que diz respeito à afronta da privacidade individual, tratando-se, pois, de um direito da personalidade. Aqui, no direito digital, não seria diferente, pois independe o lugar em que está sendo exercida a conduta delituosa, é certo que esta deve ser combatida, seja pela punição em cárcere, seja mediante o pagamento em dinheiro.

> No entanto, dada a falta de legislação específica sobre o tema, por vezes os Tribunais pátrios promulgam decisões contraditórias. Isto é, ainda se discute uma clara definição dos limites da responsabilidade civil e/ou criminal dos provedores e *sites* que colocam no “ar” conteúdo ilícito adicionado por terceiros (PINHEIRO, 2009, p. 311).

Espanta-se a falta de empenho para produzir normas que acompanhem efetivamente os novos delitos, dado que a criminalidade só vem a crescer com o pouco investimento nesse campo. Desse modo, o número de vítimas, indignadas por sinal, também aumentam, sendo resultado da ineficiência do Poder Legislativo que

[11] _____. Lei nº. 10.406, de 10 de janeiro de 2002. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm >. Acesso em: 15 nov. 2017.

ocasiona um efeito de mão dupla, deixando a sociedade desamparada no momento em que eventual dano existir.

O direito à privacidade é garantido pela atual Constituição Federal de 1988[12], em seu artigo 5º, inciso X, com a intenção de resguardar assuntos mais restritos do sujeito, o qual não seria apropriado expor essas informações a terceiros. O mesmo artigo deixa claro que em situações de violação a norma a vítima estará amparada, porque o agente infrator ficará obrigado a pagar pelo dano ocasionado, tanto material ou mesmo moral, pois o que se evita aqui é a violação.

Portanto, o melhor a ser feito é provocar o Poder Legislativo, visando uma resposta para que edite e crie normas que acompanhem o meio informático com o intuito de diminuir a criminalidade.

[12]BRASIL, Constituição da República Federativa do Brasil (1988). Disponível em <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm> Acesso em nov. de 2017.

CAPÍTULO III

3 - IMPUNIDADE FRENTE A DIFICULDADE DE IDENTIFICAR A AUTORIA DELITIVA

3.1IDENTIFICAÇÃO VIRTUAL

Atualmente há diversos meios para o acesso à Internet, seja ele por celulares, computadores de mesa, notebook, tablets e diversos outros. Cada aparelho possui uma identificação individual chamada de IP, como se fosse um “RG pessoal da máquina” e ao visitarmos um site, o aparelho que utilizamos deixará rastros de que acessamos aquele lugar.

> A identidade e o reconhecimento na rede mundial de computadores são feitos de modo semelhante aos dois modelos anteriormente apresentados; em verdade, pode-se dizer que são mescladas características da concretização qualitativa e numérica. Diferenciam-se, porém, em três importantes aspectos: a) não há – ou pelo menos não deveria haver – identidade na rede (concretização qualitativa) sem identidade numérica, ou seja, para se identificar o *host* A como um computador que faz parte de uma rede, será necessário atribuir-se um endereço numérico a ele – por exemplo, um endereço IP; a) a identidade, seja ela qualitativa (individualidade de características na rede) ou numérica (endereço), será sempre de um computador, jamais de um sujeito; c) um endereço numérico – por exemplo, um endereço IP – pode ser atribuído em um curto período de tempo (horas) a diferentes computadores, não podendo, entretanto, (em tese) possuírem o mesmo endereço, ao mesmo tempo, dois ou mais computadores individualmente considerados (COLLI, 2010, p. 88).

Acontece que os recursos disponíveis, em que pese o grande avanço já alcançado pela informática, eventualmente é falho, o que resulta na prática delitiva nesta seara tecnológica. Em consequência, usuários comuns, que usam esse meio para facilitar as atividades do cotidiano, acabam se tornando vítimas, colocando em risco seu patrimônio e até a integridade privada.

Diante disso, surgem os oportunistas *Crackers*, que são agentes maléficos que buscam burlar a rede de sistema computacional para violar os aparelhos de terceiros com o objetivo de tomar para si ou até mesmo para outrem, determinado proveito indevido. Tal atitude, muitas das vezes, acaba se tornando

impune, pois, à medida que a tecnologia avança, do mesmo modo acompanham os interessados em tomar proveito dos que estão de alguma forma vulneráveis.

A doutrinadora Liliana MinardiPaesani clareia um pouco a ideia, sinteticamente, de como isso ocorre:

> Na proteção dada pela lei penal, a falta de um corpo de delito tem sido encarada como um dos obstáculos mais graves. Exemplificando: se alguém subtrai os materiais que contêm um programa, copia-os, e torna a repô-los no seu lugar, se não for colhido no ato da subtração ou devolução, dificilmente poderá ser condenado por ter cometido o furto. A cópia em si, para uso próprio, não constitui delito (PAESANI, 2009, p. 75).

Compete às polícias investigativas – polícia federal e civil – o poder de investigar as ocorrências dos crimes, identificando a autoria delitiva e apanhando a materialidade proveniente da ação do agressor. Todavia, por falta de investimento, quer pelas poucas tecnologias disponíveis para esses servidores, quer pela inércia do Poder Público para solucionar a precariedade policial, os crimes cibernéticos acabam, infelizmente, compensando para os infratores da lei, pois eles veem como algo que dá certo, que o lucro é fácil e, muitas das vezes, obtido.

> O maior problema jurídico dos crimes virtuais é a raridade de denúncias e, pior, o despreparo da polícia investigativa e de perícia para apura-las. Embora já seja possível fazer boletins de ocorrência pela Internet, são poucas equipes e profissionais preparados para a investigação de um crime virtual. É importante lembrar que os criminosos da Internet já não são criminosos incomuns – a imagem de um sujeito extremamente inteligente e com vasto conhecimento técnico já não corresponde à realidade, pois atualmente é muito fácil encontrar na Internet o código-fonte aberto de um vírus ou trojan. Alguns criminosos praticam até mesmo a clonagem de *sites*, que, nesse caso, exige *expertise* tecnológica acima da média, utilizando-os para roubar informações dos usuários, tais como RG, CPF, residência, telefone, *e-mail*, dados bancários – informações utilizadas posteriormente para que o criminoso assuma outras identidades em operações comerciais como uso de cartão de crédito clonado. O combate a esses crimes torna-se extremamente difícil por dois motivos: a) a falta de conhecimento do usuário, que, dessa forma, não passa às autoridades informações relevantes e precisas; e b) a falta de recursos em geral das autoridades policiais (PINHEIRO, 2009, p. 230).

A melhor maneira para evitar *Crackers* ou mesmo conseguir identifica-los para posterior punição, é investindo nas carreiras policiais, pois, apesar de muito importante, apenas a criação de leis não garantirá que os indivíduos maus intencionados deixem de cometer crimes. Dessa forma, imprescindível que se tenha condições de fazer uma boa investigação, com computadores que satisfaçam as necessidades de uma boa perseguição virtual, bem como a disponibilização de cursos preparatórios, visando sempre aperfeiçoar o trabalho dos servidores públicos.

Vale salientar, ainda, a relevância de se ter, em cada cidade, delegacias especializadas sobre o assunto, com servidores capacitados, dado que assim facilitará a perseguição do delito, até porquê quanto maior for o número de profissionais trabalhando e investimento sendo aplicado nessa área, maiores serão as chances de os repelir. Assim, a demanda irá reduzir significativamente com o passar dos anos e deixará claro, aos agressores, que não vale mais a pena tentar burlar a lei no ramo informático.

> [...]há que se fazer uma ressalva: a proposta apresentada nesta obra acerca da criação de divisões policiais especializadas em cibercrimes, não tem o ambicioso condão de ser uma (ou a única) solução para os problemas até aqui apresentados. O que se quer evitar é uma visão reducionista representada por uma cognição solucionadora (e restritiva) para a investigação preliminar de infrações penais cometidas pela internet. A atividade policial, seja ela desempenhada no mundo *off-line*, seja ela desempenhada no mundo *on-line*, seja ela atribuição da Polícia Civil, seja da Polícia Federal, deverá ser orientada por uma política de segurança pública organizada e estruturada a partir de dados e informações inerentes ao lugar ou à matéria à qual as autoridades policiais estarão vinculadas (COLLI, 2010, p. 160-161).

Consoante alega EmersonWendt, no estado do Mato Grosso do Sul existe apenas uma Delegacia para atender casos do ramoVirtual. Isso demonstra a precariedade que enfrenta o assunto, dado que a população, na maioria das cidades, fica desamparada (2011, p. 77).

Outra problemática para o tema é a questão de vários usuários usarem o mesmo computador, como é no caso de uma família, em que a máquina é usada por vários integrantes, seja para atividades de lazer ou mesmo para trabalho, assim como no caso de Cyber Café/*Lan house*, sendo o número de usufruidores ainda maior, o que, em caminho, o risco também o será. Ora, a probabilidade de identificação da autoria delitiva em casos como esses se reduz de forma muito

considerável, pois já é difícil encontra-lo em casos comuns, quem dirá em situações de uso em maquinário compartilhado por vários.

Por fim, mas não menos importante, depara-se que o pensamento de que os crimes virtuais são compensatórios e de ganho fácil é, também, consequência da precária situação em que se encontram as forças policias, dada a falta de investimento, equipamento e preparação. Logo, a autoria criminosa acaba sendo desconhecida, o que gera a sensação de impunidade pela sociedade usuária dos meios eletrônicos.

3.2AUSÊNCIA DE SEGURANÇA

É notório que no mundo real a sociedade, muitas das vezes, sentem-se inseguras, pois o pequeno efetivo policial, isto é, pouca quantidade de servidores para cumprir a demanda populacional, acaba não dando conta da demanda. Isso não é diferente na área virtual, para ser franco, a situação é ainda mais extrema, visto que a cada momento novos *softwares* maliciosos são desenvolvidos e aperfeiçoados em busca de lograr as infrações.

> Desde o surgimento da escrita e da leitura, a confidencialidade da informação passou a assumir, gradativamente, elevada relevância. Proteger determinado conteúdo informativo começou a refletir não apenas perante o caráter comunicativo, mas também o econômico, o social e o particular de cada indivíduo.
> A partir de então, a busca pelo aprimoramento da proteção da informação foi aumentando, visando destiná-la apenas aos legítimos interessados (CAZELATTO; SEGATTO, 2014, p. 391.)

Percebe-se a pequena presença das forças policiais nos crimes comuns, questiona-se então como serão tratados os casos cibernéticos, já que não se pode tolerar deixá-los ao livre arbítrio daqueles que possuem a competência de fazer algo para evitar, mas não o fazem, não criam legislações eficazes, tampouco investem no setor responsável para combater os delitos. Destarte, o que resta para os usuários é a prevenção, pois, o melhor modo de impedir tais condutas é “matá-las pela raiz”, vale dizer, a prevenção, diante da ineficiência estatal, é uma das poucas ferramentas que nos resta para proteção.

Ser cauteloso em todo o momento em que for usar qualquer aparelho eletrônico se torna uma boa opção para quem não quer virar vítima da criminalidade,

pois na maioria dos casos as ocorrências se dão pelo mau uso desses meios, seja pela imperícia, seja pelo descuido. Aos poucos a sociedade está percebendo que as gravidades dos delitos informáticos são mais altas do que se pode imaginar.

Casos como clonagem de cartões de crédito, roubos de senhas de acesso e falsas ilustrações de compras são cada vez mais corriqueiras. Isso se dá, em regra, pelo desleixo do usuário, não se prevenindo ao colocar seus dados em qualquer hospedagem virtual ou mesmo abrindo *e-mails* de desconhecidos.

> Mais uma vez, deve-se ter em mente que não há como ter 100% de garantia de segurança, nem no mundo real nem no mundo virtual. Vejamos o que ocorre com os golpes em caixas eletrônicos de Bancos. Mas sabemos que a tecnologia permite ampliar essa segurança para limites adequados à manutenção da paz social, devendo cada um, individualmente, zelar e ser responsável pela segurança de suas senhas de modo a ajudar a coibir tais práticas, cada vez mais comuns (PINHEIRO, 2009, p. 164).

O que poucos sabem, e se sabem não dão valor, são as ferramentas de *backup*, as quais possuem funções imprescindíveis no caso de arquivos que não podem serem perdidos. Muito usado para guardar cópias de segurança de algunsconteúdos, obstando que criminosos sequestremdeterminados arquivos da máquina e exijam uma recompensa para a devolução – *software* malicioso conhecido como *ransomware*, dado que já existirá uma cópia salva em outro lugar, seja em um dispositivo físico ou mesmo por formas mais modernas que são as famosas “nuvens” (*cloudcomputing*), em que o cliente de algum site de hospedagem grava o arquivo pela Internet, de maneira segura e que, caso escolha, somente ele terá acesso (VIANNA; MACHADO, 2013, p. 77).

Ressalta-se, também, a imprescindibilidade de sempre deixar os programas de proteção atualizados, pois assim se adaptará as novas modalidades de *malwares*. Exemplo disso são os antivírus, em que suas listam precisam constantemente serem refrescadas, porque com o passar do tempo novos aplicativos lesivos são criados, então inovadoras maneiras de impedi-las devem serem acionadas (VIANNA; MACHADO, 2013, p. 67).

Uma boa iniciativa Estatal também será a criação de projetos de conscientização para a sociedade, deixando-as cientes dos riscos quanto ao mau manuseio dos aparelhos tecnológicos e também as ensinando a melhor utilizá-los,

pois muitos usuários, ainda mais agora com a crescente compra de celulares, acabam adquirindo um dispositivo sem ao menos ter conhecimento das funções que ele dispõe. Diante do discorrido, aprender corretamente como deve agir ao usar a informática, principalmente a Internet, só trará benefícios para os usufruidores.

3.3ELEMENTOS PROBATÓRIOS PARA O COMBATE AOS CRIMES VIRTUAIS

A materialidade delitiva é o que preocupa os estudiosos do ramo cibernético, pois seus vestígios são difíceis de serem obtidos, dada a complexidade do sistema virtual. Além disso,fica inviável descobrir o agressor das condutas informáticas com a falta de equipamentos aptos para isso.

Em um amplo olhar, visando atingir seu fim ilícito, os agentes infratores acabam preferindo enganar aqueles que menos possuem conhecimento tecnológico, pois desse modo conseguem mais facilmente persuadi-los. É o caso dos *e-mails* fraudulentos, em que o remetente pode se passar por uma agência bancária, colocando a imagem deste local e mandando uma ilusória mensagem, que, em certos casos, o destinatário acaba acreditando e colocando seus dados pessoais, tornando-se mais uma vítima (WENDT, 2011, p. 25).

Existem algumas especialidades para levantar a prova delitiva dos crimes cibernéticos, ao passo que seus rastros podem ser apagados ou mesmo camuflados pelo invasor, utilizando-se de programas que escondam sua identidade e localização. Além disso, poderá se utilizar de recursos que alterem os vestígios deixados pela infração.

Peculiar, também, são nos casos em que os agressores não residem no país da vítima,impedindo uma perseguição efetiva, dado que se deve respeitar as leis de cada local de origem. Solução para esse caso é a realização de um acordo de cooperação entre Estados, visando uma mútua ajuda, trabalhando juntos para repelir o cometimento de condutas afins.

> A aplicação dessa norma aos casos de invasão de dispositivo informático cometidos através da Internet em que o computador do agente se encontre em países diferentes do da vítima é demasiadamente simples quando em ambos os países a conduta seja tipificada. Nestes casos, pune-se tanto o agente que, no Brasil, invadisse um dispositivo informático localizado no estrangeiro,

> quanto o agente que, estando no estrangeiro, invadisse dispositivo informativo sito no Brasil.
> Bem mais complexas, no entanto, serão as soluções dos casos em que a conduta é típica em apenas um dos países. Assim, pode ocorrer que a conduta seja típica no país em que o comando é dado, porém atípica no Estado onde se dá o resultado fático. Ou, ao contrário, ser atípica no país da ação e típica no do resultado fenomênico. Para se encontrar a solução para essas duas situações, deve-se partir do pressuposto de que as normas de caráter penal são interpretadas restritivamente. Assim, havendo duas interpretações possíveis e perfeitamente lógicas para uma situação jurídica, deverá o intérprete optar por aquela que menos restringir a liberdade do cidadão (VIANNA; MACHADO, 2013, p. 58-59).

Como praticamente todas as atividades são registradas, dificilmente o criminoso conseguirá maquiar toda a sua “navegação”. Isso é perceptível desde o momento em que ligamos o computador, em que sua marca numérica de endereço IP é acionada, como também no momento de acessar a Internet, visto que em cada site que visitemos estarão marcados nossos registros pessoais.

Diante disso, não é sempre necessário que para identificar a autoria delitiva se tenha uma conta de perfil, bastando registros enquanto se utiliza a rede. Tanto é verdade que no histórico do *browser* – aplicativo que é meio para realizar pesquisas – ficam registradas todas as ações do usuário, demonstrando quais páginas foram visualizadas, bem como a hora específica de acesso.

Percebe-se, desde logo, que uma das provas mais importantes a serem colhidas para o encalço do crime é o IP (*Internet Protocol)* do violador, pois é a partir dele que será possível descobrir qual máquina foi utilizada. Todavia, partimos novamente para a hipótese em que o computador é utilizado por várias pessoas, situação em que não se poderá afirmar com certeza que o simples endereço identificador de um dispositivo será capaz de descobrir o agente delinquente, necessitando, então, que sejam juntados outros elementos probatórios.

> Em tese, para se descobrir qual máquina executou a referida operação naquele momento, busca-se inicialmente a identificação do endereço *IP* – no presente exemplo, de número X. Identificado o endereço *IP* responsável pela operação não autorizada, parte-se para a análise de qual provedor de internet possuía referido endereço *IP* – na verdade, a máquina do sujeito que fez a operação possui um *IP* que é emprestado pelo provedor, isto é, provedores de acesso à internet possuem uma gama de endereços *IPs* a sua disposição, os quais serão atribuídos aos seus clientes no momento da conexão destes à internet. Identificado o provedor de acesso, identifica-se sob qual conta de usuário estava sendo utilizado o

> referido *IP* em referido momento, a fim de se descobrir, a seguir, quem teria feito a transação bancária (COLLI, 2010, p. 90).

O trabalho dos policiais peritos são de extrema importância nessa seara, dado que são eles os responsáveis por averiguar casos mais complexos em que se exige técnicas específicas para apurar os crimes virtuais. Assim, serão incumbidos por identificar todos os vestígios deixados pelos infratores. E, enganam-se aqueles que pensam que excluir arquivos armazenados na máquina ou mesmo esvaziar a lixeira impedirá que os profissionais o encontre, pois mesmo apagados é possível recuperá-los por meio de programas estratégicos desenvolvidos para esse objetivo.

Entretanto, vale salientar que não apenas os peritos poderão buscar saber a autoria delitiva, mas outros agentes policiais também, bem como a própria vítima com o intuito de ser reparada, observando-se, é claro, a licitude das provas apanhas, pois, segundo o artigo 156, do Código de Processo Penal[13], cabe a quem alegou a incumbência de provar os possíveis fatos delitivos. Desse modo, o que se pretende é dar uma resposta não só à vítima, mas também à toda sociedade, e para isso necessário se faz aplicar a devida sanção ao invasor.

O atual Código de Processo Penal ainda menciona, em seu artigo 5º, parágrafo terceiro, que:

> [...] § 3º Qualquer pessoa do povo que tiver conhecimento da existência de infração penal em que caiba ação pública poderá, verbalmente ou por escrito, comunicá-la à autoridade policial, e esta, verificada a procedência das informações, mandará instaurar inquérito. [...]

Logo, acreditar que jamais será pego ao praticar condutas virtuais lesivas é mentir para si mesmo, pois, apesar do pouco aparato tecnológico, as forças policiais se empenham com muita garra e dedicação, obrigando o infrator, após apreciação judicial, a reparar o dano.

---

[13] _____. Decreto-Lei nº 3.689, de 3 de outubro de 1941. – Código de Processo Penal. Disponível em <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689Compilado.htm>. Acesso em: 16 nov. 2017.

CAPÍTULO IV

4 - MEIOS DE PREVENÇÕES A ATAQUES VIRTUAIS

4.1ANTI-MALWARE E FIREWALL

Atualmente a compra de aparelhos eletrônicos, sejam eles celulares, computadores e dos mais variados tipos disponíveis no mercado, tem sido fácil por parcela significativa da população, sendo comum o uso para as tarefas do dia adia. Isso só se deu em razão do baixo custo estabelecido pelos vendedores, possuindo como válvula impulsora o avanço diário da tecnologia.

Em que pese o lado positivo da agilidade para a execução das tarefas do cotidiano populacional, por outro lado, percebe-se o grande risco que acaba sendo desconhecido pela maioria dos usuários ao acessarem conteúdos hospedados sem segurança alguma. Em consequência, tornam-se vulneráveis a inúmeros tipos de ataques virtuais, colocando em risco os dados existentes em seus aparelhos pessoais.

Para que isso não aconteça, necessário se faz toda forma de cuidado ao manusearmos os aparatos tecnológicos que se encontram a nossa disposição. Assim, recomenda-se verificar sempre a autenticidade dos sites que visitamos, evitar baixar arquivos de lugares desconhecidos e até mesmo não utilizar cartões bancários pela Internet.

Há, ainda, maneiras de minimizar os efeitos dos agentes invasivos frente à falta de proteção estatal, resguardando a privacidade da sociedade usuária dos meios informáticos, não necessitando nos valer de normas para isso. Ocorre quando utilizamos de programas que impedem que nossos dispositivos sejam violados, como é o caso dos chamados antivírus ou para ser mais correto o denominamos de anti-malware, razão pela qual vírus é apenas uma categoria de *malware* e o aplicativo em comento embarca todas as categorias existentes, a depender da sua atualização de listas internas.

Existe também o*Firewall*, que é popularmente chamado de parede de fogo, em analogia a imagem de uma barreira, pois sua função é impedir que outras redes e computadores tenham acesso direto com a máquina que está sendo usada.

Assim, sempre que houver tentativas de contato externo, o *Firewall* alertará o usuário do dispositivo paciente[14].

Apesar dos recursos existentes para resguardar os dados que possuímos nos aparelhos, como anti-malware e até mesmo o *Firewall* - programas estes explicados no decorrer desta pesquisa, a melhor forma de não ser atacado por arquivos maléficos é se prevenindo, tomando todos os devidos cuidados. Logo, o modo mais consequente de ficar inseguro, é quando achamos que já estamos seguros, ao passo que, ficamos vulneráveis ao acharmos que estamos totalmente invulneráveis.

4.2CRIPTOGRAFIA

Como forma de esconder de pessoas não autorizadas o conteúdo de mensagens que estavam sendo transmitidas, a criptografia foi adaptada no meio informático. Sua maior presença fora registrada desde as primeiras grandes guerras, que, no início, era utilizada para evitar que o adversário conseguisse informações privilegiadas que pudessem causar prejuízo à equipe transmissora (ECHEVERRY, 2016).

Apesar do marco no campo de batalha, no antigo Egito já era utilizado algo parecido com a criptografia, dado o uso “mensagens subliminares” por meio de desenhos nas paredes que guardavam informações dos locais em que objetos valiosos estavam, cujo significado só algumas pessoas sabiam. Todavia, essa característica não é totalmente apropriada para classificar como criptografia, pois vai além de uma simples figura estranha (BRUNO, 2017).

Acontecimento bizarro e ao mesmo tempo impressionante era o que Leonardo Da Vinci fazia com seus documentos ao escrevê-los de trás para frente, com o intuito de evitar que espiões ou mesmo terceiros não autorizados lessem o conteúdo que escrevia – percebe-se que se usassem um espelho poder-se-ia decifrá-lo. Outrossim, “deu vida”, ainda, ao aparato tecnológico chamado de “Críptex”, cuja finalidade era criptografar e também descriptografarinformações (BROWN, 2006, p. 176).

---

[14]Microsoft. Proteja seu PC com um Firewall. Disponível em: <https://www.microsoft.com/brasil/proteja/firewall.aspx>. Acesso em: 16 nov. 2017.

Vale dizer, para que se tenha um conteúdo criptografado é preciso que existam alterações nas informações que estão sendo enviadas, não bastando uma mera problemática para maquiar o objeto que está secreto.

> Em termos técnicos, a criptografia é uma ferramenta de codificação usada para envio de mensagens seguras em redes eletrônicas. É muito utilizada no sistema bancário e financeiro. Na Internet, a tecnologia de criptografia utiliza o formato assimétrico, ou seja, codifica as informações utilizando dois códigos, chamados de chaves, sendo uma pública e outra privada para decodificação, que representam a assinatura eletrônica do documento. No Brasil, o sistema já utiliza duas chaves, pública e privada, de 128 *bits*(PINHEIRO, 2009, p. 161).

O sistema de certificação digital ou mesmo a assinatura digital está sendo muito bem implantada nos dias atuais, pois são ferramentas que elevam o grau de segurança no sistema computacional. São usados alguns critérios específicos no conteúdo transmitido, o qual é desempenhado duas chaves, podendo elas serem públicas ou mesmo privada. Para ter acesso à informação, apenas quem tem permissão é que poderá usufruir dos dados, ou seja, só quem tem a chave adequada é que conseguirá visualizar o arquivo.

Insta salientar o crescimento do uso criptográfico no setor jurídico, o qual optou por certificar as movimentações processuais, tornando online sua consulta, bem como o aperfeiçoou ao realizar a firma por meio de assinatura digital. Tais procedimentos são positivos, muito bem vistos pela sociedade, pois, não só ajuda a garantir a autenticidade do conteúdo que está sendo produzido, mas também facilita o acesso aos documentos públicos, podendo qualquer pessoa tomar conhecimento de onde quer que ela esteja, bem como evitando que o seu conteúdo se perca, diferentemente do papel, que se deteriora com o passar dos anos.

Com o sistema processual eletrônico, os advogados também foram privilegiados, visto que, ao respeitar o prazo que lhes são dados, conseguem peticionar entrando pelo sistema disponível da própria Justiça, não precisando ir até o local em que o magistrado se encontra trabalhando. Assim, facilita o trabalho dos serventuários da Justiça, bem como daqueles que desempenham funções essenciais a este órgão.

Outro ponto importante é o caso dos cartórios. Por muitos anos os cartórios foram reconhecidos por serem um lugar em que se mexe com papeladas,

sistemas burocráticos e até mesmo local em que a sociedade, por muitas das vezes, precisam gastar valores exorbitantes para obter certificados, autenticações ou registros de documentos.

Com o surgir da certificação digital e da assinatura digital esse cenário está mudando, pois muitos das escrituras podem ser obtidas de forma online, dispensando o contato com os cartórios e economizando dinheiro que antes eram gastos. Há grande receio, ainda, de que futuramente a maior parte das funções dos cartórios deixarão de ser útil, quiçá até mesmo sua própria existência.

Um dos mais famosos sistemas criptográficos nasceu nos Estados Unidos, o qual fora desenvolvido, em 1983, por estudiosos da MIT – Instituto de Tecnologia de Massachusetts. A MIT codificava e autenticava os dados dos requerentes (PINHEIRO, 2009, p. 160).

4.3PROTOCOLOS DE NAVEGAÇÃO EM REDES

Antes mesmo de falar sobre protocolos, é preciso saber que redes são interligações entre sistemas computacionais. Além disso, essas interligações poderão se dar por meio de ferramentas, como ondas eletromagnéticas, satélite, cabos de cobre,dentre outros.

Classificam-se em redes regionais/locais, que são chamadas de LAN, abreviatura esta que significa *local are network*, sendo que o seu uso é destinado para moradia ou mesmo escritórios. Por outro lado, quando se trata de uma rede com uma abrangência um pouco maior, integra-se outra classificação, qual seja as WAN, cujo significado é o termo *wide área network* e sua principal funcionalidade é a de interligar as redes regionais/locais (WENDT, 2011, p. 39).

Em síntese, protocolo é a união de princípios que normatizam as transmissões de informações entre máquinas.

> A Internet é uma rede global que consiste na interconexão de inúmeras redes que usam o mesmo protocolo. Logo, ela permite interligar sistemas informáticos de todo o planeta, proporcionando o recebimento e envio de informações.
> Cada um dos dispositivos informáticos desta rede recebe um endereço consistente em 32 bits divididos em quatro campos de um byte (oito bits) cada, variando, pois, de 0 a 255. Por exemplo:
> 32.104.87.2
> 150.164.76.80

> 198.186.203.18
> Este endereço, denominado IP (*Internet Protocol*), é o único na rede e identifica cada um dos computadores interconectados (VIANNA; MACHADO, 2013, p. 24-25).

Ocorre que o uso do IP – *Internet Protocol* – é pouco apreciado em sites de navegação, dada a complexidade em ter que ficar decorando a numeração de cada endereço de hospedagem. Por essa razão, em vez do IP, usa-se para cada local específico um tipo de domínio.

Dessa forma, o domínio é como se fosse uma ferramenta facilitadora que a informática dispõe, pois seria inviável decorar a numeração de cada site, sendo que este poderá ter uma numeração para cada região. Assim, comumente é "batizado", na sua criação, um nome para cada IP, como, por exemplo, "*www.nomedodominio.com"* (VIANNA; MACHADO, 2013, p. 25).

5-CONSIDERAÇÕES FINAIS

Percebe-se, então, que o setor tecnológico vem ganhando maior demanda com o passar dos anos, dado o interesse pela sociedade em adquirir meios que facilitem as atividades rotineiras, bem como em razão do valor que, para alguns produtos, estão sendo acessíveis por parcela significativa da população. Em decorrência dessa evolução, surgem os riscos inerentes do meio funcional e medidas preventivas devem ser adotadas para coibir qualquer conduta prejudicial.

Dessa forma, o conteúdo trabalhado nesta pesquisa visou abarcar a situação crítica das atuais normas penais brasileiras frente ao cenário virtual. Para o desdobramento do assunto, foram desenvolvidasinformações necessárias do ramo informático,desde o nascimento das máquinas, a relação destas com a Internet e as principais leis existentes. Ademais, foi analisado a impunidade dos delinquentes infratores nas hipóteses em que era impreciso identificar a sua autoria.

Além disso, o arcabouço técnico normativo embasado na Lei nº 12.737/12 teve o intuído de enfatizar os casos de violação de dados alheios, demonstrando desde o motivo da sua criação, até as falhas que nela ainda existem. Deixando, assim, pontos esclarecidos que merecem ser reformados.

Detalhou-se, ainda, os riscos gerados pelo descuido dos usuários da informática, dado o desleixo e/ou a falta de conhecimento necessário para usufruir dos benefícios que o aparelho dispõe. Sendo assim, a conscientização é adotada como um dos melhores métodos para bloquear as ações criminosas invasivas, pois, conforme se entende o modo correto do uso, evita estar vulneráveis a eventuais ataques.

Portanto, o investimento no setor de segurança pública e o acompanhamento do Poder Legislativo para criar normas que estejam lado a lado com a desenvoltura atual dos delitos virtuais fará com que diminuam a porcentagem da criminalidade cibernética, trazendo frutos positivos para a sociedade.

6–REFERÊNCIAS BIBLIOGRÁFICAS

_____. Código Penal - Decreto-lei 2848/40 | Decreto-lei no 2.848, de 7 de dezembro de 1940. Disponível em: <http://www2.camara.leg.br/legin/fed/declei/1940-1949/decreto-lei-2848-7-dezembro-1940-412868-publicacaooriginal-1-pe.html>. Acesso em: 02 nov. 2017.

_____. Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 02 nov. 2017.

_____. Decreto-Lei nº3.689, de 3 de outubro de 1941.– Código de Processo Penal. Disponível em <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689Compilado.htm>. Acesso em: 16 nov. 2017.

_____. Lei nº. 10.406, de 10 de janeiro de 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm>. Acesso em: 15 nov. 2017.

ALECRIM, Emerson. **O que é ransomware**. Disponível em: <https://www.infowester.com/ransomware.php>. Acesso em: 15 nov. 2017.

ARIMURA, Mayumi. **Saiba a diferença entre Hackers, Crackers, White Hat, Black Hat, Gray Hat, entre outros**. Disponível em: <http://www.egov.ufsc.br/portal/conteudo/saiba-diferen%C3%A7a-entre-hackers-crackers-white-hat-black-hat-gray-hat-entre-outros>. Acesso em 15 nov. 2017.

BRAGA, Giancarlo M.; ALECRIM, Emerson. **Guia de hardware para iniciantes**. Disponível em: <https://www.infowester.com/guiahdinic.php>. Acesso em: 15 nov. 2017.

BRASIL, Constituição da República Federativa do Brasil (1988). Disponível em <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 02 nov. 2017.

BRASIL, Lei nº 9.983, de 14 de julho de 2000. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/L9983.htm#art2>.Acesso em: 02 nov. 2017.

BROWN, Dan. **O Código Da Vinci**. Rio de Janeiro: Sextante, 2006.

BRUNO, ODEMIR M. .**Criptografia: de arma de guerra a pilar da sociedade moderna**. Disponível em: <https://jornal.usp.br/artigos/criptografia-de-arma-de-guerra-a-pilar-da-sociedade-moderna/>. Acesso em: 16 nov. 2017.

CAMPOS, Augusto. **O que é software livre**. BR-Linux. Disponível em: <http://softwarelivre.ceara.gov.br/index.php/component/content/article/3/318>. Acesso em: 15 nov. 2017.

CANDIDO, Fabiano. **Polícia captura menor que postou fotos de Carolina Deckmann**. Disponível em: <https://exame.abril.com.br/tecnologia/policia-captura-menor-que-postou-fotos-de-carolina/#>. Acesso em: 15 nov. 2017.

CAPELAS, Bruno. **Garagem onde Apple nasceu é um mito; diz Steve Wozniak**. Disponível em: <http://link.estadao.com.br/noticias/geral,garagem-onde-apple-nasceu-e-um-mito-diz-steve-wozniak,10000030006>. Acesso em: 15 nov. 2017.

CAZELATTO, Caio Eduardo Costa; SEGATTO, Antonio Carlos. DOS CRIMES INFORMÁTICOS SOB A ÓTICA DO MEIO AMBIENTE DIGITAL CONSTITUCIONALIZADO E DA SEGURANÇA DA INFORMAÇÃO. **Revista Jurídica Cesumar – Mestrado**, Maringá, v. 14, n. 2, p. 387-411, jul./dez. 2014. Disponível em: <periodicos.unicesumar.edu.br/index.php/revjuridica/article/download/3713/2469>. Acesso em: 12 jun. 2017.

COLLI, Maciel. **CIBERCRIMES Limites e Perspectivas à Investigação Policial de Crimes Cibernéticos.** 22. ed. Paraná: Juruá, 2010.

CUNHA, Rogério Sanches. **Manual de direito penal: parte geral (arts. 1 ao 120).** 4. ed. Salvador: JusPODIVM, 2016.

CUNHA, Rogério Sanches. **Manual de direito penal: parte especial (arts. 121 ao 361).** 8. ed. Salvador: JusPODIVM, 2016.

ECHEVERRY, Edwin. **Enigma: A matemática e a guerra.** Disponível em: <https://www.gcfaprendelivre.org/blog/misterio_a_matematica_e_a_guerra/1.do>. Acesso em: 16 nov. 2017.

FERNANDES, David Augusto. CRIMES CIBERNÉTICOS: O DESCOMPASSO DO ESTADO E A REALIDADE. **Rev. Fac. Direito UFMS**, Belo Horizonte: n. 62, p. 139-178, jan./jun., 2013.

FREITAS, Jessica. **Critérios da Auditoria de Segurança da Informação**. Disponível em: <https://www.governoeletronico.gov.br/documentos-e-arquivos/GT8135%20-%20CriteriosAuditoriaSeguranca%20V%2004_08_15.pdf/view>. Acesso em: 15 nov. 2017.

LISBOA, Edgar. **Lei Carolina Dieckmann entra em vigor hoje**. Disponível em: <http://www.edgarlisboa.com.br/lei-carolina-dieckmann-entra-em-vigor-hoje/>. Acesso em: 15 nov. 2017.

MADALENA, Juliano. REGULAÇÃO DAS FRONTEIRAS DA INTERNET: UM PRIMEIRO PASSO PARA UMA TEORIA GERAL DO DIREITO DIGITAL. **Revista dos Tribunais,** São Paulo: v. 974, n. 105, p. 81-110, dez, 2016.

MORIMOTO, Carlos E. .**A história da Apple**. Disponível em: <http://www.hardware.com.br/artigos/historia-apple/>. Acesso em: 15 nov. 2017.

NASCIMENTO, Elias. **Windows 10 tem mais de 100 milhões de instalações e domina 6,6% do mercado**. Disponível em: <https://www.tecmundo.com.br/windows-10/87401-windows-10-tem-100-milhoes-instalacoes-domina-6-6-mercado.htm>. Acesso em: 15 nov. 2017.

PACHECO, Márcia Soares Dantas. A APLICABILIDADE DA TEORIA DAS JANELAS QUEBRADAS AO CYBERSTALKING. **Revista dos Tribunais,** São Paulo: v. 970, n. 105, p. 241-264, ago, 2016.

PAESANI, Liliana Minardi. **Direito de informática: comercialização e desenvolvimento internacional do software.** 6. ed. São Paulo: Atlas, 2009.

PERON, Marluce. **A história da Microsoft**. Disponível em: <https://www.tecmundo.com.br/video-game-e-jogos/2068-a-historia-da-microsoft.htm>. Acesso em: 15 nov. 2017.

PINHEIRO, Patrícia Peck. **Direito digital.** 3. ed. São Paulo: Saraiva, 2009.

RPN REDE NACIONAL DE ENSINO E PESQUISA. **Nossa história**. Disponível em: <https://www.rnp.br/institucional/nossa-historia>. Acesso em: 15 nov. 2017.

SALES, Robson. **Conheça Linus Torvalds, o criador do Linux**. Disponível em: <http://www.techtudo.com.br/artigos/noticia/2011/11/conheca-linus-torvalds-o-criador-do-linux.html>. Acesso em: 15 nov. 2017.

The New York Times**. AT&T'sHistoryofInventionandBreakups**. Disponível em: < https://www.nytimes.com/interactive/2016/02/12/technology/att-history.html >. Acesso em: 15 nov. 2017.

VIANNA, Túlio; MACHADO, Felipe. **Crimes Informáticos Conforme A Lei nº 12.737/2012**. Belo Horizonte: Fórum, 2013.

XAVIER, Andressa. **O que é Spyware?**. Disponível em: <https://www.tecmundo.com.br/spyware/29-o-que-e-spyware-.htm>. Acesso em: 15 nov. 2017.

KUSZKA, Boris. **A história do Software Livre**. Disponível em: <https://canaltech.com.br/software/A-Historia-do-Software-Livre/>. Acesso em: 15 nov. 2017.

WENDT, Emerson. **Inteligência cibernética: a (in) segurança virtual no Brasil**. São Paulo: Delfos, 2011.