FACULDADE DAMAS DA INSTRUÇÃO CRISTÃ – FADIC
CURSO DE DIREITO

VICTOR DE COIMBRA PINTO GOMINHO

CRIMES VIRTUAIS: O SEQUESTRO DE DADOS NA DOUTRINA BRASILEIRA

RECIFE
2016

VICTOR DE COIMBRA PINTO GOMINHO

CRIMES VIRTUAIS: O SEQUESTRO DE DADOS NA DOUTRINA BRASILEIRA

Monografia apresentada à Faculdade Damas da Instrução Cristã como requisito parcial para obtenção do título de Bacharel em Direito.

RECIFE
2016

Gominho, Victor de Coimbra Pinto.
Crimes virtuais: o sequestro de dados na doutrina brasileira. / Victor de Coimbra Pinto Gominho. – Recife: O Autor, 2016.

45 f.

Orientador(a): Prof. Dr. André Carneiro Leão.
Monografia (graduação) – Faculdade Damas da Instrução Cristã. Trabalho de conclusão de curso, 2016.

Inclui bibliografia.

1. Crimes virtuais. 2. Direito penal. 3. Sequestro de dados. I. Título.

34	CDU (2.ed.)	Faculdade Damas
340	CDD (22.ed.)	TCC 2016-448

À memória de meu avô, Reginaldo.

AGRADECIMENTOS

A meus pais, Luciana e Marcos, que me motivaram e acreditaram em mim através de todos os altos e baixos dos meus estudos.

A minha avó que sempre incentivou meus estudos, e meus irmãos, que os atrapalharam. Amo vocês.

Aos meus amigos, os nobres praçadores: Arthur, Gabriel e Túlio, que me propiciaram com muitas dores e alegrias ao longo do curso.

Aos meus primos Nicolas e Pedro, sem os quais esta obra teria sido concluída muito mais cedo.

A meu orientador André Carneiro, pela ajuda e conselhos na correria do fim de semestre.

E muito obrigado a todas as pessoas, verdadeiras ou fictícias, que me ajudaram a formular este trabalho ou que fizeram parte de minha educação.

RESUMO

Este trabalho tem como objeto os crimes ocorridos no âmbito virtual, focando sua problemática no crime de sequestro de dados, cuja ascensão em número de ocorrências justifica a produção do estudo direcionado de sua estrutura. O problema a ser resolvido em decorrer desta obra: se a legislação brasileira corretamente tipifica o sequestro de dados em sua doutrina; teve como hipótese em favor do não, considerando a escassez de discussão legislativa ou doutrinária sobre o objeto. Para cumprir sua premissa, o trabalho objetivou a compreensão do sequestro de dados em sua interpretação normativa. Se utilizando da abordagem metodológica qualitativa e hipotético-dedutivo, seus objetivos específicos foram fazer o estudo dos crimes virtuais em geral, a análise de legislação pertinente ao tema, e exame, com base neste contexto, do crime de sequestro de dados. Pelo estudo e discussão sobre os crimes virtuais, incluindo crimes comuns e de informática, em especial o crime de sequestro de dados, podemos concluir que esta espécie de crime é demasiadamente precária na legislação e doutrina brasileira para ser de relevância penal. Ademais, seria preciso maior investimento na persecução dos agentes criminais para penalizar esta conduta, considerando a dificuldade das autoridades internacionais de fazer o mesmo. É necessária a criação do tipo específico e dos meios de cooperar com as autoridades de polícia e judiciárias de outros países para superar a barreira extraterritorial que protege o agente que pratica sequestro de dados.

Palavras-chave: Crimes virtuais. Direito penal. Sequestro de Dados.

ABSTRACT

This work has as its object the crimes taken place on the virtual scope, focusing its problematic on the ransomware crime, whose rise in number of occurrence justify the production of the directed study of its structure. The problem to be solved in the course of this work: Whether the Brazilian legislation correctly typifies ransomware in its doctrine; had the hypothesis in favor of not, considering the lack of legislative or doctrinal discussion on the subject. To fulfill its premise, the study aimed to understand ransomware in its normative interpretation. Using the qualitative and hypothetical-deductive approach, their specific objectives were to make the study of cybercrimes in general, the legislation analysis relevant to the subject, and based on this context, the examination of ransomware. Through the study and discussion regarding virtual crimes, including common and computer crimes, in particular the ransomware crime, we can conclude that this crimes species is too precarious in Brazilian legislation and doctrine to be of penal relevance. Furthermore, it would be needed more investments on the pursuit of criminal agents to penalize such conduct, considering the difficulty of international authorities to do the same. The creation of a specific type and means to cooperate with the police and judicial authorities of other countries to overcome the extraterritorial barrier that protects the ransomware practicing agent is required.

Keywords: Virtual crimes. Penal law. Ransomware.

SUMÁRIO

INTRODUÇÃO

Os crimes virtuais são um fenômeno atual, característico da sociedade moderna globalizada, que se encontra em ascensão tecnológica, e na qual se faz necessário à utilização dos mais eficientes meios de comunicação, de crescente número de formas. De todas as definições do termo, a melhor e mais técnica é a de Ivete Senise Ferreira: “Constitui crime de informática toda ação típica, antijurídica e culpável cometida contra ou pela utilização de processamento automático de dados ou sua transmissão” (FERREIRA, 1992, p. 142).

Com a popularização das redes sociais e a informatização de pessoas jurídicas de todas as áreas, os agentes que antes se limitavam ao meio físico para a realização de delitos, encontram um novo caminho, que é mais rápido e anônimo do que qualquer outro. Como a internet é um ambiente expansivo e transnacional, mais do que nunca se permite a quebra de paradigmas das interações sociais e comunicação das gerações anteriores, com a transmissão instantânea de ideias, opiniões, contatos.

O potencial da rede é quase infindável e, de certa forma, é exatamente este o problema. Com suas características, a internet é uma “terra de ninguém” que não é tutelada por nenhum órgão específico, tornando-a forma de expressão de liberdade, mas também de anarquia. Tratando-se de ser matéria nova para o direito, diversos autores buscaram analisar os crimes cibernéticos, como Maria Helena em sua publicação *Computer Crimes*[1], na qual ela cita o trabalho de Ulrich Sieber para classificar os delitos, partindo da forma de atuação do autor. Atualmente o sistema de classificação pode ter duas interpretações, a binária de Hervé Croze e Yves Bismuth, separando em “atos dirigidos contra um sistema de informática” e “atos que atentam contra outros valores sociais através de um sistema informático”, ou a classificação de crime informático puro ou impuro (ou próprio e impróprio) de Damásio de Jesus, classificação que por sua simplicidade, será utilizada neste trabalho. Embora o assunto ainda esteja em expansão, diversos autores, desde a década de 80 estudam-no, trazendo uma boa quantidade de material para auxiliar o desenvolver desta peça, cuja temática estudará o surgimento, classificação, espécies e efeitos do objeto, pela visão jurídica.

---

[1] Crimes de Computador.

Pelo seu caráter livre, torna-se muito difícil tutelar aqueles que se encontram vítima de crime virtual, pois a troca de informação é rápida e fácil, necessitando resposta igualmente rápida para combater a ação. Por isso, faz-se necessário um regramento especial para este tipo diferenciado de tipo.

No entanto, embora a legislação atual brasileira faça a tentativa de tipificar os crimes virtuais, sua interpretação deixa a desejar, deixando de lado os detalhes que tornam a utilização do meio virtual uma incógnita no ordenamento jurídico.

Em especial, o objeto deste trabalho é a conduta específica do sequestro de dados, crime que passou a se popularizar conforme a inclusão digital emergia no Brasil, atingindo não só o país, mas o mundo como todo. Todavia, a doutrina brasileira não tem consenso quanto ao tipo penal deste ato, sendo matéria de grande importância, porém de pouca discussão para decisivamente estabelecer a figura do crime.

Portanto, a pergunta a se fazer, que figura neste trabalho como o problema de pesquisa: o direito brasileiro tipifica corretamente o crime de sequestro de dados?

A hipótese apresentada para o problema do trabalho é não, pois embora o sequestro de dados seja considerado crime na legislação, não existe tipo específico para a conduta, que se encontra ligada a outros tipos do código penal, como o sequestro e a extorsão. No caso dos crimes virtuais em geral, não obstante o legislador ter realizado tentativas de incorporar o crime virtual no ordenamento brasileiro, as adições ao novo código penal são insuficientes para comportar a complexidade e variedade dos delitos cibernéticos. Atualmente, a legislação brasileira apenas prevê explicitamente parte dos “crimes de informática”, de forma limitada. Para encontrar a resposta para o problema apresentado, devemos considerar também a jurisprudência e os tipos penais existentes no que diz respeito à utilização dos meios virtuais para cometer os crimes. Com base no que já está apresentado nos novos tipos penais, o direito, embora admita a existência deste modo de crime, é remissivo quanto á aplicação do mesmo nos tipos já anteriormente existentes. Portanto, embora o direito esteja acompanhando o desenvolvimento tecnológico, necessita da profundidade que apresenta em outros tipos.

Assim, o presente trabalho almeja, como objetivo geral, explorar este tipo penal, buscando ressaltar suas peculiaridades que o tornam objeto de estudo, pela

interpretação da doutrina brasileira. Para tal, abordaremos percurso metodológico, especificamente, o qualitativo e hipotético-dedutivo, além de complementar com o método sistêmico, cada um com suas funções próprias. De forma a melhor organizar os tópicos a serem discutidos, dividiremos o raciocínio em três capítulos, cada um apresentando um objetivo específico, que se complementarão a fim de alcançar a referida meta.

Como primeiro objetivo, pretende-se conhecer do surgimento dos crimes virtuais, descrevendo a história dos meios cibernéticos e os primórdios da criminalidade da internet, além das definições dos delitos em estudo. Em seguida, para o segundo objetivo, deve-se explorar a legislação e jurisprudência quanto ao tema, apontando as medidas da justiça brasileira contra os crimes virtuais. Finalmente, como terceiro objetivo, almeja-se compreender o tipo do sequestro de dados em si, levantando exemplos e explorando a discussão quanto à tipificação da conduta para melhor compreender o posicionamento do Poder Jurídico quanto ao tema. Pelo desenvolvimento dos três capítulos, cada um com seu objetivo específico, analisaremos nosso objeto de estudo através de vários pontos de vista e campos de pesquisa, sem nos esquecermos do caráter jurídico do trabalho, mas abrangendo o foco o suficiente para a compreensão do raciocínio.

2 A HISTÓRIA E DEFINIÇÕES DE CRIMES VIRTUAIS

Antes de adentrarmos o estudo dos crimes virtuais pela perspectiva jurídica, é importante contribuir com o contexto histórico da evolução e desenvolvimento da característica base dessa espécie penal, que neste caso é a utilização do meio virtual.

2.1. O surgimento e evolução dos meios de informática

O estudo e desenvolvimento de tecnologias de informação e comunicação, em comparação a outras grandes invenções da história, é relativamente recente e breve, tendo seu auge nos 30 anos antes da virada do século XX. Ainda que breve, é considerada uma grande revolução, a Revolução Informacional, como pode-se chamar. Esta revolução se caracteriza pelo estudo e criação de mecanismos de processamento de dados, tendo seus primórdios em meados de 1940.

Esse estudo, no entanto, apenas atingiria seu reconhecimento e significância na Segunda Guerra Mundial, onde foi criado o primeiro computador, de uso militar e funcionando com uma série de válvulas. Era conhecido como *Colossus*, cuja função era a decodificação de transmissões inimigas. Após o término da guerra, John Mauchly e John Eckert apresentaram o ENIAC, um computador de uso comum com 30 toneladas e 2,75 metros de altura. Com a invenção do Transistor, possibilitando o processamento de impulsos elétricos com eficiência, foi criada a base para os chips e a microeletrônica, diminuindo as dimensões dos aparelhos e tornando seu uso mais prático. O primeiro computador com armazenamento de programas foi criado em 1947, o EDSAC e em 1951 foi lançado o computador comercial, o UNIVAC-1.

Em 1955, a força aérea dos Estados Unidos criou a primeira conexão entre computadores, um sistema de detecção, decisão e resposta em tempo real. O design dos chips foi aprimorado e foi produzido nos anos 60 o circuito integrado em miniatura, mais eficiente e barato. Ainda na época, a companhia IBM era líder da indústria com o computador Mainframe 360/370, um aparelho que ainda tinha grandes dimensões, sendo utilizado somente em grandes galpões. O modelo que possibilitava seu uso doméstico se chamava PDP-8, da empresa DEC, relativamente

menor. No fim da década, o primeiro computador eletrônico, o ESS-1 da *Bell Laboratories* foi produzido com o sistema operacional UNIX, possibilitando o acesso entre computadores. Mas isso era apenas possível através da ARPANET, uma rede de computadores patrocinada pela Agência de Projetos de Pesquisa Avançada do Departamento de Defesa dos EUA (DARPA).

O engenheiro Ted Hoff, no Vale do Silício (EUA), criou o microprocessador em 1971, possibilitando o processo de informação em qualquer aparelho e possibilitando o surgimento dos computares digitais e aposentando o computador analógico. Dois anos depois, Vinton Cerf da Universidade da Califórnia registrou o Protocolo de Controle de Transmissão / Protocolo Internet (TPC/IP), um código que permitiu a comunicação entre várias redes por programas e sistemas.

A partir de 1975, após o engenheiro Ed Roberts construir o Altair, os computadores passaram a ser em pequena escala, com microprocessadores e sistemas operacionais para mais facilmente interagir com o usuário. Nesse meio, Bill Gates e Paul Allen, estudantes da Universidade de Harvard criaram o sistema BASIC, especificamente para funcionar no Altair 8800. Em conjunto das duas tecnologias, em 1976, a *Apple Computers* lançou ao mercado os modelos *Apple I* e *Apple II*, os primeiros computadores de sucesso popular. Em 1981, a IBM inseriu para venda o tipo de computador mais popular da história, o Computador Pessoal (PC), cujo sistema operacional foi criado pela empresa *Microsoft* de Bill Gates, o famoso Sistema Operacional de Disco, ou MS-DOS. Neste mesmo ano foi lançada a primeira versão do *Windows*, possibilitando a interação do usuário com o computador através do *mouse*, e o emprego de imagens e janelas na tela.

Em 1984 houve a divisão da rede de escopo científico da DARPA na sua original ARPANET e a militar MILNET, e para conectar todas essas redes, foi operada pela Fundação Nacional da Ciência a rede das redes conexas, a INTERNET. Finalmente, Através da especialização do sistema operacional UNIX ao protocolo TCP/IP, em 1989 o Laboratório Europeu de Física de Altas Energias de Genebra, na Itália, criou a *World Wide Web* (WWW ou W3).

Diante dessa nova realidade da comunicação e do impacto social que a evolução tecnológica trazia, Bill Gates é citado como escrevendo: “Todos os computadores vão se unir para se comunicar conosco e por nós. Interconectados globalmente, formarão uma rede que está sendo chamada de estrada da informação” (GATES. 1995 p. 14).

Em pleno século XXI, é possível observar o quanto a evolução da tecnologia afetou o dia a dia do indivíduo: computadores estão em todos os lugares, com múltiplos tamanhos e funções. Com um toque, podemos nos comunicar com qualquer pessoa do planeta, capturar imagens, e ter acesso ao conhecimento de milhares de documentos e artigos. Esse acesso à informação, que décadas antes era descrita como ficção científica, permitiu-nos não só realizarmos tarefas de modo mais rápido e prático, como também nos proporcionou um modo diferente de nos vermos como sociedade. Em um mundo conectado, fronteiras e nações se parecem como algo ultrapassado, visto que qualquer pessoa com o uso das redes de comunicação pode se comunicar instantaneamente com outra do outro lado do mundo.

Claro, uma revolução cibernética como esta não veio sem custo, pois nunca se houve tantas privacidades escancaradas para o mundo ver como no fenômeno das redes sociais, que embora sejam um grande meio de comunicar e expressar-se, ao mesmo tempo expõem seus usuários que muitas vezes estão sujeitos a descuidos quanto a essa revelação de seus dados pessoais. Estas consequências foram inclusive previstas já em 1988, quando Nicolau Youssef e Paz Fernandez (1988, p. 49-50) escreveram: "Se não houver um nível satisfatório de reflexão a respeito da informatização da sociedade e das alterações por ela produzidas, pode-se caminhar para uma situação que ofereça graves riscos sociais."

Neste contexto, a utilização da informática como meio criminal é um passo lógico na evolução dos meios de comunicação, assim como se utilizam os telefones para se cometer crimes, o agente criminoso, em sua engenhosidade, especializou-se para fazer do computador sua ferramenta de delito. É neste meio que se relaciona a informática com o direito, não só ao informatizar os processos administrativos e judiciais, como também na utilização de meios eletrônicos pelo indivíduo autor de crime.

Em seus primórdios, os crimes virtuais eram mais limitados, visto que a função primária da informática, antes de sua expansão, era a coleta e acesso a informação e dados. Sendo assim os delitos tinham a dimensão jurídica mais isolada na responsabilidade civil quanto a danos causados pela disseminação das informações sigilosas e incorretas armazenadas eletronicamente. Claro, com a popularidade da internet e com a informatização dos bancos e lojas, os crimes virtuais ganharam uma nova dimensão, com ação da esfera penal sendo necessária,

além da preocupação com a segurança de dados pessoais, tendo em vista a grande vulnerabilidade dos usuários dos dispositivos. Os primeiros casos de crimes virtuais surgiram em documentos dos anos 60, embora ainda fossem incomuns, devido às limitações da época. Apenas na década de 80 a prática dos delitos seria comum.

2.2. Conceitos de Crimes Virtuais

A criminalidade informática possui características inerentes ao seu meio, que lhes concedem vantagens sobre outros tipos, como sua Transnacionalidade, visto que a integração de todos os países na internet permite que todos sejam alvo, independente de nível social e econômico. Outra vantagem é a Universalidade, pois os delitos são dependentes apenas da acessibilidade à computação, podendo vir de qualquer indivíduo. Finalmente, os crimes virtuais têm Ubiqüidade, estando presentes em todos os setores da sociedade.

Quanto aos autores, qualquer indivíduo com conhecimento de informática é capaz da conduta criminosa no meio virtual, embora exista a necessidade de especialização para realizar as condutas mais específicas. Por isso, os criminosos especializados nesse meio, capazes de utilizar com perícia as ferramentas de computador para realizar seu intento, são considerados autores atípicos, chamados genericamente de *hackers*. No entanto é de grande importância levar à atenção ao fato de que não são todos os *hackers* criminosos: o termo é na verdade melhor associado com o especialista em segurança de programas e redes de computador, que pode se utilizar de suas habilidades para auxiliar empresas e órgãos a combater invasões e proteger dados. De fato, muitos são empregados, cuja tarefa é testar as defesas de sistemas, para aperfeiçoá-los contra danos reais, embora alguns consideram o ato de invadir como mero passatempo, contanto que não exista dano ou subtração advinda de sua ação. Muitos *hackers* usam seus conhecimentos para combater criminosos reais, trabalhando em conjunto com autoridades policiais.

Em contrapartida, o agente criminoso por definição, o *hacker* não ético, é denominado *cracker*, que é facilmente confundido com o anterior pela semelhança entre os termos. O *cracker* é o indivíduo que além de invadir, subtrai e/ou depreda sistemas de computador para obter vantagens indevidas para si ou para outrem. Eles se valem de uma variedade de técnicas, não necessariamente complexas,

combinando tentativa e erro, limitações do servidor e engenharia social. Por isso torna-se ainda mais difícil sua identificação, visto que o número de pessoas capazes da prática de ilícitos é muito grande, ainda que existam muitos *crackers* capazes de golpes complexos e técnicas avançadas, mas estes conhecem os meios de se manter no anonimato, não importa a gravidade do dano.

Existem também os *phreakers*, que se especializam em crimes de telecomunicação, mais especificamente, contra linhas telefônicas e redes de celular, seja interrompendo o serviço, os utilizando clandestinamente, ou comercializando a sua utilização ilegalmente. Ao escrever sobre a relação destes com *crackers*, David Icove é citado por Vladimir Aras:

> Muitos *crackers* também são *phreakers*: eles buscam maneiras de fazer repetidas conexões aos computadores que estão atacando sem serem cobrados por estas conexões, e de certa forma isso faz ser difícil ou impossível o rastreio de suas chamadas por meios convencionais. [2] (ICOVE, 1995 apud ARAS, 2001, p.5)

Outra forma de grande potencial para dano, muito utilizada pelos autores de crimes virtuais, é pelo uso dos famosos vírus de computador, *worms*, e *trojan horses*[3]. Esses programas são um grande diferencial dos crimes virtuais, pois o vírus pode se espalhar indefinitivamente pela rede, atingindo um número indeterminável de pessoas. Não só isso, estes programas podem ser de uma multitude de funções, algumas mais danosas que outras, com o problema adicional de serem discretos, entrando nos sistemas desprotegidos, indetectados.

Conforme explanado, com suas vantagens, as redes de informação se tornaram um grande facilitador para os crimes virtuais, dadas as múltiplas maneiras de se praticar os delitos com a proteção do anonimato e dos escassos vestígios deixados, tornando sua repressão uma árdua tarefa. Como qualquer fenômeno de relevância, vários autores estudaram esse tipo de crime, dando vários conceitos e denominações quanto ao tema. Ainda assim, é difícil colocar a termo uma definição

---

[2] "Many crackers are also phreakers: they seek ways to make repeated modem connections to computers they are attacking without being charged for those connections, and in a way that makes it difficult or impossible to trace their calls using conventional means." (ICOVE, David. 1995. p. 423)

[3] *Worms* ou vermes, em português, são programas que se alastram de sistema em sistema de forma automática, infectando usuários e se reproduzindo. *Trojan Horses* são os famosos Cavalos de Tróia, são programas executáveis, normalmente disfarçados de jogos ou utilidades similares que ao serem abertos pela vítima, dão acesso ao *cracker* para conectar-se remotamente.

universal de crime virtual. No entendimento da Organização para Cooperação Econômica e Desenvolvimento (OECD) da ONU, são definidos os delitos de computador como “qualquer comportamento ilegal aético ou não autorizado envolvendo processamento automático de dados e/ou transmissão de dados”. Esta organização, desde 1983, procura um acordo para uniformizar a legislação sobre crimes cibernéticos no mundo. Conforme Antônio Celso Galdino Fraga, em 1986, foi publicado relatório intitulado *Computer-Related Crime: Analysis of Legal Policy* pela OECD no qual foi discutido o problema de criminalidade informática e a necessidade de tipificação das condutas de crimes específicos de computador.

É importante também destacar, conforme ensinamento de Ivette Senise Ferreira (1992, p.142), que é característica fundamental, para configuração do crime, a tipicidade da conduta. Em outras palavras, as características dos crimes virtuais são a conduta típica e antijurídica e o objeto ou ferramenta do delito como sistema informatizado. Todavia, ainda se encontram condutas que não possuem tipicidade, mas ainda possuem caráter antijurídico de acordo com o ordenamento jurídico brasileiro.

2.3. Classificando os crimes virtuais

Quanto à classificação, houve tentativas de diversos autores para implementar um sistema apropriado, com diferentes critérios para procurar melhor efetividade. Dentre estes, podemos destacar o sistema de forma de atuação do autor, por Ulrich Sieber, citado por Maria Helena Reis (1997, p.29), estabelecendo que os crimes eletrônicos podem ser: de Fraude por manipulação de computador contra um sistema de processamento de dado; Espionagem informática e furto de *software*; Sabotagem informática; Furto de tempo; Acesso não autorizado; Ofensas tradicionais. Em contrapartida, Marc Jaeger utilizou a expressão “Fraude Informática” para designar atos ilícitos cibernéticos, classificando-os simplesmente em Fraudes propriamente ditas e Atentados à vida privada. Em outro ponto de vista, Jean Pradel e Cristian Feuillard tomaram como foco o objetivo do crime, limitando-se a crimes contra sistemas eletrônicos: classificaram as finalidades como para obtenção de dinheiro e obtenção de informações, um sistema inteligente, mas que foi criticado por não levar em conta os crimes cujo objetivo é danificar o aparelho, sem obter vantagem.

O sistema mais celebrado, utilizado em doutrinas internacionais é o Sistema Binário proposto por Hervé Croze e Yves Bismuth, dividindo os crimes virtuais tão somente em: Atos dirigidos contra um sistema de informática, independente da motivação do autor; e Atos contra outros valores sociais através de um sistema informático. Desse sistema, é interessante observar a existência de duas situações distintas, nas quais uma delas é a utilização de sistema informático, como instrumento da ação, para atentar contra outro bem jurídico, ou seja, o objeto da ação. Em contrapartida, a outra situação é de ato praticado contra sistema de informática, sua integridade, ou os dados contidos nele, sendo este, nessa hipótese, o objeto da ação. Ou seja, temos dois casos, nos quais existe sempre ato praticado com o uso de computador, a diferença sendo no objeto lesado pela ação, podendo ser o sistema de informática instrumento, meio e objeto ao mesmo tempo.

O Sistema Binário inspirou muitos autores, que passaram a concordar majoritariamente com sua classificação. No âmbito nacional, Luís Flávio Gomes dividiu de forma semelhante os crimes informáticos, entre crimes praticados contra o computador em sentido amplo e crimes por meio de computador. Neste sentido, é mais famosa a adaptação de Damásio de Jesus, que classifica crimes virtuais em puros e impuros ou próprios e impróprios. O primeiro tem como o meio um sistema eletrônico, e seu resultado se opera também em sistema eletrônico, ou seja, o sistema é meio e também obejeto protegido. Os impuros ou impróprios são aqueles em que o sistema de informática é instrumento para a prática de ato lesivo contra outros bens protegidos não relacionados com os de informática, protegidos por outras normas penais. Desta classificação binária destes autores, nota-se um padrão da classificação dos delitos: existem crimes denominados como Crimes de Informática, aqueles que são específicos de computação, em que o computador é meio e objeto ao mesmo tempo, ou seja, em que necessariamente o objeto lesado será contido em aparelho eletrônico. Os demais crimes, tentativamente chamados de Crimes Comuns, são aqueles em que o computador é meio da prática do delito, mas a conduta e seu objeto se encaixam em tipo penal existente, com o diferencial do meio virtual. Por exemplo, o crime de invasão de sistema seria Crime de Informática, visto que o objeto lesado necessariamente teria que ser contido em sistema de informática, enquanto o agente que propõe proposta fraudulenta através de correio eletrônico comete Crime Comum, o de fraude, com o diferencial sendo o meio utilizado.

Ao constatar a predominância de sistemas binários de classificação, João Araújo Monteiro Neto e Francisca Jordânia Freitas da Silva buscaram um sistema que não somente separasse Crimes de Informática e Crimes Comuns, e reformularam a classificação de crimes virtuais utilizando critérios quanto aos efeitos e quanto aos objetivos. Quanto aos efeitos, os delitos podem ser divididos entre Crimes eletrônicos de efeitos tangíveis e Crimes eletrônicos de efeitos intangíveis. Os primeiros relacionam-se aos atos praticados no meio virtual cujos efeitos se consumam diretamente no mundo real, enquanto os efeitos intangíveis são causados pelos crimes que causam dano somente aos dados imateriais do sistema informacional, ou armazenados em rede. Quanto aos objetivos, podem ser classificados como Crimes eletrônicos de mero acesso e Crimes eletrônicos de dano ou lesão. O primeiro se consuma simplesmente com o acesso à rede ou sistema, não necessitando de nenhum outro efeito ou ato. O segundo, por outro lado, é o ato de diretamente lesar o aparelho, ainda que não seja para obter vantagem para o autor ou terceiro.

Em conclusão quanto às maneiras de classificar os crimes virtuais, embora não haja uma forma definitiva de se utilizar estes sistemas, não se pode negar o valor doutrinário e didático das ideias inseridas nestes. Cumprindo ressaltar quanto à diferença dos Crimes de Informática e os Crimes Comuns, uma vez que para o estudo dos crimes de computação, todavia haja a necessidade de foco no primeiro, os Crimes Comuns não podem serem considerados como crimes virtuais, visto que estes já possuem tipificação de suas condutas, servindo seu estudo como causa para anexar à definição existente a situação diferenciada do uso de computador. Os Crimes de Informática, embora tenham o fator comum do instrumento do delito, são situação totalmente à parte, não devendo ser confundidos, sob perigo de confusão de direito.

No Brasil, a chamada revolução informática data da década de 90, sendo fato muito recente, o país ainda está em pleno processo de informatização, afetando todos os aspectos sociais e, segundo German (2000), causando um novo fenômeno de exclusão social, entre a elite com suas máquinas pessoais e o excluído desconectado. Independente disso pode-se dizer que os órgãos do estado e suas empresas já estão inseridos no espaço virtual, com grande eficiência, como se pode ver pelo sistema bancário nacional e a rede de previdência social, por exemplo. Claro, nosso país não é alheio aos perigos da informatização, visto que o Brasil já

possui sua variedade de crimes em detrimento de bens virtuais e de dados protegidos digitalmente, embora as prioridades dos órgãos de investigação sejam a proteção do sigilo de informações guardadas em entes públicos e a proibição de interceptação de dados eletrônicos, ou seja, salvaguardar o direito a privacidade e intimidade. Também é foco de proteção os direitos do autor, embora o sucesso dessa ação seja a grande custo, visto que com a internet, a disseminação de dados protegidos é uma garantia, pela facilidade de cópia causada pelo computador.

De acordo com a constituição brasileira, em seu artigo 5º, dispõe quanto à igualdade de todos perante lei, sem qualquer distinção, garantindo aos brasileiros e estrangeiros residentes no país a inviolabilidade dos direitos à vida, à liberdade, à igualdade, à segurança e à prosperidade. Seu inciso IV indica que “é livre a manifestação do pensamento, sendo vedado o anonimato” caso que não se aplica à internet, sendo verdadeira “terra de ninguém”, pois sua estrutura facilita o anonimato, trocando nomes por apelidos. Com o anonimato, qualquer usuário fica livre pra expressar seus pensamentos, pelo bem ou pelo mal, podendo serem fraudulentos e agressivos. Os incisos X e XII consagram a proteção constitucional da inviolabilidade da intimidade , da imagem e da honra, além dos dados pessoais de comunicação, outro caso cuja eficácia é limitada diante da informatização, que incentiva à exposição de sua informação para melhor comunicação entre círculos sociais, mas termina por ser um grave risco de invasão de privacidade. Pela violação desses princípios da constituição tomar uma forma tão gravosa, existe significativo debate quanto à extensão desses direitos. Neste mérito, Monteiro (2009) explica:

> Numa afirmação simples e direta podemos relacionar os direitos à intimidade e à vida privada com os traços ou elementos reveladores da forma de vida, costumes, preferências ou planos das pessoas (esfera de sua conduta e modo de ser não realizada perante a comunidade). Assim, admitindo a existência de distinção entre intimidade e vida privada, premissa não aceita por inúmeros juristas que advogam uma identidade entre as noções, podemos considerar que intimidade envolve informações e relações em âmbito extremamente restrito e vida privada, por sua vez, considera informações e relações pessoais mais abrangentes, mas ainda não inseridas no universo das relações sociais perante a comunidade [...].

Deve-se ressaltar de que o direito à privacidade deve proteger não só o acesso à informações pessoas, como também garante a inviolabilidade da tranquilidade do indivíduo na sua esfera íntima da vida privada, ou seja, pela interpretação do direito à privacidade, é ilegal a perturbação do lar, como ambiente

privado da pessoa humana. Dito isso, segundo relatório de fraude da *RSA Anti-Fraud Command Center*, divisão de segurança da corporação ECM2, o Brasil é o 4º colocado na lista de países com mais fraudes corporativas digitais no mundo, ficando atrás dos EUA, Reino Unido e Índia, com aumento na tendência do roubo de identidade. Isso porque o crime é facilitado pela exposição de alto risco dos usuários de redes sociais, pois conforme avisa Guerra (2013), da Universidade Federal de Pernambuco (UFPE), ao se colocar uma informação na internet, ela não pode ser apagada. No máximo, existe a possibilidade de ocultação, mas os servidores guardam qualquer informação publicada pelos usuários, mesmo que estes não saibam. Portanto a única maneira de evitar a exposição é o não fornecimento das informações. Complementa:

> Os mais *experts* também conseguem navegar por esses arquivos ocultos na chamada *deep web*, que tem um conteúdo superior, e que os mecanismos de busca padrão não conseguem acessar em uma simples pesquisa. Por isso, oriento as pessoas a, de vez em quando, fazerem uma varredura para descobrir se tem algum lugar armazenando os seus dados.

O primeiro autor a tratar de camadas da internet, foi Bergman, em 2001, que compara a pesquisa na internet como jogar uma rede de pesca no oceano: Você consegue pescar o que está na superfície, mas o maior conteúdo está sempre mais fundo. Bergman trata da internet comum pelo nome de *surface web*, onde a maioria dos internautas pode acessar páginas do índice normalmente e não é necessário grande conhecimento técnico para sua navegação. É nesta parte da rede que empresas realizam vendas, universidades disponibilizam informações, jornais publicam notícias, ou seja, onde o tráfego é livre e conhecido por seus usuários. Crimes cometidos na *surface web*, embora de difícil responsabilização, podem ser rastreados com perícia.

A *deep web*, ou rede profunda, em contrapartida, é um dos assuntos mais complexos ao se falar sobre a punibilidade de crimes virtuais. É de difícil acesso a usuários comuns, pois seu conteúdo é oculto e os endereços eletrônicos não podem serem acessados sem procedimentos específicos, na *deep web* se escondem informações do mais alto escalão do governo e de agências de inteligência e militares, pelo seu sigilo absoluto. Infelizmente, é também esconderijo das atividades ilícitas de agentes criminosos mais especializados e inescrupulosos, que pela proteção da *deep web*, não temem a persecução criminal. De fato, é extremamente

difícil o rastreio de criminosos escondidos nessa rede oculta, cujo nome não poderia ser mais apropriado: Deve seu nome ao fato de ser muito maior de que se imagina, pelo menos milhares de vezes o tamanho da internet normal. Qualquer lei que o poder legislativo criar será de difícil ou impossível execução em relação a esta camada da internet, visto que se a *surface web* é de tutela escassa, aqui ela é inexistente.

Em suma, os crimes virtuais, embora possuam uma história recente, assim como o desenvolvimento do computador, possuem uma acelerada expansão, que o direito precisa lutar para acompanhar, sob pena de cair na impunidade. Parte dessa ideia a opinião do professor de ciências, Arandas (2013):

> Tudo no meio virtual é muito rápido e a legislação não consegue acompanhar. Além disso, o maior problema não é o sistema, são os usuários. Quanto mais a gente acessa, mais nos expomos. Mas, se tomarmos todos os cuidados necessários, há como minimizar muito os riscos de uma informação ser mal utilizada.

A mais nova legislação quanto aos crimes virtuais está no novo código penal, inserida pela Lei 12.737/2012, conhecida como Lei Carolina Dieckmann, baseada no projeto da Lei Azeredo, que tramita no congresso desde 1999. Mas como qualquer fenômeno de relevância atual, ainda pode mudar muito o tratamento dos crimes virtuais, que por enquanto, está em sua infância na doutrina brasileira.

3 A LEGISLAÇÃO E DOUTRINA BRASILEIRA

De antemão, é de imperativa importância destacar a linha de pensamento adotada por este trabalho, em relação à definição do tipo e interpretação da norma. Para este propósito, segue-se o pensamento de Brandão (2010) e Mayer (1951) para com a definição de tipicidade. O tipo assim é o conjunto de elementos que descrevem o delito. Na verdade, não só uma descrição do crime, como também uma imagem ou modelo da conduta incriminadora. A tipicidade é a relação da conduta humana e o tipo, sendo as condutas desprovidas de tipo penalmente irrelevantes.

> Para Mayer, o tipo penal não pode ser considerado como uma mera descrição objetiva, por conta da existência dos elementos normativos do tipo, que são uma conexão entre a tipicidade e a antijuridicidade. Um exemplo de um elemento normativo é a inclusão da qualidade de *alheia* à coisa, no furto. Esse elemento é normativo porque somente pode ser compreendido através de uma valoração, decorrente do direito de propriedade. Por conseguinte, o caráter alheio da coisa decorre do Direito, não sendo uma simples descrição isenta de valoração. (BRANDÃO, 2010, p.161)

O tipo é uma construção abstrata da conduta traduzida em expressões linguísticas, cujo fulcro é individualizar os atos relevantes ao Direito Penal. Ao fazermos a análise do tipo, nosso método utilizará de três planos: valorativo, da linguagem e da realidade. No plano valorativo estuda-se o tipo com referência ao bem jurídico, analisando o dano da conduta ao objeto protegido pela norma e seus efeitos, sendo causa de agravamento ou amenização, até a aplicação do princípio da insignificância. O plano da linguagem leva em consideração a descrição da conduta feita através de elementos descritivos de linguagem, que podem ter maior ou menor êxito, generalizando e abstraindo a conduta criminosa. Finalmente, o plano da realidade estuda o substrato material do tipo, ou seja, os elementos do fato: sujeitos ativo e passivo, objeto material e elementos objetivo e subjetivo.

Os elementos objetivos do tipo são simples em sua compreensão, pois o tipo como modelo contém um verbo nuclear para identifica-lo. O elemento objetivo é representado pelos efeitos no mundo exterior, da ação do crime. O elemento subjetivo se refere à consciência e vontade do agente, presentes em todos os tipos. A teoria finalista da ação caracteriza-se ao acentuar a importância desses fatores para a culpabilidade da conduta, descrevendo o tipo penal como ação combinada ao

dolo e culpa. Além destes, a doutrina também reconhece a existência do dolo específico, ou elementos subjetivos de injusto, que se diferem dos demais por existirem de modo implícito no tipo e se referem a estados e ações específicas do agente. Como exemplificado por Brandão (2010, p.169), ao referir-se ao art. 159 do código penal, que diz: “Sequestrar pessoa, com o fim de obter qualquer vantagem, como condição ou preço do resgate”, o propósito do agente de “obter qualquer vantagem” é fundamental para configurar o crime, e é exemplo de elemento subjetivo do injusto.

3.1. Origens da Legislação Brasileira dos Crimes Virtuais

No Brasil, inicialmente os crimes virtuais foram considerados pela doutrina como ramo do direito penal econômico, pois a preferência era dada à proteção de programas de computador, para defender os direitos autorais das empresas multinacionais que os desenvolviam, como foi editado na Lei 7.646/87. Depois foi adicionada pela Lei 8.137/90, que rege sobre os delitos contra a ordem tributária, o crime de “utilizar ou divulgar programas de processamento de dados para fins de sonegação fiscal”. Em 1995, a Lei 9.100 dispôs dos crimes de informática que atentavam contra as eleições, com os tipos de do artigo 67, incisos VII e VIII.

A edição da Lei 9.983/00 trouxe novos artigos no Código Penal para proteger dados e sistemas de informações, conforme consta o artigo 313-B, crime próprio de funcionário público que penaliza a modificação de sistemas informáticos da Administração Pública, ou que divulgue informações sigilosas de bancos de dados oficiais, de acordo com o artigo 153, §1-A do Diploma Penal. Mas mesmo com estes institutos, existia uma deficiência legislativa quanto ao assunto, conforme cita Mazoni (2009), que é expressa por jurisprudência do STF, ao julgar o HC nº 76.689:

> CRIME DE COMPUTADOR: PUBLICAÇÃO DE CENA DE SEXO INFATO JUVENIL (E.C.A., ART. 241). MEDIANTE INSERÇÃO EM REDE BBS/INTERNET DE COMPUTADORES, ATRIBUÍDA A MENORES: TIPICIDADE: PROVA PERICIAL NECESSÁRIA À DEMONSTRAÇÃO DA AUTORIA: HC DEFERIDO EM PARTE. 1. O tipo cogitado - na modalidade de 'publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente' - ao contrário do que sucede por exemplo aos da Lei de Imprensa, no tocante ao processo da publicação incriminada é uma norma aberta: basta-lhe à realização do núcleo da ação punível a idoneidade

> técnica do veículo utilizado à difusão da imagem para número indeterminado de pessoas, que parece indiscutível na inserção de fotos obscenas em rede BBS/Internet de computador. 2. Não se trata no caso, pois, de colmatar lacuna da lei incriminadora por analogia: uma vez que se compreenda na decisão típica da conduta criminada, o meio técnico empregado para realizá-la pode até ser de invenção posterior à edição da lei penal: a invenção da pólvora não reclamou redefinição do homicídio para tornar explícito que nela se compreendia a morte dada a outrem mediante arma de fogo. [...] (SUPREMO TRIBUNAL DE JUSTIÇA, 1998, p.3)

3.2. Legislação brasileira atual

A importância de legislar sobre os crimes virtuais não foi destacada até maio de 2012, quando circularam pela internet imagens íntimas da atriz Carolina Dieckmann, pela ação de criminosos cibernéticos. O caso obteve grande repercussão e impacto social, e abriu o caminho para a edição da Lei nº 12.737, do fim de 2012, que foi apelidada de “Lei Carolina Dieckmann”, que dispôs sobre a tipificação dos delitos informáticos e editou a redação de artigos pré-existentes do Código Penal brasileiro.

Antes do ocorrido, sem legislação específica, a apuração de crimes virtuais era muito difícil, pois a legislação vigente tratava dos crimes de forma geral, sem considerar o meio utilizado para sua prática. Sem tipos adequados aos delitos, se utilizava da lei comum por analogia, usando o Código Penal, Estatuto da Criança e do Adolescente (Lei nº 8.069/90), e a Lei de Segurança Nacional (nº 7.170/83). Também se adequava a Lei dos Crimes de Software (nº 9.609/98), também conhecida como lei antipirataria, que tem boa contribuição contra crimes cibernéticos, ainda que de forma limitada. Esta lei em seu 1º artigo define a expressão “programa da computador”:

> Programa de computador é a expressão de um conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de qualquer natureza, de emprego necessário em máquinas automáticas de tratamento da informação, dispositivos, instrumentos ou equipamentos periféricos, baseados em técnica digital ou análoga, para fazê-los funcionar de modo e para fins determinados. (BRASIL, 1998)

O restante da lei antipirataria, no entanto, tem como foco os direitos autorais de programas de computador, tendo utilidade limitada no contexto geral dos crimes virtuais. O tipo único descrito nesta lei é o do artigo 12, o crime de violar o direito do autor de programa de computador. Importante salientar que incorre da

pena o agente que reproduz o programa, em todo ou em parte, para fins comerciais ou não. Interessante que exista a Lei nº 9.610/98 (Lei dos Direitos Autorais) em paralelo à lei antipirataria, pois ambas tem o mesmo objetivo, tendo pouca diferença. A diferença real da Lei nº 9.609 é o contexto cibernético. Embora ainda preveja a aplicação subsidiária da nº 9.610, somente pelo meio do crime cibernético, é preciso uma lei específica para regular os variados meios de quebra dos direitos autorais de programas de computador.

A lei nº 12.737 dispõe sobre a tipificação dos crimes de informática, acrescentando os artigos 154-A e 154-B ao Código Penal, além de editar a redação dos artigos 266 e 298. O artigo 154-A dispõe sobre o crime de Invasão de dispositivo informático, crime comum, cujo bem jurídico alvo é a liberdade, privacidade e intimidade da vítima. O artigo descreve o tipo como invasão de dispositivo informático, conectado ou não à rede, mediante violação de seus sistemas de segurança, para obter, modificar ou destruir seus dados ou informações, ou para tornar o sistema vulnerável e passível de outras vantagens indevidas, claro, sem a autorização expressa ou tácita do titular do dispositivo. No §1º, em sua forma equiparada, pratica do mesmo crime aquele que produz, vende ou distribui programas ou dispositivos com o propósito de ajudar nos atos descritos no caput. Destaca-se que a forma do crime do caput é crime formal, sendo apenas necessária a invasão para consumar o crime, diferente da sua forma equiparada, que é crime material.

O artigo também prevê diversas formas qualificadoras do delito, aumentando a pena nos casos de prejuízo econômico, obtenção de segredos industriais ou comerciais ou outras informações sigilosas, e ao possibilitar o controle remoto do dispositivo. Aumenta-se a pena ainda no caso da comercialização dos dados e informações obtidos ilicitamente e nos casos do crime ser praticado contra representantes do estado e da administração direta e indireta. O artigo 154-B trata da ação penal adequada a esses delitos, na qual esta procede somente mediante representação, excetos nos casos dos crimes praticados contra a administração pública ou os Poderes da União, Estados, DF, Municípios e empresas de serviços públicos.

As alterações propostas pela lei aos artigos 266 e 298 do Código Penal foram simples, meramente incluindo a possibilidade do meio eletrônico na prática dos tipos de Interrupção ou perturbação de serviço telegráfico, telefônico,

informático, telemático ou de informação de utilidade pública e de Falsificação de documento particular. No primeiro artigo, foi adicionado parágrafo para descrever a forma equiparada do tipo, adicionando os serviços telemático e de informação entre objetos do tipo. O segundo artigo dispôs que para os fins de Falsificação de documento particular, equipara-se o cartão de crédito ou débito a documento particular.

A Lei 12.737, embora curta em conteúdo, representa um grande avanço ao combate de crimes virtuais, abrangendo fortemente os crimes de informática em suas diversas facetas. Não só isso, representa também o aumento da preocupação do Legislativo com a segurança e proteção do âmbito digital. No entanto, não se pode deixar de comentar que esta abrange apenas uma das espécies de crime virtual, classificados em duas metades do gênero, ainda existe uma deficiência na tipificação dos crimes comuns em sua forma cibernética. Ademais, ainda é necessário esclarecimento quanto à aplicabilidade do que a lei dispõe, visto que esta se posiciona muito subjetivamente e de forma geral a esses delitos, necessitando de especificação da norma para funcionar plenamente, principalmente pela grande quantidade de termos especiais de informática que esses tipos deverão utilizar para serem eficazes. Seria preciso a criação de um verdadeiro novo ramo de direito, especializado em direito digital, pois este é o maior problema para o combate aos crimes virtuais atualmente, a não existência do direito especializado, em face da gravidade desses delitos. O Ministro Costa Leite (2011) do STJ, reconheceu esta deficiência, comentando sobre a dificuldade de punir os delitos.

Além da dificuldade em identificar o crime, a ação penal também sofre, com a proposta da lei sendo na linha da ação penal privada, muitas condutas inseridas no meio virtual vão ter seu efeito multiplicado quando praticadas em domínio público, gerando múltiplas ações individuais, advindas de múltiplos lugares, pela vantagem multiterritorial da rede afetada, gerando um grande desafio no julgamento do crime. Conforme o artigo 6º do código penal considera-se o local do crime onde ocorreu a ação, em todo ou parcialmente assim como onde se produziu ou deveria se produzir o resultado. No caso da transnacionalidade da conduta, ambos os países deverão concordar com a interpretação da pena, mas surge um problema quando a conduta praticada não é punível em todos os países afetados. Este seria apenas solucionado por tratado, sob a pena violar o artigo 4º, III da constituição federal, que versa sobre a autodeterminação dos povos.

A identificação do agente nem sempre será certa, pois o meio virtual facilita o anonimato e torna desnecessária a proximidade e interação do agente com o objeto atentado pelo crime. Os elementos para a persecução criminal, no caso dos crimes virtuais, segundo Ana Mara dos Santos, deverão ser os IPs, ou seja, os endereços da máquina que enviou e da que recebeu os dados, que podem ser rastreados para sua localização. É um método preciso, porém nem sempre eficaz, pois o IP pode levar até a máquina utilizada, mas se o autor se utilizou de computador alheio ou de lugares de acesso público, como bibliotecas ou *lan houses*, de pouco adianta. O único método certo para a identificação do agente é na possibilidade deste precisar utilizar elementos corporais para obter acesso ao dispositivo e rede, isto é, mecanismos que necessitem de identificação biométrica do indivíduo, como a leitura de impressão digital ou análise da voz.

Aqueles que expressam a opinião de que a internet necessita de maior regulamentação e censura, para suprir a necessidade de ordem e auxiliar o estabelecimento de medidas preventivas contra a criminalidade encontram forte oposição, pois a maioria dos usuários vê o controle de conteúdo como opressão à liberdade virtual, principalmente após tentativas fracassadas de governos em restringir o acesso ou volume de informação de usuários. E sem dúvida, com a restrição de dados existiria uma crise moderna de dependência de internet, com prejuízo para o povo. Seria preciso mudança sensível para satisfazer ambos o judiciário e os usuários, uma difícil façanha. Majoritariamente, os usuários encaram a mão do estado na rede como uma grande inconveniência. Conforme dita Rutherford (2016), o ciberespaço é regido por um sistema que vai além do liberalismo, a ponto de aproximar-se a uma anarquia, onde a interferência do governo é vista como inaceitável. Nesta sociedade cibernética, vemos um retorno ao estado de natureza, ou seja, sem lei. Realmente, a liberdade exacerbada do mundo informático pode ser visto muitas vezes como o velho oeste moderno: uma terra sem lei, tutelada apenas pelos seus próprios usuários e moderadores seletos.

3.3. Crimes comuns no âmbito virtual

Como existem crimes virtuais não descritos em lei específica, mas o poder judiciário não pode ser ausente na apreciação dos crimes contra o direito, o código penal é frequentemente utilizado. Como já comentado neste trabalho, na falta

de tipo perfeito para os crimes virtuais, procura-se aquele que melhor se adequar ao fato do crime, que é o caso dos crimes comuns, praticados por meios virtuais.

Devemos observar como cada interpretação do tipo se modifica ao mudar-se o método da ação praticada, como por exemplo, no caso dos crimes contra a vida, que não são imaginados no âmbito cibernético com frequência, pois o meio digital acrescenta distância ao agente de sua vítima. Claro, o atentado à vida neste caso poderá apenas ser executado indiretamente, pelo induzimento ao erro ou suicídio. Ramos (2008), neste sentido, oferece um bom exemplo de indução ao erro: O agente invade o sistema de computadores de um hospital e modifica o remédio ou dosagem a ser aplicado à sua vítima, fazendo o médico ou enfermeira aplicar a medicação erroneamente, matando o paciente. No caso do suicídio, pode ser considerado o exemplo da assistência ao suicídio, em que o agente sugere a vitima a suicidar-se ou a orienta sobre o procedimento, se utilizando dos meios de comunicação da internet. Pode-se considerar nesse exemplo os casos de *cyberbullying* em seu estágio grave, em que a vítima do abuso pelas redes sociais é levada a cometer tais atos. Nestes casos, a conduta pode ser tipificada nos artigos 121 e 122 do código penal.

Mais comuns na internet, em redes sociais e bate-papo, os crimes contra a honra, calúnia, difamação e injúria, dos artigos 138, 139 e 140 do código penal, são de fácil consumação no âmbito virtual. Os meios de comunicação proporcionados pela informática permitem a rápida divulgação de comentários com potencial lesivo à imagem do indivíduo, sobretudo em comunicação aberta e pública. Existem inúmeros exemplos de como poderiam se consumar estes três crimes, principalmente em sua forma escrita, que facilita a prova e persecução penal cabível. Quanto a esta espécie, é importante atentar que a retratação é cabível para excluir sua punibilidade, contanto que esta seja completa e inequívoca, além de pública, para que não reste dúvida ou dano a ser causado.

Os crimes contra a liberdade pessoal também são possíveis no meio cibernético, nos casos de Constrangimento Ilegal (art. 146, CP) e de Ameaça (art. 147, CP). Ambos teriam que ser praticados de forma similar aos crimes já comentados, por meios de comunicação do âmbito cibernético. O constrangimento ilegal se faz pela violência ou grave ameaça, portanto, no caso do crime digital, apenas pela grave ameaça, por exemplo, no caso do agente que obtém favor de sua vítima ao ameaça-la de denunciar às autoridades crime cometido por esta. A

ameaça do art. 147 se faz pelo simples anúncio de intenções danosas pelo autor do crime à pessoa ou patrimônio da vítima, facilmente traduzido em meio virtual para sua consumação.

Os crimes contra a inviolabilidade de correspondência e dos segredos são similares em sua ação na espécie de delito, mas existe uma ressalva quanto ao primeiro bem tutelado: apesar do artigo 151 do código penal tratar do crime de violação de correspondência, segundo argumento doutrinário, é impossível a analogia para a proteção da correspondência virtual, ou *e-mail*, pelo princípio da reserva legal, pois a lei não prevê a proteção deste. Todavia, no caso dos artigos 153 e 154 do código penal, os crimes de Divulgação de Segredo e de Violação de Segredo Profissional, são possíveis no meio virtual, em suas formas descritas no tipo. Basta a publicação de mensagem com informação considerada confidencial, e no segundo tipo, que a informação tenha sido confiada ao autor do crime por razão de sua função, ministério, ofício ou profissão. Ambos os crimes, para se consumarem, deverão produzir dano, para confirmar a importância da confidencialidade da informação.

Muito praticados na internet, os crimes contra o patrimônio se tornaram um temor presente para todos os usuários do *internet banking*, serviço bancário conectado pela internet, bastante utilizado por sua conveniência pelo usuário não precisar se deslocar a uma agência ou se preocupar com horários de funcionamento. Neste cenário o Furto (art. 155, CP) é muito comum, visto que ao invadir o sistema bancário, o criminoso pode transferir valores das contas alvo sem a permissão de seus titulares. No crime de Extorsão (art. 158, CP), a vítima é ameaçada pelo dano em potencial da invasão do agente, com o intento de obter vantagem econômica, por exemplo, o *cracker* que ameaça excluir todos os arquivos do sistema da vítima, caso esta não o dê determinada quantia. O crime de Dano (art. 163, CP) merece destaque, pois no âmbito virtual, existe um bem tutelado que é único e próprio deste: os dados de informação. Ao invadir, ou infiltrar programas maliciosos, com a intenção de destruir dados do dispositivo alvo, o agente pratica este crime, embora exista uma dificuldade em dizer quanto a gravidade deste dano, pois os dados podem conter virtualmente qualquer tipo de informação, de contas bancárias a vídeos e fotos. Dependendo de quanto foi danificado, é difícil calcular o quanto se perde na conduta praticada. Também é comum o crime de Estelionato (art. 171, CP), que geralmente explora a ingenuidade ou falta de conhecimento

específico de internautas. O envio de *e-mails* suspeitos, clonagem de *sites*, esquemas falsos, todos estes artifícios são meios deste tipo, em que o agente procura enganar sua vítima, para obter vantagem econômica indevida, ou dados pessoais alheios. Esta espécie de crime foi e continua sendo utilizada conforme a sociedade procura incluir-se na era da informação, aproveitando-se do usuário desavisado.

No mundo cibernético também pode ser cometido crimes contra o sentimento religioso. Mais especificado no artigo 208 do código penal, significa publicamente ridicularizar alguém por sua crença, algo de fácil execução por meio da comunicação virtual, similar aos crimes contra a honra, porém com a diferença de que este crime é mais difícil de se identificar. É necessária a dedicação do juízo e provas inequívocas do excesso da liberdade de pensamento, para não cair na impunidade do ato.

Os crimes contra os costumes, como Favorecimento da Prostituição (art. 228, CP) e Ato Obsceno (art. 233, CP) também estão presentes, o primeiro podendo ocorrer com o verbo “incitar” e “facilitar”, como nos exemplos do incentivo de prostituição pela troca de mensagens, e da manutenção de *site* para intermediar e facilitar o ato. O crime de ato obsceno no contexto cibernético tem o requisito de que o ato seja publicado em local inadequado, de modo que qualquer pessoa tenha acesso à visualização da conduta praticada, ainda que não a busque diretamente, como numa rede social ou fórum.

Como em crimes já explorados neste trabalho, os crimes contra a paz pública podem ocorrer no âmbito virtual com a mesma facilidade, a Incitação ao Crime (art. 286, CP) pelo simples incentivo ao crime em publicação visível em rede; a Apologia de Crime (art. 287, CP) ao ensinar amigos na internet como praticar ações ilícitas; e Formação de Quadrilha (art. 288, CP) pela reunião, não necessariamente digital, de três ou mais pessoas para prática de crimes digitais.

Também frequente é o crime contra a fé publica de Falsa Identidade, disposto no artigo 307 do código penal, pela facilidade trazida pelo anonimato na internet, que dificulta a obtenção de provas e a persecução e identificação do agente. É comum o praticante deste delito criar nomes, apelidos e endereços falsos, com a intenção de praticar outros crimes virtuais e desaparecer sobre a proteção da identidade que criou.

Além dos tipos apresentados anteriormente existem muitos outros que podem ser adequados ao âmbito cibernético, como crimes contra a administração, contra a criança e adolescente, contra a segurança nacional, entre outros. E é pela quantidade destes delitos que se percebe a importância de especificar esta adaptação tecnológica do crime em lei, além de providenciar os métodos de persecução criminais cabíveis. Além dos artigos presentes no código penal, também devemos comentar a proteção do artigo 5º da Constituição Federal, sobre os direitos fundamentais da pessoa humana, especificamente o inciso X:

> Art. 5.º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> (…)
> X – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; (…). (BRASIL, 1988)

Com efeito, o direito de inviolabilidade da intimidade e vida privada se presta a assegurar a todos a proteção dos dados e informações que desejem preservar e manter confidencialidade e sejam próprios de sua esfera privada. Ainda como direito fundamental está prevista no inciso LXXII do mesmo artigo a ação de *habeas data*, promovida por aquele interessado ao acesso de suas informações registradas, assegurado o conhecimento delas, além dos registros e bancos de dados do estado ou públicos, além de poder retificar estas no caso de erros.

A proteção da vida privada e intimidade é de grande importância na doutrina jurídica brasileira, existindo artigos esparsos que complementam esta proteção, como o artigo 21 do Código Civil que além de reforçar a inviolabilidade do bem jurídico, responsabiliza o judiciário para tomar medidas necessárias para impedir atentados a este direito. O artigo 186 do mesmo tomo dispõe que a violação do direito é passível de indenização por danos materiais e morais. No Código de Defesa do Consumidor, em seus artigos 43 e seguintes, prevê que o consumidor deverá ser informado sobre a coleta de dados necessários para preencher fichas de cadastro ou registros, além de permitir seu acesso a estes dados. Os artigos 72 e 74 tipificam os delitos de impedir ou dificultar o acesso do consumidor a sua informação.

Ainda há outros crimes esparsos ao Código Penal, a saber: os crimes contra a criança e o adolescente; crimes contra a segurança nacional – propaganda ofensiva à segurança nacional e à ordem política e social, e incitação à subversão da ordem política ou social; crimes contra a Liberdade Individual. Por conseguinte, a Lei de Telecomunicações, Lei 9.472/1997, garante ao usuário a proteção à sua privacidade e intimidade, além do respeito à privacidade nos documentos de cobrança e na utilização de seus dados pela prestadora de serviço, em elenco do seu art. 3.º. Já a LC 105/2001, que dispõe sobre o sigilo das operações de instituições financeiras, impõe o dever de sigilo sobre os dados bancários de correntistas, tratando como crime, no art. 10, a quebra de sigilo.

Para aplicação da norma, o Brasil tem investido na criação de órgãos de investigação especializados para combater os crimes virtuais, como por exemplo as Delegacias Especializadas de Repressão a Crimes contra Informática e Fraudes Eletrônicas. Na esfera de ação Federal foi criada em 1996 a Unidade de Perícia Informática da Polícia Federal. Além de agentes públicos, foram desenvolvidas iniciativas privadas especializadas para apoiar a população. No caso da SaferNet Brasil, parceira do MPF, é uma ONG voltada ao recebimento de denúncias de crimes contra direitos humanos praticados no meio virtual.

3.4. Crimes cibernéticos no direito internacional

Fora do Brasil, diversos países legislaram acerca da criminalidade informática, visando a proteção dos bens e a soberania de seus territórios, como os Estados Unidos, Suécia, França, Alemanha, entre outros. Na visão de Ulrich Sieber, existem neste sentido cinco correntes legislativas para a criação dessas leis: Proteção da privacidade, Direito Penal econômico, Proteção da propriedade intelectual, Conteúdo ilegal e lesivo e as Leis de segurança. A primeira são as leis do direito fundamental humano à sua privacidade e intimidade. A segunda é a corrente das leis criadas para defender a ordem econômica e os danos causados pelas fraudes de rede. A terceira visa proteger direitos autorais, tanto sob os programas quanto aos arquivos de mídia espalhados pela internet clandestinamente. A quarta rege o conteúdo ilegal: venda de drogas, pornografia infantil, dados sigilosos. E a quinta é composta das leis contra invasões de sistema.

E de fato, existem diversos países que assinaram tratados para acordar quanto aos cibercrimes em suas legislações. A Convenção de Budapeste sobre o Cibercrime foi aprovada pelo Conselho da Europa em 2001 e foi considerada um marco na história de combate aos crimes virtuais. A convenção foi assinada por 43 países, porém o Brasil não assinou, só indo a tratar do assunto com a Lei 11.829, 7 anos depois. Na convenção estão previstos os crimes de acesso ilícito; interceptação ilícita; interferência em dados e em sistemas; produção, venda, obtenção para utilização, importação e distribuição de dispositivos concebidos para a prática de crimes cibernéticos. Além disso, a convenção tipifica os crimes de falsificação de dados em quaisquer sistemas informáticos; violação de direitos autorais quando essa ocorrer em grande escala e por meio de sistemas informatizados; e pornografia infantil.

Também são estabelecidos na Convenção os procedimentos para a investigação dos crimes virtuais. Somente no caso de crimes graves será permitida a interceptação do tráfego de dados, mas neste caso, os fornecedores do serviço deverão conservar estes dados para investigação. Também obriga estes fornecedores a comunicar às autoridades competentes dados cadastrais ou outros dados informáticos que ajudem a identificar responsáveis com crimes cibernéticos.

Ainda que o Brasil tenha visto grande avanço na legislação sobre crimes de informática, para combater estes de forma eficiente é preciso a cooperação plena internacional, tanto em sentido administrativo quanto judicial. Embora esteja longe de ser uma solução perfeita, é pensamento majoritário entre os estudiosos sobre o tema de que estaria nos interesses do Brasil adotar as diretrizes da Convenção para atingir este objetivo de forma célere. Conforme Ana Karolina Calado da Silva:

> [...] é possível verificar como alternativa, com grandes chances de êxito em sua eficácia, a assinatura do Brasil à Convenção de Budapeste, já assinada por vários países da europa, que trata o cibercrime desde a sua definição até normas procedimentais, aliada à cooperação penal internacional, tanto na sua investigação quanto na sua produção probatória, devendo esta ser oficialmente assinada uma vez que somente se confere de forma concreta a cooperação internacional através de documento oficialmente assinado pelos países participantes.[...] (SILVA, 2013, p.20)

Como observado, os crimes comuns podem ser praticados tão facilmente quanto os crimes de informática pelo uso do meio digital. Porém o foco deste trabalho, o sequestro de dados, não possui tipificação específica, tanto como crime

comum quanto informático. Percebe-se uma grave deficiência na discussão deste crime, pois embora seja considerado um ato de grande potencial lesivo, possui pouca fundamentação legislativa no Brasil. O sequestro de dados, também chamado de *Ransomware*, neologismo formado pela junção das palavras *ransom* (valor pago em sequestro) e *malware* (programa malicioso de computador), é um dos grandes crimes de informática dos últimos anos, movimentando massivas quantias de dinheiro, obtidas ilegalmente, todos os dias. Segundo dados do FBI (*Federal Bureau of Investigation)*, no ano de 2015, o prejuízo causado por este crime chega a centenas de milhões de reais. Logo deve-se salientar a importância do estudo desta conduta e buscar a adequação desta nos moldes de nossa doutrina de direito. A seguir, iremos nos dedicar a explanar este crime, apresentando exemplos de casos ocorridos no Brasil.

4 O CRIME DE SEQUESTRO DE DADOS

Primeiramente, precisamos definir o que é sequestro de dados. É uma prática que envolve o uso de um programa invasivo, disseminado como vírus, que se infiltra no sistema da vítima disfarçado como um arquivo inofensivo, que o usuário abre e em consequência infecta o seu computador com o *malware.* O meio mais comum é um dos mais simples, pelo correio eletrônico. Faz parte mos muitos programas danosos que são adquiridos pelo usuário desavisado. Este programa restringe o acesso do usuário a seus arquivos, bloqueando eles por meio de senhas e criptografia. O agente então manda mensagens para a vítima, oferecendo desbloquear os dados por um preço, normalmente para ser pago em *bitcoins*, uma moeda eletrônica de difícil rastreamento, conforme explica anúncio publicado pelo FBI:

> A maioria dos criminosos envolvidos em esquemas de sequestro de dados demanda pagamento em *bitcoin*. Criminosos preferem o *bitcoin* porque é fácil de usar, rápido, disponível publicamente, descentralizado e propicia uma sensação de maior segurança ou anonimato. (2015)

Outros casos dessa espécie de golpe disfarçam a mensagem recebida pela vítima como ajuda especializada ou contato da polícia, pedindo para pagar uma multa para evitar problemas com seus arquivos.

O porém é que nada impede o agente de após receber o resgate manter os arquivos bloqueados, pois o sistema permanece sob total controle do agente, já que normalmente o programa permanece escondido no computador da vítima. A mesma vítima pode ter seu sistema afetado múltiplas vezes, até que o usuário pare de pagar.

4.1. Sequestro de dados no Brasil

Segundo pesquisa feita pela empresa de segurança de rede Kaspersky Lab, em parceria com B2B Internacional, corporações de alto renome em círculos de programação, O Brasil é o páis na América Latina com maior índice de ataques de sequestro de dados. Este cenário preocupante é sentido em maior parte pelas empresas brasileiras, cuja informatização e dependência em dados as torna alvos

fáceis para agente criminosos na rede. São objetivos óbvios para um crime onde a meta extorquir valores monetários.

No Brasil, a cidade de Japorã, no estado de Mato Grosso do Sul, a cidade de IDH mais baixo da região, teve o sistema de sua prefeitura infectado duas vezes, resultando em um grande prejuízo para a administração em sua contabilidade e gestão de pessoas, pois os arquivos de seus registros e cadastros foram sequestrados.

Existem relatos também do delito ter sido praticado com hospitais, clínicas e laboratórios como alvo, bloqueando prescrições e fichas de pacientes. Estes casos são exemplos mais graves, pois não só podem prejudicar o estabelecimento médico economicamente, como também causa dano aos próprios pacientes. Este tipo de situação pode causar ações judiciais e medidas administrativas, pois o artigo 4º do Código do Consumidor (Lei 8.078/90) prevê a proteção contra danos materiais e morais. Não só isso, como as fichas de pacientes contém informações sob sigilo médico, protegidos pelos artigos 73 a 77 do Código de Ética Médica.

Na verdade, todos os setores de serviços são requeridos por lei de manter o zelo sobre as informações que estes mantêm guardadas, o que causa um dano secundário imprevisto pelo agente que pratica o sequestro de dados. Neste sentido, comenta o mestre Renato Opice Blum (2016): “Afinal, embora provavelmente não estivesse ciente disso, não só no vigor física/mental das pessoas se funda o Setor de Saúde: a salubridade dos seus dados, mantidos em integridade, também pode contribuir para uma vida sem vicissitudes”.

Embora o crime esteja em sua maior ascensão nos anos recentes, os primeiros registros de casos de *ransomware* datam de 1989, com um vírus chamado “AIDS info disk” que bloqueava arquivos ao ligar o computador, e solicitava a renovação de licença do sistema mediante pagamento de determinado valor.

A ação penal neste tipo é difícil, considerando que todos os atos são praticados remotamente, como é característica dos crimes virtuais. É pior, pois o programa pode ser obtido de diversas maneiras, ainda mais se múltiplos agentes espalham o *malware* em rede. Não é incomum que um *cracker* venda o programa para agentes criminosos, que lucram com o golpe e pagam uma quantia para o vendedor, que efetivamente terceiriza os atos no delito. Neste caso, o esquema de pirâmide formado concede proteção adicional contra a ação policial, que passa a perseguir diversos agentes residentes em lugares diferentes.

Provavelmente o programa de Sequestro de dados mais famoso é o chamado *CryptoLocker*, que costuma infectar computadores na América do Norte, Europa e Ásia. Embora não seja diferente de outros programas, este assustou muitos especialistas pela velocidade de infecção e a força da criptografia dos arquivos afetados. Como a maioria de outros esquemas de *ransomware*, por trás do programa existe um grupo de *crackers* que trabalha em sua composição e o aprimora constantemente. Este grupo vende o programa por um valor acessível, através das páginas ocultas da internet e lucra com a ação criminosa de seus "clientes". Justamente por esta razão, o conselho da maioria das autoridades em segurança cibernética aconselha não pagar a quantia exigida para recuperar os arquivos. Além de não haver garantia de recupera-los, pagar proporciona o incentivo para os agentes continuarem a desenvolver o programa e infectar outros sistemas.

4.2. A tipificação do Sequestro de Dados

O sequestro de dados não está expressamente previsto na legislação brasileira. Considerando o nome deste tipo, foram feitas tentativas para enquadrar a conduta nos tipos de extorsão (art. 158, CP) e extorsão mediante sequestro (159, CP), mas ambos não são adequados para descrever o crime. Podemos considerar a possibilidade de utilizar a conduta do artigo 154-A do CP que descreve a invasão de sistemas de informática, porém o delito prevê somente a invasão de sistema com o intuito de apropriar-se, modificar ou destruir os dados, o que não é o caso da conduta em pauta. Como este crime contém a exigência de valores, isto o transformaria no crime de extorsão. Todavia, devemos lembrar que este tipo é consumado com o emprego de violência ou grave ameaça, tornando seu enquadramento em sequestro de dados, problemático. O emprego de violência é altamente improvável neste caso (para não dizer impossível), porém a grave ameaça neste tipo subtende uma ameaça capaz de causar um temor equivalente aquele causado pelo emprego de violência, o que não necessariamente é traduzido no crime de sequestro de dados. Ainda mais considerando que o objeto do crime são os dados virtuais bloqueados, um objeto de valor abstrato para o direito penal.

Talvez esta comparação seja mais bem exemplificada no caso do agente que se passa por agente policial, como acontece em Portugal, com o malware conhecido como "vírus da polícia de Portugal", em que a vítima recebe um e-mail

supostamente do setor administrativo da polícia, ou em alguns casos da Interpol, no qual a vítima é multada por possuir pornografia infantil em seu computador. O agente então encoraja a vítima a pagar uma multa, para evitar a persecução penal. Neste caso, a perspectiva de ir a cárcere pode ser interpretada como grave ameaça, justificando a interpretação de que o crime equivale à extorsão, considerando ainda o crime de falsidade ideológica do agente.

O entendimento atual da doutrina brasileira, é que o sequestro de dados melhor se encaixa no crime de Invasão a Dispositivo Informático, do 154-A do CP. Embora o *ransomware* descreva uma conduta mais complexa, como sugere o tipo de extorsão, o anterior é parte da legislação mais especializada. Não podemos falar de extorsão mediante sequestro, pois este o objeto deste crime é necessariamente uma pessoa e a invasão de sistema não abrange a complexidade dos atos realizados no delito.

4.3. A necessidade de cooperação internacional

Com base nestes argumentos, podemos concluir que não existe dúvida de que o sequestro de dados é uma conduta penalizada no ordenamento brasileiro, mas com a falta de tipo específico, tendo somente fundamento com base no crime de extorsão, existem poucas instâncias de processos realizados relativos a este delito. No caso da possibilidade do Brasil assinar tratado internacional com o objetivo de combater delitos transnacionais, seria consideravelmente mais eficiente a ação policial contra os crimes virtuais em geral, pois atualmente a lei brasileira só pode ser aplicada no exterior excepcionalmente, tornando os atos consumados em território nacional por agente estrangeiro fora de nossa esfera penal.

Nos Estados Unidos, existe uma divisão específica de combate a crimes de informática, o *Computer Crime and Intellectual Property Section Criminal Division* (Divisão Criminal da Seção de Crimes de Computador e Propriedade Intelectual), cuja jurisdição inclui o crime de sequestro de dados. Existe uma lista de leis que são utilizadas para penalizar esta conduta, embora não exista por si próprio o tipo para *ransomware*. O crime de extorsão da legislação americana inclui a modalidade de transmissão de dados, além de a conduta ser prevista nos crimes de Negação de Serviço (*Denial of Service*), Fraude de Internet, e Acesso Indevido. Outras leis e estatutos são aplicados conforme o tipo de extorsão ou valor extorquido.

Silva (2013), ao fazer o estudo comparado da doutrina, lembra que os EUA utilizam o sistema de Common Law, que se utiliza majoritariamente de precedentes jurídicos, além de prevalecer o Federalismo, em que cada estado americano possui suas próprias regras para reger o processo legislativo. Assim, o combate aos crimes virtuais possui duas frentes: Estadual e Federal.

A lei federal utiliza a Lei de Proteção aos Sistemas Computacionais, que tem como espécie penal o crime de utilizar computador para praticar fraude, furto ou qualquer outra apropriação ilegal. A lei mais importante que responsabiliza os crimes virtuais para os EUA é a Lei de Fraude e Abuso Computacional, cujo objetivo é prevenir contra o acesso de sistemas com a intenção de se apropriar de informação sigilosa nacional ou vantagens econômicas.

Ainda assim, o crime de sequestro de dados é de árdua persecução. Os melhores resultados foram vistos através da cooperação de forças policiais com empresas de segurança digital para eliminar programas nocivos da rede, porém, sem grandes avanços na punibilidade dos agentes que os inseriram. A maior dificuldade neste sentido continua por ser a extraterritorialidade dos crimes virtuais, visto que seria necessária a cooperação de diversas forças de combate a esta espécie de crime para efetivamente perseguir o agente criminoso. Fator agravante deste delito é que todos são vulneráveis a sua ação. Existem múltiplos relatos de delegacias sendo infestadas pelo programa de *ransomware*, obstruindo a ação policial do órgão.

Seja pela falta de legislação específica ou recursos materiais, o crime de sequestro de dados, embora considerado penalmente punível, é quase impossível o fazer na prática, considerando os obstáculos proporcionados por o que muitos diriam serem as vantagens de se utilizar da internet. Os crimes virtuais em geral possuem por si próprios uma camada de proteção, e o sequestro de dados é de maior gravidade por ser facilitado pela simples execução do arquivo malicioso. É evidente neste caso, que a melhor proteção contra essa espécie de crime é a autotutela dos usuários. Este crime preda os iniciantes ao uso da rede, que possuem um grau de ingenuidade contra as armadilhas que podem ser colocadas ao navegar na internet. Inclusive esta é a melhor recomendação das autoridades e empresas de segurança. O cuidado ao executar arquivos, assim como possuir um programa de antivírus pode evitar a maioria dos transtornos causados por este delito. Em uma visão otimista, é possível que com a conscientização dos usuários e com a formação de hábitos de

defesa, esta espécie de crime tenha sua frequência reduzida. Todavia existe a chance de uma evolução do *malware* a um ponto que o programa se torne cada vez mais invasivo, mais fácil de se infiltrar e executar. É uma questão de adaptação, se com a inclusão digital da população esta ameaça continuará relevante ou será substituída por novos técnicas mais avançadas.

CONCLUSÃO

Em conclusão, ao retomarmos o problema desta obra: A legislação brasileira tipifica corretamente o crime de sequestro de dados? A hipótese apresentada inicialmente era que não, pois não foi criada previsão expressa na legislação. No decorrer deste trabalho foi observado que este se encontra precariamente inserido no tipo de invasão de dispositivo informático do código penal, auxiliado pela esparsa legislação específica dos crimes de informática e códigos variados. A hipótese assim foi parcialmente confirmada, pois embora o crime esteja inserido na doutrina brasileira, sua aplicação é imperfeita, pendendo na interpretação do tipo de invasão de sistema, sem possuir a complexidade para fazer frente aos atos da conduta. Ademais, a penalização deste crime no Brasil é atualmente quase suprimida, pela dificuldade das autoridades policiais em identificar o agente criminoso. O ideal, é claro, seria a conduta de sequestro de dados ser especificamente inserida entre os tipos do código penal ou, quem sabe, a formulação de lei específica para crimes praticados no meio cibernético. Mas ainda que sua inclusão na doutrina possibilite a punibilidade dos agentes que praticam este delito, é uma dificuldade extraterritorial levar os mesmos à justiça. É necessária a cooperação administrativa e judicial entre polícia e juízes a nível internacional, fator dificultado pela exclusão do Brasil em tratados internacionais que acordam quanto a este objeto.

Enquanto existir o discurso a favor da tutela do estado sobre o fluxo de dados da rede, aqueles que acreditam na internet livre irão ser contrários ao mesmo. Se há de haver a proteção do direito de forma eficiente, um meio termo deverá ser acordado, em prol da proteção dos direitos dos usuários. É importante no entanto não descaracterizar a internet de suas numerosas vantagens, que auxiliam inclusive o avanço da justiça. Seria o caso da tutela limitada do estado sobre seus sistemas e serviços fundamentais, os quais são alvos constantes de *ransomware.*

A melhor defesa contra os crimes virtuais mais danosos, por agora, é dependente dos usuários, não do estado. A cautela contra programas desconhecidos advindos de fontes dúbias é a maior parte do desafio na luta contra os tipos penais cibernéticos. Conforme os usuários ganham experiência em navegar em rede, as chances de infecção diminuem gradualmente. No caso do pior ocorrer,

no caso de *ransomware*, há pouca esperança de recuperar o dano sofrido ou de encontrar o agente criminoso. É importante manter cópias de segurança de dados importantes, enquanto não houver solução definitiva para o delito.

Conforme a legislação evoluir, é possível vermos avanço quanto aos crimes virtuais, enquanto eles forem relevantes para a sociedade e enquanto a inclusão digital do Brasil estiver em curso. Só resta saber se a evolução das leis acompanhará o progresso do mundo virtual, visto que este, diferente do poder legislativo, prescinde de prazos, despachos e audiências. E cujos usuários, embora se encontrem abertos a um mundo sem fronteiras, estão vulneráveis a ameaças advindas de qualquer ponto do planeta, necessitando de um clique em falso para serem vítimas de delito cibernético.

REFERÊNCIAS

FERREIRA, Ivette Senise. **Os crimes da informática**. In: BARRA, Rubens Prestes; ANDREUCCI, Ricardo Antunes (Coord.). Estudos Jurídicos. São Paulo: RT, 1992, p. 142.

_____. **A criminalidade informática**. In: LUCCA, Newton de; SIMÃO FILHO, Adalberto (Coord.). Direito e internet. Bauru: Edipro, 2000.

BRASIL. Constituição (1988). **Constituição**: República Federativa do Brasil. Brasília: Senado Federal, 1988.

_____. **Lei 9.296**, de 24 de julho de 1996. Disponível em: <www.planalto.gov.br/ccivil_03/leis/l9296.htm>. Acesso em: 31.03.2016.

_____. **Lei 12.735**, de 30 de novembro de 2012. Disponível em: <www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm>. Acesso em: 31.03.2016.

_____. **Lei 12.737**, de 30 de novembro de 2012. Disponível em: <www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 31.03. 2016.

_____. Projeto de Lei do Senado nº 236, de 09 de julho de 2012. **Reforma do Código Penal Brasileiro**. Brasília: Senado Federal, 2012.

YOUSSEF, Antonio Nicolau; FERNANDEZ, Vicente Paz. **Informática e sociedade.** 2ª ed. São Paulo: Ática, 1988, p. 49-50.

INELLAS, Gabriel César Zaccaria de. **Crimes na internet***.* São Paulo: Editora Juarez de Oliveira, 2004.

JUNQUEIRA, Maria Helena. ***Computer crimes***. São Paulo: Del Rey, 1997, p.29.

FRAGA, Antônio Celso Galdino. **Crimes de informática** – a ameaça virtual na era da informação digital, in Internet: o direito na era virtual. SCHOUERI, Luís Eduardo (Coord.). Rio de Janeiro: Forense, 2001, p. 366.

JAEGER, Marc apud FERREIRA, Ivette Senise. **A criminalidade informática**. In: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.), Bauru: Edipro, 2000, p. 214.

PRADEL, Jean; FEUILLARD, Cristian apud FERREIRA, Ivette Senise. **A criminalidade informática**. In: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.), op. cit, 2000, p.214.

BISMUTH, Yves; CROZE, Hervé apud FERREIRA, Ivette Senise. **A criminalidade informática**. In: LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.), op. cit, 2000, p. 215.

JESUS, Damásio E. de apud ARAS, Vladimir. **Crimes de Informática**. Jus Navigandi, Ed. 12, out. 2001. Disponível em: < http://www1.jus.com.br/doutrina/texto.asp?id=2250 >. Acesso em: 21 out. 2015.

GATES, Bill. **A Estrada do Futuro**. Tradução Beth Vieira et al. São Paulo: Companhia das Letras, 1995, p. 14.

ROSSINI, Augusto. **Brevíssimas considerações sobre delitos informáticos**. Caderno Jurídico**,** São Paulo, n. 4, ano 2, jul. 2002.

MONTEIRO NETO, João; FREITAS DA SILVA, Francisca. In: XVIII Congresso Nacional do CONPEDI, São Paulo, 4-7 de nov. de 2009. **Os crimes eletrônicos no ordenamento jurídico brasileiro**. Disponível em: < http://www.publicadireito.com.br/conpedi/manaus/arquivos/Anais/sao_paulo/2319.pdf >. Acesso em: 6 nov. 2015.

MONTEIRO, Renato Leite. In: XVIII Congresso Nacional do CONPEDI, São Paulo, 4-7 de nov. de 2009. **Cibernética**: a invasão da privacidade e da intimidade. Disponível em: < http://www.publicadireito.com.br/conpedi/manaus/arquivos/Anais/sao_paulo/2513.pdf >. Acesso em: 6 nov. 2015.

SOUZA, Aline. **Brasil é o quarto país em crimes virtuais**. Em.com.br, Minas Gerais, 21 de nov. de 2013. Disponível em: < http://www.em.com.br/app/noticia/tecnologia/2013/11/21/interna_tecnologia,472182/brasil-e-o-quarto-pais-em-vitimas-de-crimes-virtuais.shtml>. Acesso em: 4 dez. 2015.

HAJE, Lara. **Saiba como os crimes na internet são tratados em outros países**. In: MACHADO, Ralph. Brasília, DF: Agência Câmara Notícias, 8 jul. 2011. Disponível em: < http://www2.camara.leg.br/camaranoticias/noticias/CIENCIA-E-TECNOLOGIA/199806-SAIBA-COMO-OS-CRIMES-NA-INTERNET-SAO-TRATADOS-EM-OUTROS-PAISES.html> . Acesso em: 25 maio 2016.

SILVA, Ana Karolina Calado da. **O estudo comparado dos crimes cibernéticos**: uma abordagem instrumentalista-constitucional acerca da sua produção probatória em contraponto à jurisprudência contemporânea brasileira. In: Âmbito Jurídico, Rio Grande, XVI, n. 109, fev. 2013. Disponível em: <http://www.ambito-juridico.com.br/site/index.php/?n_link=revista_artigos_leitura&artigo_id=12778&revista_caderno=17>. Acesso em: 25 maio 2016.

SIEBER, Ulrich. Apud. CRESPO, Xavier de Freitas. **Diretivas Internacionais e Direito Estrangeiro**. São Paulo: Saraiva, 2011.. P.120-155.

MAZONI. Ana Carolina. **Crimes na Internet e a Convenção de Budapeste.** Dissertação (monografia), 2009, Faculdade de Ciências Jurídicas e Sociais, Brasília.

BRANDÃO, Claúdio. **Curso de direito penal**: parte geral. 2ª ed. Rio de Janeiro: Forense, 2010.

SUPERIOR TRIBUNAL DE JUSTIÇA. 1ª Turma. **HC nº 76.689**. Ementa:[...]Relator: Sepúlveda Pertence. Brasília, DF, 28 set. 98. DJU 6.11.1998.

JARRETT, H. Marshall; BAILIE, Michael W. **Prosecuting computer crimes**. In: ELTRINGHAM, Office of Legal Education. Scott. 14 jan. 2015. Disponível em: <https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf> . Acesso em: 25 maio 2016.

ESTADOS UNIDOS DA AMÉRICA. Federal Bureau of Investigation. **Criminals continue to defraud and extort from victims using cryptowall ramsomware schemes**. Washington, DC. 23 jun 2015. Disponível em: <http://www.ic3.gov/media/2015/150623.aspx>. Acesso em: 25 maio 2016.

ONU. United Nations Office on Drugs and Crime. **Comprehensive study on cybercrime**. Nova York, fev. 2013.

CRESPO, Marcelo. ***Ransomware* e sua tipificação no Brasil**. Canal Ciências Criminais, nov. 2015. Disponível em: <http://canalcienciascriminais.jusbrasil.com.br/artigos/249364352/ransonware-e-sua-tipificacao-no-brasil>. Acesso em: 23 maio 2016.

RUTHERFORD, Mikhail. **Crimes na internet**. In: VIEIRA NETO, Raul José. Jusbrasil.com, 22 set 2015. Disponível em: <http://mikhail.jusbrasil.com.br/artigos/234313175/crimes-na-internet-falta-de-normatizacao-dificuldades-na-regulamentacao-e-entendimentos-sobre-o-assunto>. Acesso em: 26 maio 2016.