UNIVERSIDADE REGIONAL INTEGRADA DO ALTO URUGUAI E DAS MISSÕES
PRÓ-REITORIA DE ENSINO, PESQUISA E PÓS-GRADUAÇÃO
CAMPUS DE ERECHIM
DEPARTAMENTO DE CIÊNCIAS SOCIAIS APLICADAS
CURSO DE DIREITO

BERNARDO RIEDER

RANSOMWARE: A EXTORSÃO DIGITAL E SUAS IMPLICAÇÕES JURÍDICO PENAIS

ERECHIM
2018

BERNARDO RIEDER

RANSOMWARE: A EXTORSÃO DIGITAL E SUAS IMPLICAÇÕES JURÍDICO PENAIS

Trabalho de conclusão de curso apresentado como requisito parcial à obtenção do grau de Bacharel em Direito, Departamento de Ciências Sociais Aplicadas da Universidade Regional Integrada do Alto Uruguai e das Missões – Erechim.

Orientadora: Prof.ª. Me. Diana Casarin Zanatta.

ERECHIM

2018

BERNARDO RIEDER

RANSOMWARE: A EXTORSÃO DIGITAL E SUAS IMPLICAÇÕES JURÍDICO PENAIS

Trabalho de conclusão de curso apresentado como requisito parcial à obtenção do grau de Bacharel em Direito, Departamento de Ciências Sociais Aplicadas da Universidade Regional Integrada do Alto Uruguai e das Missões – Erechim.

Erechim, 21 de novembro de 2018.

BANCA EXAMINADORA

_____

Prof.ª. Me. Diana Casarin Zanatta

URI - Erechim

_____

Prof.ª. Me. Simone Gasberin de Albuquerque

URI - Erechim

_____

Prof. Me. José Plínio Rigotti

URI - Erechim

Dedico este trabalho à minha família, amigos e colegas, que me apoiaram e acreditaram na elaboração deste trabalho acadêmico.

AGRADECIMENTOS

Agradeço, inicialmente, à Universidade Regional Integrada das Missões e do Alto Uruguai, a sua direção e administração pelo ambiente acolhedor e amigável que proporciona.

Aos meus pais, por todo desempenho, amor e motivação, por terem acreditado na minha caminhada até o momento.

À minha namorada Sara Luzia Ongaratto, por toda paciência, zelo e compreensão, para que fosse possível a realização deste trabalho.

À minha professora e orientadora Me. Diana Casarin Zanatta, pelo conhecimento, dedicação, compreensão e suporte no pouco tempo que lhe coube, pelas suas correções e incentivos.

Às professoras Luciane Gressana e Simone Gasperin de Albuquerque, por todo esforço e atenção na condução do trabalho.

Ao Delegado Marco Antônio Arruda Guns pelo apoio e presteza na resolução do questionário ofertado sobre o tema deste trabalho.

Ao Andrey Henrique Andreolla pelo conhecimento e pelos conselhos prestados na condução da temática do trabalho.

Por fim, agradeço aos meus colegas que me acompanharam durante estes cinco anos na minha formação, bem como todas as demais pessoas que de alguma forma contribuíram para a conclusão do curso superior em Direito. Obrigado!

O Direito deve refletir a realidade de uma determinada sociedade, fazendo-se necessário à sua adaptação conforme o processo evolutivo humano avança.

(Patrícia Peck Pinheiro)

RESUMO

O presente estudo tem o objetivo de analisar a extorsão digital por meio do código malicioso *ransomware.* A evolução digital trouxe novas formas de condutas delituosas até então desconhecidas, por ser um ambiente rentável e favorável para a prática de crimes. Dessa maneira, o uso do *ransomware* para praticar extorsões digitais vem se tornando uma atividade corriqueira no mundo virtual. Analisa-se, contudo, as implicações desse *malware*, considerando-se as principais incidências e efeitos que provocou na sociedade nos últimos anos. Para tanto, utiliza-se de um embasamento teórico através de pesquisa bibliográfica e documental, utilizando-se do método indutivo e analítico-descritivo. Ao longo da abordagem sobre o tema, procura-se, primeiramente, examinar a origem da *Internet* e dos Crimes cibernéticos*,* bem como as suas principais espécies e classificações no mundo virtual. Em seguida, procura-se explicar o conceito, classificação, funcionamento e demais particularidades do *ransomware* para prática da extorsão digital. Por fim, busca-se analisar as incidências ocorridas na atualidade, em âmbito nacional e internacional, do *ransomware*, bem como analisar os principais efeitos e consequências causados na sociedade.

Palavras-chave: Crimes cibernéticos. Extorsão digital. *Ransomware*. Incidências. Consequências.

ABSTRACT

The present study aims to analyze digital extortion through the ransomware malicious code. Digital evolution has brought new forms of criminal conduct hitherto unknown, as it is a profitable and favorable environment for the practice of crimes. In this way, the use of ransomware to practice digital extortion has become a commonplace activity in the virtual world. It analyzes, however, the implications of this malware, considering the main impacts and effects it has caused in society in recent years. For that, a theoretical basis is used through bibliographical and documentary research, using the inductive and analytic-descriptive method. Throughout the approach on the subject, it is sought, first, to examine the origin of the Internet and the Cybernetic Crimes, as well as their main species and classifications in the virtual world. Next, we try to explain the concept, classification, operation and other peculiarities of ransomware to practice digital extortion. Finally, it seeks to analyze the current national and international incidence of ransomware, as well as to analyze the main effects and consequences caused in society.

Keywords: Cyber crimes. Digital extortion. Ransomware. Incidences. Consequences.

SUMÁRIO

1 INTRODUÇÃO

Há anos a Internet vem interligando o mundo de uma maneira simples e rápida, possibilitando a comunicação e o compartilhamento de informações em nível global, sem qualquer limitação temporal ou espacial. Ocorre que, junto a essa evolução digital, notadamente de sua exploração econômica, o crime renovou-se, trazendo novas formas de condutas delituosas até então desconhecidas pelos usuários digitais, ao passo que se tornou um ambiente rentável e favorável à prática de crimes, tal como o delito de extorsão digital utilizando-se do código malicioso *ransomware*, que foi responsável por inúmeras ocorrências de delitos informáticos desde 2016.

A partir desse cenário, compreender as mudanças e a extensão dos crimes cibernéticos é de grande relevância acadêmica e social, tendo em vista a estreita relação entre a área jurídica e a tecnologia digital na contemporaneidade. Além disso, o espaço virtual se transformou em uma ferramenta cotidiana e indispensável para grande parte da sociedade, com mais de 3 bilhões e 200 milhões de usuários ativos na rede global de computadores, correspondendo, em média, há 44% da população do planeta.

Nesse contexto, o uso do *ransomware* para a prática de extorsões digitais tem se tornado uma prática corriqueira no mundo digital, à medida que o agente se utiliza desse meio e se aproveita da vulnerabilidade do sistema, sequestrando, através da criptografia, os arquivos digitais salvos no computador da vítima, ou em nuvem, impedindo-a de acessá-los. Ocorrendo, posteriormente, em um segundo momento, o constrangimento da vítima ao pagamento de um resgate por meio de moedas digitais, às quais dificultam o rastreamento e garantem aos criminosos a rápida extração dos valores.

O presente estudo destina-se a analisar os aspectos relativos da prática da extorsão, tipificada no artigo 158 do Código Penal Brasileiro, por meio do código malicioso *ransomware* no âmbito informático, analisando as principais características e consequências dos ataques cibernéticos ocorridos nos últimos anos. Para melhor atingir o objetivo proposto, o estudo divide em três capítulos e utiliza de embasamento teórico em pesquisa bibliográfica e documental, seguindo o método indutivo e analítico-descritivo. Emprega-se, também, entrevista realizada com delegado de polícia de delegacia especializada em repressão de crimes cibernético.

O primeiro capítulo é destinado à análise da forma como se deu o processo evolutivo da Internet e dos crimes cibernéticos, enfatizando-se as principais incidências históricas que influenciaram o desenvolvimento de ambos os institutos. Além disso, é realizado um estudo dirigido aos conceitos de delitos digitais, com enfoque nas classificações e principais espécies de códigos maliciosos utilizados para a prática de condutas ilegais. Por fim, explora-se os diferentes tipos de sujeitos que utilizam os seus conhecimentos para perpetrar certas condutas na Internet.

No segundo capítulo, por seu turno, estuda-se o funcionamento do *ransomware* para a prática da extorsão digital, especialmente as suas classificações e formas de manifestações, além de sua integração e estruturação no ordenamento jurídico brasileiro e internacional.

Concluindo o trabalho de pesquisa, o terceiro capítulo aborda as implicações que o *ransomware* se manifesta no meio da sociedade, seus efeitos, consequências e estatísticas da prática criminosa, a partir de documentários, notícias jornalísticas e depoimentos pessoais de profissionais que vivenciam tal prática criminosa diariamente.

Ao longo do presente trabalho, portanto, buscar-se-á responder a estes questionamentos, sempre empregando amparo em meios jurídicos disponíveis, através de entendimentos doutrinários atuais, com enfoque a documentários concretos, de maneira a possibilitar a ideia mais ampla e atualizada das particularidades da extorsão digital por meio do código malicioso *ransomware.*

2 A INTERNET, OS CRIMES CIBERNÉTICOS E SEUS ELEMENTOS ESTRUTURANTES

Nesse primeiro momento do estudo, importa compreender a evolução histórica, os conceitos, sujeitos e classificações inerentes à internet e aos crimes cibernéticos, a fim de que se possa adentrar no estudo da extorsão digital por meio do *malware ransomware*.

2.1 Conceito e evolução histórica da internet e dos crimes cibernéticos

A internet é uma rede mundialmente aceita que foi criada com o objetivo de possibilitar a comunicação social de milhares de usuários digitais. Por meio dela, os indivíduos conseguem trocar informações de forma célere, prática e instantânea, sem qualquer limitação temporal ou espacial.

De acordo com a ANATEL - Agência Nacional de Telecomunicações, em sua Portaria nº 148, de 31 de maio de 1995, a Internet é o "nome genérico que designa o conjunto de redes, os meios de transmissão e comutação, roteadores, equipamentos e protocolos necessários à comunicação entre computadores, bem como o "software" e os dados contidos nestes computadores". (BRASIL, 1995). No mesmo sentido, Patrícia Peck Pinheiro define a internet como:

> Tecnicamente, a Internet consiste na interligação de milhares de dispositivos do mundo inteiro, interconectados medicante protocolos (IP, abreviação de *Internet Protocol*). Ou seja, essa interligação é possível porque utiliza um mesmo padrão de transmissão da dados. A ligação é feita por meio de linhas telefônicas, fibra óptica, satélite, ondas de rádio ou infravermelho. A conexão do computador com a rede pode ser direta ou através de outro computador, conhecido como servidor. Este servidor pode ser próprio ou, no caso dos provedores de acesso, de terceiros. O usuário navega na Internet por meio de um *browser*, programa usado para visualizar páginas disponíveis na rede, que interpreta as informações do *website* indicado, exibindo na tela do usuário textos, sons e imagens. São *browsers* o MS Internet Explores, da *Microsoft*, o *Netscape Navigator*, da *Netscape*, *Mozilla*, da *The Mozilla Organization* como cooperação da *Netcape*, entre outros. (PINHEIRO, 2016, p. 63).

Nos últimos 80 anos, em razão das inovações tecnológicas e das infraestruturas de telecomunicações, os países sofreram uma transformação de tamanha proporção que afetaram as suas sustentações econômicas. (PINHEIRO, 2016). Com efeito, o processo evolutivo da internet partiu da necessidade de se

proteger de eventual guerra ou ataque nuclear na Guerra Fria, fazendo, assim, o desenvolvimento tecnológico acelerar. Através de um projeto militar norte-americano, em 1969, foi criada uma rede capaz de interligar computadores que estivessem distantes para possibilitar a comunicação de dados, bem como permanecer hígida diante de guerras, como exemplo, de um ataque nuclear. (LIMA, 2016).

Essa rede foi chamada de ARPANET, a qual, em um curto período de tempo, disseminou-se pelos Estados Unidos, principalmente entre universidades, órgãos militares e governo. Em 1986, a ARPANET começou a ser chamada de Internet:

> Com o passar dos anos se consolidou a importância de criar uma rede capaz de integrar computadores que estivessem distantes e que por intermédio dela fosse permitida a comunicação de dados. Sob esse ponto de vista foi criada a ARPANET, inicialmente interligando a Universidade da Califórnia (*Los Angeles* e Santa Bárbara), a Universidade de *Stanford* (Santa Cruz) e a Universidade de *Utah* (*Salt Lake City*). (WENDY; JORGE, 2013, p. 7).

Posteriormente, a criação do *e-mail* em 1971 marcou o período inicial da era digital, tornando-se uma importante ferramenta de comunicação social daquela época. Entre 1990 a 1994 surgiram os grandes provedores de internet, os quais disponibilizaram conexões aos usuários. Na sequência, em 1999, foram criados os primeiros ambientes de discussões digitais, atualmente conhecidos como redes sociais, aos quais ofereciam aos usuários o envio de mensagens de forma simples e rápida, sem a necessidade de maiores conhecimentos técnicos:

> Alguns com pressa, para que o avanço tecnológico seja mais intenso, outros temendo-o, assim como aconteceu em todas as revoluções. Isso porque lá em meados de 1994, ao iniciar a era comercial da internet, tudo mudou numa velocidade jamais vista pela humanidade. Uma mensagem que antes demoraria semanas para chegar em um destino distante agora trafega ao simples toque de um *enter*. Antes, um gigante computador e conhecimento avançados em informática eram necessários. Hoje, uma criança e um pequeno *smartphone* são cúmplices de um enorme avanço tecnológico. (LIMA, 2016, p. 6).

O surgimento de grandes redes sociais a partir de 2004, como o *Orkut* e o *Facebook*, marcaram o segundo período de grande importância para a internet, denominada de *Web* 2.0. Em suma, trouxeram diferentes formas de comunicações digitais, sem contar na facilitação na propagação de informações, à medida que uma simples publicação, por exemplo de alguma imagem pessoal, tinha a capacidade de causar prejuízos imensuráveis a terceiros. (LIMA, 2016).

Em seguida, a partir de 2007, a tecnologia migrou para equipamentos menores e mais compactos, aos quais possibilitaram a conexão e a troca de informações sem qualquer limitação temporal e espacial, tal como observa Glaydson de Farias Lima:

> Até que, no início de 2007, Steve Jobs surpreende o mundo com o lançamento do primeiro IPhone. Temos um novo gigante passo. O mundo migraria grande parte das atividades de computadores para estes dispositivos menores e, com a melhoria na qualidade da conexão móvel, passaríamos a estar conectados a todo momento, recebendo e enviando informações no carro, no ônibus, na rua, na cama [...] (LIMA, 2016, p. 6).

No Brasil, o computador começou a ser utilizado em 1964 pelo Instituto Brasileiro de Geografia e Estatísticas (IBGE). Em contrapartida, o primeiro computador a ser fabricado em solo brasileiro foi em 1972, também denominado de “patinho feio” pela Universidade Federal de São Paulo (USP). (WENDT; JORGE, 2013).

Quanto à internet no Brasil, a primeira conexão realizada sucedeu-se em 1988 com a *Bitnet* da Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), do Laboratório Nacional de Computação Científica (LNCC) e da Universidade Federal do Rio de Janeiro (UFRJ). Em 1992, a Internet começou a ser implantada com a criação da primeira rede conectada à internet, que interligava as principais universidades brasileiras. (WENDT; JORGE, 2013).

Consequentemente, a internet, ao longo do tempo, tornou-se uma ferramenta útil nas vidas das pessoas, em razão de ser uma rede mundialmente interligada, sem limites geográficos, capaz de transmitir dados com apenas um clique. No entanto, da mesma forma que o meio virtual evoluiu e se transformou em um recurso indispensável ao cotidiano da sociedade, os crimes cibernéticos vieram logo em seguida, com a utilização de novas práticas criminosas até então desconhecidas. (BARRETO; WENDT; CASELLI, 2017).

A definição de crimes cibernético para o Direito Digital, conforme ensina Patrícia Peck Pinheiro, é a mesma atribuída ao Direito Penal, isto é, uma ação típica, ilícita e culpável. Porém, para facilitar o crime, principalmente no que tange ao anonimato, a conduta é praticada por meio de uma ferramenta denominada Internet:

> O crime eletrônico é, em princípio, um crime meio, isto é, utiliza-se de um meio virtual. Não é um crime de fim, por natureza, ou seja, o crime cuja modalidade só ocorra em ambiente virtual, à exceção dos crimes cometidos por hackers, que de algum modo podem ser enquadrados na categoria de

> estelionato, extorsão, falsidade ideológica, fraude, entre outros. Isso quer dizer que o meio de materialização da conduta criminosa pode ser virtual; contudo, em certos casos, o crime não. (PINHEIRO, 2016, p. 379-380).

Além do mais, os crimes cibernéticos são os praticados em meios virtuais e apresentam várias classificações. Para Emerson Wendt e Higor Vinicius Nogueira Jorge o instituto subdivide-se em ações prejudiciais atípicas e crimes cibernéticos. O primeiro consiste nas condutas praticadas por meio da rede mundial de computadores, que por sua vez não são punidas em razão da ausência de tipificação legal. O segundo, entretanto, crimes cibernéticos, subdividem-se em abertos e exclusivamente cibernéticos, sendo estes praticados somente por meio do uso de computadores ou sistemas informáticos, ao passo que aqueles podem ser realizados por diversos meios, inclusive os meios informáticos. (WENDT; JORGE, 2013).

Conforme leciona Renan Cabral Saisse, os crimes cibernéticos também podem ser classificados como impuros ou impróprios, puros ou próprios e mistos. Os crimes impuros ou impróprios são aqueles em que o dispositivo informático é utilizado apenas como meio para a consumação de um crime tradicional. Por outro lado, os puros ou próprios têm como função afetar diretamente dispositivos informáticos. E, por fim, os mistos que envolvem mais de um bem jurídico, isto é, uma mistura das classificações anteriores:

> Doutrinariamente podemos adotar três classificações principais para crimes cibernéticos: Impuros ou Impróprios: O dispositivo informático é utilizado apenas como meio/instrumento para consumação/execução de um crime tradicional. Exemplo: Crimes contra a honra como calúnia (art.138 CP), difamação (art.139 CP) ou injúria (art. 140 CP) realizados em redes sociais ou por envio de e-mails Puros ou Próprios: O bem jurídico afetado é a inviolabilidade da informação automatizada (dados), ou seja, objetiva afetar diretamente dispositivos informáticos e seus dados. Exemplo: Interromper serviço telemático ou de informação de utilidade pública, ou impedir/dificultar o seu restabelecimento (Art. 266, §1º CP). Mistos: Crimes complexos que envolvem mais de um bem jurídico de natureza diversa, sendo um deles a inviolabilidade de informações automatizadas, ou seja, daquelas armazenadas e processadas em sistemas computacionais. Exemplo: 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 – afeta a inviolabilidade de informações automatizadas e a privacidade – ou instalar vulnerabilidades para obter vantagem ilícita – pode afetar o patrimônio (Art.154-A CP). (SAISSE, 2016, p. 1).

Para a doutrina, no que tange ao processo evolutivo dos crimes cibernéticos, a primeira forma de ataque virtual, que se tem notícia, partiu da década de 60, originado

a partir de um jogo e criado através de um grupo de programadores, tinha a função de sobrecarregar o computador do adversário. Da mesma forma que foi criada a ameaça, também fora desenvolvida uma forma de reverter a situação ocasionada, conhecida atualmente como antivírus:

> Tudo começou quando um grupo de programadores desenvolveu um jogo chamado Core Wars, capaz de se reproduzir cada vez que era executado, sobrecarregando a memória da máquina do outro jogador. Os inventores desse jogo também criaram o primeiro antivírus, batizado de Reeper, com capacidade de destruir as cópias geradas pelo Core Wars. A existência desse jogo, seus efeitos e a forma de desativá-lo, no entanto, vieram a público somente em 1983, por um artigo escrito por um de sus criadores, publicado em uma conceituada revista científica da época. (A EPIDEMIA, 2018, p.1).

Daí em diante as formas e maneiras maliciosas de se infectar computadores tornaram-se cada vez mais diversas e perigosas. Até 1995, embora existissem outros, o vírus de *boot* representava em média 70% das ameaças. Em seguida, por volta de 2004, surgiu nas Filipinas o primeiro vírus de celular, denominado *Cabir*, o qual disseminava-se via *Bluetooth* e sua principal função era descarregar a bateria dos celulares infectados. (WENDT; JORGE, 2013).

Assim, nesta nova era digital, a crescente utilização da Internet, principalmente de sua exploração econômica, trouxe novas formas de condutas criminosas até então desconhecidas, à medida que os criminosos se depararam com um sistema desconhecido por meio do qual conseguiam praticar condutas criminosas sem sequer serem identificados:

> É importante compreender que a ressaca tecnológica traz uma relação de dependência, atingindo pessoas, empresas, governos e instituições. As relações comerciais migram para a Internet. Nesta janela, a possibilidade de visibilidade do mundo atual traz também os ricos inerentes à acessibilidade, tais como segurança da informação, concorrência desleal, plágio, sabotagem por hacker, entre outros. Assim, na mesma velocidade da evolução da rede, em virtudade do relativo anonimato proporcionado pela Internet, crescem os crimes, as reclamações devido a informações ao Código de Defesa do Consumidor, as infrações à propriedade intelectual, marcas e patentes, entre outras. (PINHEIRO, 2016, p. 78).

2.2 Sujeitos dos crimes cibernéticos

O sujeito ativo de crime cibernético assim como nos crimes comuns é aquele que prática uma conduta típica, antijurídica e culpável. Entretanto, tal sujeito apresenta certas características que o distinguem dos criminosos comuns. O primeiro aspecto,

de extrema relevância, é o alto conhecimento de sistemas informáticos, por meio do qual o delinquente consegue êxito em suas condutas, com a invasão de sistemas, adulteração, destruição ou sequestro de dados. Em suma, os criminosos não são leigos, ao passo que são inteligentes, cultos, alfabetizados e com reduzidos antecedentes criminais:

> Conforme já escrito acima, aquele que aproveita seu grande conhecimento em informática para por meio dela obter vantagem indevida possui traços de maior intelectualidade, normalmente não possui antecedentes criminais, trata-se de grande conhecedor também em assuntos gerais, dificilmente praticaria a conduta senão através de um computador, não possui traços de pessoa violenta, na maioria das vezes fala ao menos duas línguas. (COSTA, 2011, p. 118).

No âmbito digital, ao passar do tempo surgiu a necessidade de fazer uma distinção entre os sujeitos que utilizavam os seus conhecimentos informáticos para praticar certas condutas na Internet. Por causa disso, criaram-se as nomenclaturas *Hackers* e *Crackers*. (ALMEIDA et al., 2015).

Hackers são os *experts* em informática que utilizaram os seus conhecimentos para praticar condutas geralmente não criminosas. Muitas vezes procuram a fama com a invasão de sistemas informáticos, encontrando falhas e ajudando a corrigi-las. (COSTA, 2011).

Crackers, por outro lado, utilizam-se os seus conhecimentos informáticos para praticar condutas ilícitas. Também conhecidos como *hackers* não éticos, dotados da mentalidade criminosa. Porém, nem sempre os sujeitos ativos dos crimes virtuais são necessariamente *crackers*, à medida que um leigo em informática, dependendo do crime, pode perfeitamente cometer crimes cibernéticos. (COSTA, 2011). No mesmo sentido, explica Luiz Regis Prado:

> Segundo a terminologia utilizada na informática, aquele que invade tais dispositivos com finalidade ilegal, de obtenção de vantagem indevida ou de prejuízo alheio, é denominado *cracker. Cracker* é, portanto, o sujeito que 'invade sistema de computadores de outra pessoa, frequentemente em uma rede, supera senhas ou licenças em programas de computadores ou de outras formas intencionalmente quebra a segurança de computadores. Um *cracker* pode fazer isso visando lucro, maliciosamente ou para alguma finalidade ou causa altruística, ou porque o desafio está lá. Algumas invasões têm sido realizadas para demonstrar pontos fracos no sistema de segurança de um site'. Não se pode confundir *cracker* com *hacker.* Termo utilizado para designar o sujeito que é um 'aficionado por informática, profundo conhecedor de linguagem de programação, que se dedica à compreensão mais íntima do funcionamento de sistemas operacionais e a desvendar códigos de acesso a outros computadores. (PRADO, 2013, p. 394-395).

Quanto ao sujeito passivo, isto é, a pessoa pela qual sofreu a conduta omissiva ou comissiva, pode ser física ou jurídica. Normalmente, considerando o poder aquisitivo, as empresas ou instituições financeiras são as principais vítimas dos crimes informáticos, bem como entes públicos:

> Vê-se, assim, que não obstante os crimes cibernéticos sejam em sua maioria aptos a vitimar pessoa física ou jurídica, inclusive o Estado, como observado alhures, tem-se que as pessoas jurídicas são as principais ofendidas por tal espécie delituosa. Além de figurar no *cibercrime* como a principal vítima, sua posição nesta seara se mostra merecedora de muita atenção, como se verá adiante. (COSTA, 2011, p. 121).

2.3 Principais tipos de ataques cibernéticos

Com a crescente criação de novas ferramentas de entretenimento para os usuários, houve um aumento de oportunidades para os criminosos que utilizam esses meios. Por isso, quer seja através de e-mails, redes sociais, aplicativos, sites falsos ou códigos maliciosos infiltrados, o agente sempre utiliza da vulnerabilidade de sistemas informáticos ou da ingenuidade dos usuários para satisfazer o seu intento, a fim de que o indivíduo execute uma ação ou preste alguma informação:

> A prática de crimes de Internet é explorada através de vulnerabilidade de segurança nos equipamentos, softwares ou até mesmo pela ingenuidade humana, conforme descrito anteriormente. Antigamente, todas as ameaças eram tratadas como vírus de computador, porém hoje há uma gama imensa de tipos de ataques. (GUISSO, 2017, p. 27).

Os crimes cibernéticos geralmente são praticados por meio de códigos maliciosos, também denominados de *malwares*, com o intuito de executar ações danosas e atividades maliciosas em um computador. Em suma, os *malwares* são programas maliciosos desenvolvidos principalmente para atacar a vulnerabilidade de sistemas informáticos, praticando, assim, ataques e golpes em usuários com a consequente obtenção de informações confidenciais ou vantagens financeiras. (CERT.BR, 2017).

Além disso, os *malwares* não se limitam a uma única classificação específica. Existem uma série de tipos de ataques diferentes, dentre os principais, destacam-se o Vírus*, Worm*, Cavalo de Tróia, *Spyware, Botnets, Phishing*, *Backdoors*, *Hoax* e *Ransomware*.

O vírus tem a capacidade de se infectar em determinados arquivos e criar cópias de si mesmo, podendo, inclusive, alterar dados ou sistemas, destruir, alterar arquivos e programas (LIMA, 2016). Importante notar que o vírus não causa efeitos até que seja executado por alguém, ou seja, é imprescindível a execução do vírus para gerar danos ao sistema operacional do computador. (GUISSO, 2017).

Do vírus originam-se diversas espécies, como exemplo o vírus de *boot* que foi o percursor de todos os vírus, o qual se fixa na inicialização do sistema, impedindo-o de iniciar. Outra espécie, não menos importante, é o vírus *time bomb*, denominado também como bomba-relógio ou gatilho, no qual o programador determina um momento para que o vírus seja acionado e produza os seus efeitos no computador infectado. (WENDT; JORGE, 2013).

O *worm*, diferentemente do vírus, caracteriza-se pela capacidade de se reproduzir automaticamente sem a necessidade de se hospedar em arquivos. Geralmente se instalam em computadores por meio da vulnerabilidade do sistema ou por causa da falta de atualização de programas. Esses *malwares* são comumente encontrados nos e-mails que são enviados para todos os contatos da vítima ou também por meio de redes sociais. (WENDT; JORGE, 2013). Não bastasse isso, a cartilha de segurança do CERT.BR explica:

> Tipo de código malicioso. Programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o *worm* não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para se propagar. Sua propagação se dá por meio da exploração de vulnerabilidades existentes ou falhas na configuração de programas instalados em computadores. (CERT.BR, 2018, p.1).

Na sequência, o Cavalo de Tróia, também chamado de *trojan horse*, possibilita o acesso de forma remota do computador infectado, com a consequente obtenção de informações confidenciais como exemplo de senhas bancárias. (WENDT; JORGE, 2013). Para a Cartilha de Segurança do CERT, o Cavalo de Tróia “[...] é um programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário”. (CERT.BR, 2017, p. 1).

Glaydson de Farias Lima faz uma comparação histórica para explicar o Cavalo de Tróia como uma figura aparente, em forma de presente, utilizada para enganar o inimigo e invadir o seu território:

> Na história grega, Troia possuía uma imensa muralha intransponível pelo exército inimigo grego. Com a finalidade de invadir o espaço rival, os gregos ofereceram um gigante cavalo de madeira como presente aos troianos. Ao aceita-lo, deixaram que uma considerável quantidade de inimigos escondidos pudesse entrar nas defesas de Troia, permitindo a abertura dos portões para a posterior invasão dos demais soldados. (LIMA, 2016, p. 80).

Em contrapartida, o *Spyware* é denominado frequentemente com um sistema de monitoramento, por meio do qual coleta informações sobre o usuário do computador e enviam a terceiros. Normalmente é cometido por meio de *keylogger* e *screenlogger*. O primeiro é capaz de gravar os dados digitados no teclado do computador, ao passo que o segundo serve para capturar imagens do monitor e do cursor do mouse. (CERT.BR).

Os *botnets*, por sua vez, também conhecidos como zumbis, são programas maliciosos que permitem ao invasor o controle do computador de terceiro de forma remota, sem o conhecimento da vítima. Para Emerson Wendt e Higor Vinicius Nogueira Jorge (2013, p. 25), o *malware* em comento "[...] permite que um criminoso controle o sistema à distância. A vítima não sabe que o seu computador está infectado, nem que está realizando ataques contra outros computadores".

Segundo Glaydson de Farias Lima, os *botnets* servem para formar um grupo de computadores zumbis, que aguardam os comandos do agente para praticar uma conduta conjunta. Geralmente são usados para sobrecarregarem ambientes virtuais, impossibilitando que terceiros os utilizem. (LIMA, 2016).

Do mesmo modo, o *Phishing* tem o papel principal de buscar informações sobre os usuários de computadores através de envio de mensagens com a finalidade de induzir a vítima a preencher formulários com seus dados privados ou a instalar código maliciosos. As mensagens falsas geralmente simulam e-mails de bancos, órgãos governamentais, empresas, etc. (WENDT; JORGE, 2013). Sobre o tema, afirma Glaydson de Farias Lima:

> Com a redução do uso do e-mail (seu principal meio de propagação) e com a melhor dos filtros *anti-phishing* utilizados pelos principais sistemas de correios eletrônico do mundo, os criminosos têm migrado suas ações para o lançamento de falsas informações em sistemas de anúncio de redes sociais como o *Facebook* e o *Twiter*. (LIMA, p. 87, p. 2016).

No que tange o *Backdoor,* denominado também de "porta dos fundos", o criminoso pode controlar o computador infectado à distância por meio de uma rede ou

pela internet. A principal função é permitir executar comandos, apagar dados e alterar configurações do sistema, sem contar no furto de informações e até mesmo acionar a *webcam* para monitorar o que se passa na residência da vítima. (GUISSO, 2017).

Na sequência, o *malware Hoax* nada mais é do que um conjunto de falsas histórias divulgadas na internet, notadamente a fatos inexistentes, falsos e alarmantes. São comumente recebidos por meio de e-mails, nos quais os destinatários recebem a informação como forma de procurar ajudar, seja por ajuda financeira para entidades ou pessoas doentes, como também de pessoas desaparecidas, notícias sobre conspirações e perigos inexistentes que de alguma forma cause transtorno ou prejuízo para a vítima. (WENDT; JORGE, 2013). Nessa senda, a Cartilha de Segurança para Internet (CERT.br) define o *Hoax* como:

> Um boato, ou *hoax*, é uma mensagem que possui conteúdo alarmante ou falso e que, geralmente, tem como remetente, ou aponta como autora, alguma instituição, empresa importante ou órgão governamental. Por meio uma leitura minuciosa de seu conteúdo, normalmente, é possível identificar informações sem sentido e tentativas de golpes, como correntes e pirâmides. Boatos podem trazer diversos problemas, tanto para aqueles que os recebem e os distribuem, como para aqueles que são citados em seus conteúdos. (CERT.BR, 2018, p. 1).

Por fim, a utilização do código malicioso *ransomware* serve como suporte para que o agente, após se aproveitar da vulnerabilidade do sistema, sequestre, através da criptografia, os arquivos pessoais salvos no computador da vítima, impedindo-a de acessá-los. Em seguida, para obter o resgate dos arquivos sequestrados, o agente constrange a vítima a pagar uma determinada quantia, que é paga, geralmente, através de moedas digitais. (LIMA, 2016). No mesmo sentido, analisa a Central de Proteção e Segurança da Microsoft:

> O *Ransomware* é uma espécie de malware (software mal-intencionado) que os criminosos instalam em seu computador sem seu consentimento. O *ransomware* dá aos criminosos a possibilidade de bloquear seu computador de um local remoto. Depois, ele apresenta uma janela pop-up com um aviso de que seu computador está bloqueado e você não poderá acessá-lo, a menos que pague. (MICROSOFT, 2018, p. 1).

Dessa forma, pode-se dizer que o *ransomware* é uma ameaça que realiza o sequestro de arquivos e impede que o proprietário possa ter acesso aos seus dados. Por isso, o código malicioso em comento será abordado e detalhado minuciosamente no segundo capítulo.

3 O CÓDIGO MALICIOSO *RANSOMWARE*

O *ransomware* há anos vem se tornando uma preocupação para as autoridades policiais, vez que é um código malicioso que afeta não apenas pessoas físicas, como também empresas através de computadores ou dispositivos móveis das mais variadas formas. Além disso, anualmente, os ataques de *ransomwares* tornam-se mais sofisticados e causam danos consideráveis às vítimas.

À vista disso, entender o funcionamento do *ransomware* é de extrema importância para analisar os casos práticos, notadamente a conceituação, a classificação, as diferentes formas de manifestações, a tipificação legal da conduta e, não menos importante, a legislação nacional e internacional aplicável.

3.1 Conceitos e funcionamento do *ransomware*

O termo *Ransomware* se originou basicamente pela forma como se manifesta esse tipo de *malware*, derivando-se da junção entre as palavras *ransom* (resgate) e *software* (código/programa), que significa um programa de resgate. Assim, o *ransomware* é um tipo de *software* que se infiltra em dispositivos informáticos e criptografa ou compacta dados com senha, de forma que a vítima não consiga acessar os arquivos infectados. Por conseguinte, é formulado um pedido de resgate mediante um pagamento, através de exibição de imagens ou mensagens, que é realizada, geralmente, por meio de moedas *bitcoins*, não dissente:

> *Ransomwares* são softwares do tipo malware criados com o objetivo de infiltrar-se em sistemas sem a percepção de seu titular. Possui por diretriz criptografar ou compactar dados com senhas e assim bloqueando o acesso aos mesmos e, em muitos casos, inutilizando o dispositivo infectado. Posteriormente é iniciado um mecanismo de exibição de imagens/mensagens informando sobre como realizar o resgate dos dados mediante um pagamento. Estas solicitações são normalmente valoradas em bitcoins, devido ao extremo anonimato sobre as transações realizadas nesse sistema de pagamentos. (SAISSE, 2016, p. 1).

De acordo com o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil:

> *Ransomware* é um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate (*ransom*) para restabelecer o acesso ao usuário.

> O pagamento do resgate geralmente é feito via *bitcoins*. (CERT.BR, 2017, p.1).

As primeiras manifestações do *ransonware*, que se tem notícias, são datadas de 1989, período em que o código malicioso era denominado como AIDS, desenvolvido, inicialmente, por Joseph Popp. A sua principal função era de criptografar os arquivos existentes no computador e, após disso, exigir pagamento para que os dados fossem liberados. Todavia, uma vez descoberta a chave de criptografia, o código malicioso era facilmente ser derrotado, removido e rastreado o autor, o que causou a prisão e condenação na época de Popp ao cárcere privado pela *New Scotland Yard*. (SAISSE, 2016).

Em seguida, diante da evolução de sistemas operacionais mais complexos que favoreceram à prática de crimes informáticos, o *ransomware* voltou a ter impulso em 2005, surgindo uma nova era de ataques por meio desse código malicioso, que extorque as vítimas por meio de pequenas vulnerabilidades do computador e de um conhecimento socioeconômico mínimo do alvo:

> O *ransomware* realmente saiu de moda no final dos anos 90 e não voltou a entrar em evidência até 2005. A disponibilidade de esquemas mais complexos de criptografia, junto com uma maior capacidade de processamento dos sistemas, ajudou a dar impulso a essa nova era do *ransonware*, que continua em aceleração. Atualmente o *ransomware* é considerado uma das formas de ataques predominantes contra sistemas de computadores, exigindo apenas uma exposição limitada a vulnerabilidade e um reconhecimento mínimo do alo. Estima-se que uma das variantes mais conhecidas, o *CryptoWall* (atualmente extinto), foi capaz de extorquir 18 milhões de dólares até meados de junho de 2015 [...]. (LISKA; GALLO, 2017, p. 17).

Atualmente, além do *ransomware* ser um programa altamente sofisticado e veloz, as consequências têm o potencial de causar danos imensuráveis, uma vez que não há limites quanto o objeto do crime, podendo ser afetados hospitais, escolas, empresas, órgãos do judiciário e principalmente redes domésticas. (BORTOT, 2017).

O *ransomware*, em outras palavras, pertence a uma classe de códigos maliciosos que servem para extorquir digitalmente as vítimas, fazendo-as pagar um determinado preço. Além do mais, propaga-se das mais variadas formas, tanto em computadores como em dispositivos móveis, utilizando-se de sites, e-mails, arquivos disfarçados e até mesmo pela instalação de aplicativos vulneráveis:

> O *ransomware* é um tipo de malware que bloqueia sua tela de computador, impedindo que você acesse seus arquivos até que você pague uma certa taxa ou “resgate”, envolvendo fornecer sua senha ou seu dinheiro para o agressor anônimo. No passado, o *ransomware* foi projetado para desligar seus sistemas, travando telas de computador com uma mensagem de alerta exigindo um pagamento. Eles estão por aí há muito tempo e assumiram uma série de formas diferentes, mas, como qualquer outro empreendimento de sucesso, o *ransomware* evoluiu para uma série de variantes mais novas e mais perigosas. (MICRO, 2015, p. 1).

Muito embora cada ataque com o *ransomware* tenha particularidades diferentes, as principais formas são aquelas que criptografam ou impedem o acesso aos arquivos, bem como aquelas que restringem ou bloqueiam os usuários dos sistemas. Segundo Liska e Gallo (2017, p. 22) “as variantes modernas e eficientes de *cryptoransomware* tirarão proveito inicialmente de algum tipo de vírus de macro ou de falhas de PDF exploradas para acessar o sistema; sabe-se também que WSF, *Java* e *Adobe Flash* são usados”. Quanto a isso, outrossim, defende Renan Cabral Saisse:

> O *ransomware* é propagado das mais variadas formas, seja por intermédio de acesso aos sites suspeitos que liberam o código malicioso apenas com a visita do usuário ou por arquivos disfarçados (músicas, imagens, etc.), normalmente divulgados em redes sociais ou enviados por e-mail aparentando algo comum, de interesse público, cobranças, causas sociais, etc. Ainda podem ser liberados via instalação de aplicativos vulneráveis em dispositivos móveis ou computadores. (SAISSE, 2016, p.1).

No que tange aos mecanismos de funcionamento, o *malware* se opera inicialmente de forma silenciosa, sem que a vítima perceba ou tenha conhecimento, até que esteja totalmente incorporado ao sistema operacional. Posteriormente, faz-se um juízo de valor se a máquina valha realmente a pena ser infectada, em caso afirmativo, procede-se a desativação dos meios de proteção existentes no computador, como exemplo, a recuperação do sistema e qualquer programa *anti-malware* que possam comprometer o ataque cibernético pretendido. (LISKA; GALLO, 2017).

Em um segundo momento, o código malicioso passa a fase de acesso às informações do usuário, filtrando as informações específicas e relevantes que possam ser alvos de criptografia, tais como documentos de trabalho, multimídias e até mesmo imagens; podendo se infiltrar basicamente em qualquer arquivo existente no computador, não existindo limites. (LISKA; GALLO, 2017).

Além disso, segundo Allan Liska e Timothy Gallo (2017), o comando e a troca de informações entre o sistema operacional do criminoso com o computador da vítima

acontecem por meio de um canal de comunicação, também denominado de canal de comando. Por meio deste, possibilita ao criminoso avaliar se o alvo do ataque é realmente valioso, determinando assim a quantidade do resgate a ser pedido. Sem contar que, não poucas vezes, é provável que um usuário tenha um *ransomware* em estado dormente em seu computador neste exato momento esperando receber ordens do agente pelo canal de comunicação:

> Em um ataque de *ransomware*, depois que é implantando e instalado, o código malicioso começará a acessar seus servidores de comando em busca de instruções. Essas instruções podem ser quaisquer requisições específicas. Elas incluem de tudo, desde identificar os tipos de arquivo que devem ser alvos de criptografia, quanto tempo devem esperar para iniciar o processo e se devem continuar a se espalhar antes de inicia-lo. Em algumas variantes de *ransomware*, os código maliciosos também devolverão um volume significativo de informações sobre o sistema, incluindo endereço IP, nome de domínio, sistema operacional, navegadores instalados e produtos anti-malware. Essas informações podem ajudar uma organização criminosa a determinar não só quem foi infectado, mas também de um alvo altamente valioso foi atingido, sugerindo, assim, que esse comprometimento seja usado para propósitos mais nefastos que uma simples infecção de *ransomware*. (LISKA; GALLO, 2017, p. 24).

Ao final, depois de criptografados os arquivos selecionados, tornando-os inacessíveis, uma mensagem na tela do computador da vítima aparece informando sobre o bloqueio dos dados, bem como a quantidade ou a forma do resgate a ser paga para que ocorra a liberação dos respectivos dados. (SAISSE, 2016).

Ainda que não exista um único método de exigir o pagamento, algumas variantes de *ransomwares* atemorizam a vítima através do aumento progressivo do valor do resgate ou pela eliminação de parte dos arquivos criptografados pela demora da vítima para efetuar o pagamento. Todavia, insta esclarecer que mesmo procedendo o pagamento solicitado pelo agente, não existem garantias de recuperação dos dados:

> Depois que os arquivos são criptografados, uma tela é apresentada às vítimas informando-lhes como ocorreu o comprometimento. Os extorsionários usam vários métodos para exigir o pagamento. Algumas variantes de *ransomware* permitirão que você descriptografe um arquivo gratuitamente para provar que há uma chave para o seu sistema. Outras variantes têm pagamentos cujo preço a pagar aumenta com o passar do tempo até a chave ser apagada. O custo típico para desbloquear um sistema gira em torno de 300 a 500 dólares em bitcoins, mas algumas das variantes cujos alvos são corporações já cobraram valores que atingem dezenas de milhares de dólares. Algumas variantes mais recentes apagam arquivos para elevar o montante a ser pago e aterrorizar você a fim de força-lo a pagar o resgate mais rapidamente. Mesmo que você pague, não há garantias de que a chave

> que lhe será fornecida descriptografará seus arquivos. Além disso, não há garantias de que o *ransomware* será removido. De fato, os adversários espertos usarão a velocidade com que você pagará o resgate inicial, junto com qualquer informação adicional revelada pelo malware na própria rede, para determinar quais serão os próximos alvos em sua rede; esses podem incluir backups, repositórios na rede ou outros sistemas operacionais que sejam essenciais à operação de seus negócios. Então, eles usarão um *ransomware* mais ágil e sofisticado para fazer com que você continue pagando. (LISKA; GALLO, 2017, p. 26).

Como visto, a exigência do resgate dos dados se procede por meio de pagamento de um determinado valor, que gira em torno de 300 a 500 dólares, através de *bitcoins* ou de outras criptomoedas. A utilização de moedas digitais garante ao agente o anonimato de sua conduta e o recebimento seguro do valor, uma vez que essas moedas são como o real, euro ou dólar, entretanto, totalmente digitais e armazenadas em carteiras digitais nas nuvens ou nos computadores dos usuários, sem nenhuma regulamentação cambial de bancos ou Estados. (CERT.BR, 2017).

O *bitcoin*, principalmente nos dias de hoje, é uma moeda conhecida mundialmente e que pode ser utilizada por qualquer pessoa. Muito embora em casos excepcionais possam ser identificados os indivíduos por trás das transações, o processo de rastreamento é demorado e garante ao criminoso a rápida extração dos valores de carteiras de *Bitcoin*, conseguindo, assim, dinheiro vivo antes de ser rastreado:

> Mediante o exposto vemos o motivo da *bitcoin* ser tão atraente à seus adeptos, ainda que a necessidade de anunciar todas as transações publicamente por meio do *blockchain* possa parecer um risco à privacidade, porém não é, uma vez que as transações armazenadas publicamente possuem chaves criptografadas que precisam ser decifradas para descobrir a origem/destino, e ainda que sejam decifradas não necessariamente o possuidor da origem transacional será descoberto, uma vez que o mesmo pode utilizar pseudônimos e softwares ponto-a-ponto de difícil rastreabilidade como o navegador TOR. O usuário ainda pode operar de forma totalmente anônima na rede tomando medidas preventivas para ocultar o seu endereço IP e assim obter um nível máximo de privacidade, já que é dispensável a intermediação de instituições financeiras estando fora do alcance da administração tributária no caso do Brasil. (SAISSE, 2016, p. 1).

3.2 Principais espécies de *ransomwares*

A prática da extorsão por meio do *ransomware* atualmente afeta usuários de diversos países, principalmente aqueles em processo de crescimento. Porém, da mesma forma que os meios tecnológicos se desenvolveram os ataques de *ransomwares* evoluíram-se do mesmo modo. À vista disso, ao longo do tempo,

surgiram as mais variadas formas de *ransomwares*, embora com pequenas variações, cada versão apresentou peculiaridade que as distinguiram e demonstraram as suas eficiências em determinado caso. Dentre as principais surgidas nos últimos anos, impende destacar o *Ransomware Cerber, CryptoWall, Locky, CryptXXX, Petya, Wannacry* e para dispositivos móveis.

As primeiras famílias de *ransomwares* foram denominadas de *Cerber*, que era distribuído através de um *e-mail* ou *link*, e podia funcionar, até mesmo, desconectado da internet. Foi um dos primeiros ataques maliciosos que conversava com as vítimas através de um arquivo de áudio, de modo que aceitava resgate menor dos usuários que pagassem de forma antecipada, a fim de incentivar as vítimas a pagar o mais rápido possível e a não buscar outros meios de evitar o ataque. (MATEIU, 2017).

O *CryptoWall* foi uma das famílias de *ransomwares* que surgiu em 2013, e que teve uma grande popularidade, tendo em vista que se propagava através de *phishing* usando de anexos, ou explorava vulnerabilidades de programas, principalmente do *Adobe Flash*. As vítimas desse tipo de ataque, além de ter de lidar com a criptografia tinham que detectar quais arquivos eram infectados, porque alterava os nomes dos arquivos que criptografava. (LISKA; GALLO, 2017).

Na sequência, em meados de 2016, surgiu o *ransomware* Locky. Diferentemente de outras famílias, a criptografia do *Locky* não foi quebrada, isto é, por ser tão complexo e desenvolvido, não foi encontrado pontos fracos no processo de criptografia que permitissem que os arquivos fossem recuperados. Propagava-se, geralmente, por meio de faturas ou recibos de pedidos enviados por *e-mails*, os quais eram baixados e, a partir daí se infectava no sistema operacional. (LISKA; GALLO, 2017).

No mesmo ano, em 2016, surgiu o CryptXXX, que explorava falhas na *web*, notadamente por meio de sites comprometidos e anúncios infectados de códigos maliciosos. Os alvos no sistema operacional da vítima eram frequentemente os programas *Adobe Flash, Microsoft Silverlight* e *Java.* Além disso, a principal característica dessa família é que não criptografava apenas os arquivos, como também se apropriava de qualquer informação bancária que pudesse estar salvo no computador da vítima. (LISKA; GALLO, 2017).

De acordo com a Avast, outra família de *ransomwares* que teve grande impacto juntamente com o *ransomware WannaCry* foi o *Petya,* também originado em 2016. Uma das principais diferenças é que em vez de criptografar arquivo por arquivo, ele

bloqueava todo o disco rígido da vítima, impossibilitando de iniciar o *Windows*. Espalhava-se geralmente por meio de falsos aplicativos de *e-mail* contendo um *link* de *download* no *Dropbox*:

> Acredita-se que o *Petya* esteja por trás do imenso ataque de *ransomware* que afetou empresas e organizações em todo o mundo no final de junho de 2017. O país mais afetado nesse ataque foi a Ucrânia, com o metrô de Kiev, o Banco Nacional da Ucrânia e vários aeroportos, para citar alguns de seus alvos mais chamativos. Muitas empresas multinacionais também relataram que foram afetadas, como a Nivea, Maersk, WPP ou Mondelez. (AVAST, 2018, p.1).

Em seguida, uma família de *ransomware* aparentemente nova começou a infectar dispositivos a partir de maio de 2017, que passou a ser conhecido como *ransomare WannaCry*. (MATEIU, 2018). Ganhou sua reputação tendo em vista a amplitude dos primeiros ataques, chegando a criptografar arquivos e dados de vítimas em 150 países, notadamente instituições em todo o mundo, tal como verifica Jonathan Lemonnier:

> Os países mais afetados, de acordo com nossos dados, são (em ordem): Rússia, Ucrânia, Taiwan, Índia, Brasil, Tailândia, Romênia, Filipinas, Armênia e Paquistão. Mais da metade das tentativas de ataque que registramos foi na Rússia. Grandes instituições também foram muito afetadas, especialmente hospitais e outros serviços públicos. Muitos deles dependem de sistemas desatualizados para operar e simplesmente não atualizam seus sistemas. (LEMONNIER, 2017, p. 1).

O que diferençou das outras famílias foi que esta não oferecia nenhuma garantia de desbloqueio dos arquivos, muito embora fosse pago o resgaste. Além disso, outra peculiaridade presente no ataque era a infecção nos computadores das vítimas através de redes, a qual tinha a capacidade de se multiplicar em milhares de dispositivos em apenas algumas horas.

Por fim, como dito anteriormente, conforme a tecnologia evoluiu, os ataques virtuais adaptaram-se do mesmo jeito. Dessa forma, houve também um aumento gradativo de ataques de *ransomwares* em dispositivos móveis, principalmente em celulares com sistemas *Android* que são suscetíveis de ataques em razão do seu ecossistema maior, em relação dos *iPhones* da Apple:

> Infecções por *ransomware* em dispositivos móveis continuam a aumentar porque, como no mundo dos microcomputadores, eles são rentáveis. Infecções por *ransomware* em dispositivos móveis geralmente lidam com

> pouco dinheiro, entre 50 a 100 dólares, e geralmente não exigem uma conta de bitcoin para pagamento do resgate. Algumas das equipes de *ransomwares* móveis aceitam vales-presentes do iTunes como pagamento, enquanto outras buscam formas criativas para receber o pagamento. Para a maioria dos usuários de celular, pagar o resgate de valor relativamente baixo é mais barato no que diz respeito ao tempo gasto, em comparação a tentar reiniciar o dispositivo e restaurar os dados backup. (LISKA; GALLO, 2017, p. 215).

O método desse tipo de ataque, geralmente, é por meio de bloqueio que configura e restabelece o PIN do dispositivo (código de acesso), no qual sequer há uma criptografia e sim um bloqueio de acesso do sistema. (KASPERSKY, 2017).

3.3 Tipificação jurídica em âmbito nacional e internacional

Embora tenha sido uma prática difundida a pouco tempo e tenha ganhado relevância para o direito penal, não há legislação específica que tipifica e incrimina a prática de extorsão digital por meio de *ransomware*. Até porque o delito, praticado por meio deste meio, pode ser perfeitamente enquadrado nos tipos penais existentes no ordenamento jurídico brasileiro, não sendo necessário criar uma nova tipificação legal.

Por outro lado, esclarece Manuel Davi Masseno e Emerson Wendt (2018) que um dos únicos países a mencionar de forma expressa o *ransomware* foram os Estados Unidos, especificamente Código Penal da Califórnia (EUA, 2017), dispondo:

> Ransomware significa um contaminante de computador, conforme definido na Seção 502, ou trava colocada ou introduzida sem autorização em um computador, sistema de computador ou rede de computadores que restrinja o acesso de uma pessoa autorizada ao computador, sistema de computador, rede de computadores ou qualquer dados contidos nas circunstâncias em que a pessoa responsável pela colocação ou introdução do *ransomware* exigir o pagamento de dinheiro ou outra consideração para remover o contaminante do computador, restaurar o acesso ao computador, sistema de computador, rede de computadores ou dados, ou ainda remediar o impacto do contaminante do computador ou bloqueio. (MASSENO; WENDT, 2017, p. 1 apud Califórnia *Penal Code*, 2017, seção 523).

Na mesma linha, o Tratado de Conselho Europeu sobre Crime Cibernético (Convenção de Budapeste), adotado em 23 de novembro de 2001, teve grande importância sobre ataques informáticos. A referida convenção foi assinada por 43 países e ratificada por 21 das nações signatárias, na qual o Brasil não é membro efetivo, embora de ela estar aberta à adesão de outros países. (MASSENO; WENDT, 2017).

A Convenção de Budapeste, instrumento penal e processual penal de direito público internacional, foi criada, precipuamente, com a finalidade de manter a cooperação internacional das nações signatárias, por meio de criação de medidas preventivas e repressivas locais ao combate dos delitos praticados na Internet:

> A cooperação prevista nesse instrumento de direito público internacional se materializa por meio da criação de novos tipos penais puníveis - trata-se do primeiro instrumento jurídico transnacional de regulamentação da Web - que certamente deverá influenciar doutrinas e jurisprudências mesmo de países não signatários, como já vem acontecendo com a Lei Modelo da Uncitral e o comércio eletrônico. (KAMINSKI, 2016, p. 1).

Consequentemente, surgiram diversos instrumentos legais sobre delitos informáticos, que se originaram, essencialmente, pela transposição dos ensinamentos já constantes na Convenção de Budapeste. Exemplo disso foi Portugal em suas legislações internas, tais como o Código Penal (de 1995, com múltiplas atualizações), a Lei do Cibercrime (Lei n.º 109/2009, de 15 de setembro) e, também, a Lei da Proteção de Dados Pessoais (Lei n.º 67/98, de 26 de outubro). (MASSENO; WENDT, 2017).

No que tange ao Brasil, há a chamada Lei Carolina Dieckmann (BRASIL, Lei 12. 737/2012), que tipificou penalmente atos cibernéticos prejudiciais, tendo em vista o episódio que se sucedeu com a atriz Carolina Dieckmann, em que teve seu computador invadido, seus arquivos pessoais subtraídos e expostos na rede mundial de computadores. Dessa forma, incluiu-se no Código Penal Brasileiro o art. 154-A, que criminalizou a invasão de dispositivos informáticos. (BRASIL, 1940):

> 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. [...]. (BRASIL, 1940).

Em uma análise do tipo penal, nas palavras de Rogério Sanchez Cunha (2016, p. 241), o objeto jurídico do crime “é privacidade individual e/ou profissional, resguarda (armazenada) em dispositivo informático [...]”, por fundamento no art. 5º, X, da Constituição Federal de 1988, que tutela a inviolabilidade da intimidade, da vida

privada, da honra e da imagem das pessoas. (BRASIL, 1988). Por essa razão, a conduta é punida pela invasão de dispositivo informático alheio, mediante violação indevida de mecanismo de segurança ou instalação de vulnerabilidades. O dispositivo informático é entendido como qualquer instrumento com capacidade de armazenar e processar automaticamente informações, tais como *notebook, netbook, tablet, Ipad, Iphone, Smartphone, pendrive* etc. Além disso, com exceção da sua forma qualificada e majorada, o crime é de menor potencial ofensivo. (CUNHA, 2016).

Entretanto, tanto a legislação brasileira como a de Portugal são unânimes em afirmar que o *modus operandi* do *ransomware* corresponde ao crime de extorsão, uma vez que a invasão de dispositivo informático é absorvida pela consunção, por ser um crime de passagem necessária ao real crime pretendido pelo agente, que no caso, configura o delito de extorsão:

> Também conhecido como princípio da absorção, verifica-se a continência e tipos, ou seja, o crime previsto por uma norma (consumida) não passa de uma fase de realização do crime previsto por outra (consuntiva) ou é uma forma normal de transição para o último (crime progressivo). (CUNHA, 2016, p. 144).

O Código Penal Brasileiro tipifica a extorsão no art. 158, consubstanciando-se a conduta no verbo nuclear do tipo ‘constranger’ alguém a fazer algo, tolerar que se faça ou deixar de fazer alguma coisa, mediante violência ou grave ameaça, com pena de reclusão de quatro a dez anos, acumulados de multa:

> Art. 158 - Constranger alguém, mediante violência ou grave ameaça, e com o intuito de obter para si ou para outrem indevida vantagem econômica, a fazer, tolerar que se faça ou deixar de fazer alguma coisa: Pena - reclusão, de quatro a dez anos, e multa. § 1º - Se o crime é cometido por duas ou mais pessoas, ou com emprego de arma, aumenta-se a pena de um terço até metade. § 2º - Aplica-se à extorsão praticada mediante violência o disposto no § 3º do artigo anterior. § 3º Se o crime é cometido mediante a restrição da liberdade da vítima, e essa condição é necessária para a obtenção da vantagem econômica, a pena é de reclusão, de 6 (seis) a 12 (doze) anos, além da multa; se resulta lesão corporal grave ou morte, aplicam-se as penas previstas no art. 159, §§ 2º e 3º, respectivamente. (BRASIL, 1940).

No caso do *ransomware* a grave ameaça se resume na hipótese, resultante da criptografia, de a vítima vir a perder definitivamente a indisponibilidade do sistema informático e/ou dos dados pessoais armazenados. (MASSENO; WENDT, 2017). A grave ameaça, outrossim, por ser um instituto complexo, em que se leva em conta vários fatores, pode ser entendido como a intimidação psicológica de um castigo ou

malefício injusto e capaz de causar efetivo temor à vítima. No ponto, esclarece Rogério Sanches Cunha:

> A grave ameaça consiste na intimidação, isto é, coação psicológica, na promessa, direta ou indireta, implícita ou explícita, de castigo ou de malefício. A sua análise foge da esfera física para atuar no plano da atividade mental. Por isso mesmo sua definição é complexa, porque atuam fatores diversos, como a fragilidade da vítima, o momento (dia ou noite), o local (ermo, escuro etc.) e até mesmo a aparência do agente. Note-se que, não obstante a grave ameaça deva ser dirigida a alguma pessoa, não é necessário que seja contra sua integridade física, bastando que o mal prometido seja injusto e capaz de causar efetivo temor [...]. (CUNHA, 2016, p. 281).

Nesse contexto, impende destacar que o crime é formal, consumando-se independentemente da obtenção da vantagem desejada pelo agente. Em outras palavras, a extorsão se consuma independentemente do pagamento do resgate, por ser mero exaurimento da conduta. Da mesma forma, não obstante as expressões resgate ou sequestro de dados, não se aplicam os crimes de sequestro previsto no art. 148, tampouco da extorsão mediante sequestro do art. 159, ambos do Código Penal (BRASIL, 1940), haja vista que para esses delitos é necessário a privação da liberdade de uma pessoa, o que não acontece com o modos operante do *ransomware*:

> Analisando friamente poderíamos enquadrá-lo no Art. 154-A, § 2º, devido ao prejuízo patrimonial à vítima ou tentativa do mesmo, porém, além da observação do próprio parágrafo 2º sobre não constituir crime mais grave, o ordenamento jurídico brasileiro adota a Princípio da Consunção ou Absorção, ou seja, ação ou efeito de incluir algo menor em algo maior ou mais amplo. O crime claro, segundo o modus operandi do *ransomware*, é o crime de Extorsão (Art. 158 CP) por intermédio de dispositivo informático e assim absorvendo o crime de invasão de dispositivo informático (art.154-A). Vale ressaltar que, apesar da expressão sequestro de dados, o ato não se aplica ao crime de sequestro (art. 148 CP) ou extorsão mediante sequestro (159 CP), pois em ambos os casos é necessário haver privação de liberdade da vítima. (SAISSE, 2016, p. 1).

Portanto, apesar de o *ransomware* apresentar diferentes formas de agir, em regra trata-se de extorsão prevista no art. 158 do Código Penal, uma vez que o delito se manifesta através do constrangimento de vítima, por meio da criptografia de dados pessoais, mediante ameaça pelo fato de a vítima vir a perder todo o conteúdo do dispositivo informático (BRASIL, 1940). Além disso, a obtenção de vantagem econômica se perfectibiliza no momento em que é solicitado o resgate através do pagamento de uma determinada quantia em dinheiro da vítima. (CRESPO, 2015).

4 RANSOMWARE: A EXTORSÃO DIGITAL E SUAS IMPLICAÇÕES

Compreendidos o processo evolutivo, o conceito, as classificações e as características dos crimes cibernéticos, notadamente as reflexões a respeito do *ransomware*, faz-se importante analisar as implicações que essa nova prática criminosa se manifesta no meio da sociedade, a partir de documentários, notícias jornalísticas e depoimentos pessoais de profissionais que vivenciam tal pratica criminosa diariamente.

De início, cumpre destacar que todas as pessoas são alvos potenciais dos ataques de *ransomware*s, de modo que a simples vulnerabilidade no sistema operacional ou o despreparo dos usuários sobre conhecimentos mínimos de proteção são suficientes para gerar uma porta de entrada aos *cibercriminosos*. Por esse motivo, através de *bitcoins* e demais recursos tecnológicos, os criminosos estão utilizando gradativamente destes meios, por encontrar ambientes virtuais favoráveis à prática de extorsões por meio de *ransomwares*, principalmente em razão do anonimato e por não exigir um grau de conhecimento exacerbado de informática para invadir o computador da vítima e, porventura, extorqui-la a pagar o resgate.

Apesar de os ataques de *ransomware* terem evoluído consideravelmente, pode-se dizer que ainda não atingiram sua máxima capacidade danosa. A doutrina costuma dizer que estão na infância, no sentido de que ainda podem evoluir ainda mais, em sua capacidade de causar prejuízos aos usuários da rede. Visto que, da mesma forma que existem ferramentas disponíveis de segurança às empresas, há uma rede clandestina sofisticada promovendo, diariamente, a criação de novos tipos de códigos maliciosos e famílias de *ransomwares* prontas para serem testadas no âmbito virtual:

> Em outras palavras, as famílias de ransomware ainda estão em sua infância, porém estão evoluindo rapidamente, e até os grupos mais sofisticados de hackers as estão usando em seus ataques. O ransomware entrou no cenário de segurança em um momento interessante. Embora haja uma série de ferramentas avançadas disponíveis às empresas, desenvolvidas para detectar e interromper ataques de ransomware, há também uma infraestrutura clandestina sofisticada, instalada para promover um rápido desenvolvimento e implantação de novas famílias de ransomware. Há também um corpo significativo de conhecimento disponível online sobre o que funciona e o que não funciona na tentativa de implantar novos malwares. Esse corpo de conhecimento incluiu muitos códigos compartilhados em fóruns clandestinos, além de aprendizado a partir de erros em famílias mais antigas de ransomwares. Assim, de modo diferente dos desenvolvedores de tipos anteriores de malwares, os desenvolvedores de ransomware não estão

> começando do zero, e é por isso que essa ameaça encontrou rapidamente um lugar no arsenal de hackers com todos os níveis de habilidade. (LISKA; GALLO, 2017, p. 55-56).

Com efeito, as primeiras versões de *ransomwares* visavam apenas usuários de computadores domésticos, não sendo comum que empresas fossem vítimas de tais ataques. Atualmente, em contrapartida, as empresas têm sido alvos comuns da extorsão digital. Isso porque os donos dessas empresas, geralmente, utilizam sistemas eletrônicos antigos e com escassa proteção digital, o que se tornam alvos fáceis para os agentes:

> Em nenhuma área essa evolução rápida do ransomware é mais aparente do que no estudo de seus alvos. As primeiras versões de ransomwares tinham quase exclusivamente usuários de computadores domésticos como alvos. Era muito raro ouvir falar de uma empresa infectada por um ransomware [...]. Contudo, não demorou muito para que grupos de hackers percebessem que o mais provável era que as empresas pagassem resgates para fazer com que seus sistemas voltassem a executar. Companhas de spam em massa rapidamente se transformaram em campanhas de phishing, e essas campanhas começaram a ter certo nível de sucesso. Essa estratégia faz sentido, especialmente para ransomwares entregues como anexos. Muitos usuários domésticos não têm Microsoft Office instalado em seus computadores, mas quase todas as empresas têm. Considerando a popularidade dos documentos Microsoft Office como vetor de ataque, lanças ataques de ransomware contra empresas passou a ser um passo lógico. (LISKA; GALLO, 2017, p. 65).

De acordo com estudos divulgados pela TrendMicro em 2016, uma das maiores organizações de segurança de computadores do mundo, constatou-se que dentre 300 empresas brasileiras entrevistadas, 51% disseram ter sido vítimas de ataques de *ransomware* no ano anterior, 56% não tinham sistemas de proteção eletrônico e 54% responderam não possuir sistemas de detecção de criptografia. Não bastasse isso, os setores mais afetados no Brasil, dentre os 10 seguimentos analisados que foram atacados por *ransomware*, destacou-se, em primeiro lugar, a educação com 82%, o governo com 59% e o varejo com 57%. (TRENDMICRO, 2016).

Os agentes acabam por direcionar os ataques cibernéticos paras as empresas, porquanto tendem ser um negócio mais rentável e as chances são maiores de obter o pagamento do resgate solicitado. Não poucas vezes, as empresas chegam a pagar milhares de reais, ou até mesmo uma quantia superior, para recuperar as informações criptografadas, vez que a interrupção de serviços internos gera prejuízos financeiros imensuráveis para empresas, principalmente para aquelas que utilizam o sistema

eletrônico como principal ferramenta de trabalho. (LISKA; GALLO, 2017). No mesmo sentido, leciona Patrícia Peck Pinheiro:

> Pela nossa experiência, grandes empresas estão mais expostas, portanto, são alvos mais fáceis. Quanto mais famosa e conhecida uma marca, mais incidentes ela está sujeita a passar na Internet no tocante a uso não autorizado de marca, abuso de liberdade de expressão por terceiros, registro indevido de domínio ou similar a um domínio existente para fins de *cybersquatting*, uso da marca em *e-mails* falsos para ludibriar pessoas a passarem dados e a se contaminarem por arquivos maliciosos. (PECK, 2016, p. 391).

Para o Delegado de Polícia Civil do Estado do Rio Grande do Sul, Marco Antônio Arruda Guns, titular da Delegacia de Repressão aos Crimes Informáticos (DRCI), os ataques de *ransonwares* tiveram um aumento significativo devido ao fato da necessidade e dependência que o setor econômico passou a ter do meio virtual, precipuamente no que tange a banco de dados, como uma fonte de armazenamento de informações. (GUNS, 2018).

Nesta senda, através de uma análise no âmbito do Estado do Rio Grande do Sul, consoante informações prestadas pela Polícia Civil, tramitam cerca de quarenta investigações envolvendo extorsões virtuais por meio de *ransomwares*. Sendo que um desses casos foi vivenciado pela Audiprol Assessoria Contábil e Tributária S/S EPP, de Porto Alegre, em agosto de 2017. (ROLLSING; LOPES, 2018).

Conforme relatos do diretor da empresa, o ataque foi percebido ao chegar no trabalho e notar que os computadores, que continham informações de cerca de 6 mil empregados atendidas pela contabilidade, não estavam funcionando. Com o auxílio de técnicos em informática, constatou-se um *link* de acesso a uma janela de bate-papo, no qual era solicitado 10 *bitcoins* para devolver os dados sequestrados, equivalente a R$ 40 mil naquela época. Além do mais, observa o diretor da empresa:

> No primeiro impacto, entendi que não deveria pagar, embora o sistema fosse de extrema necessidade. Mandamos o HD (disco rígido) para três empresas de recuperação de dados. Nenhuma conseguiu. Isso levou 10 dias. Aí tive de voltar a negociar. [...]. Eram quase 40 anos de história dos clientes no sistema. Reconstruir isso era impossível. (ROLLSING; LOPES, 2018, p.1).

Entretanto, as atividades da empresa pararam, não lhe restou outra alternativa a não ser pagar o resgate. Através do chat de bate-papo, a empresa conseguiu reduzir o valor do resgate para 1 *bitcoin* (nove mil e seiscentos reais), tendo realizada a

conversão pelo *Citibank*, em uma conta não identificada. Ao final, enviada a chave para desbloquear a criptografia e não constatada a autoria do delito, os prejuízos somaram R$ 40 mil para a empresa:

> O prejuízo somou R$ 40 mil. Foram R$ 10 mil pelo resgate, R$ 20 mil nas tentativas frustradas de recuperar os dados do HD e mais R$ 10 mil investidos em segurança tecnológica. Na polícia, o inquérito que apurou o caso foi concluído sem autoria do delito [...]. (ROLLSING; LOPES, 2018, p.1).

Muito embora seja apenas um caso específico no Estado do Rio Grande do Sul, os ataques não param por ali. De acordo com um levantamento realizado em março de 2017, por Bruno Ferrari (2017, p. 1), "o ritmo de ataque às empresas brasileiras mostra o segundo maior crescimento do mundo, atrás apenas da índia", sem contar que em muitas situações os casos sequer chegam a ser levados a público, as empresas preferem manter o sigilo para não afetar a sua credibilidade e confiança:

> Ao longo das últimas semanas, ÉPOCA acompanhou casos de brasileiros donos de empresas de vários portes que sofreram ataques de ransomware. Todas pediram que não fossem identificadas. Por se tratar de exigências de resgate relativamente baixo para o orçamento de empresas – os criminosos pedem em média entre R$ 5 mil e R$ 20 mil –, muitas aceitam pagar e não comunicam a polícia. Quando decidem procurar alguma autoridade, as vítimas desses ataques raramente encontram respaldo adequado. "Cheguei a procurar a delegacia especializada em crimes digitais de São Paulo, mas fui orientada a fazer o registro da ocorrência numa delegacia comum", diz Maria. "Acabei eu mesma contratando um 'hacker do bem' para investigar as brechas e blindar nosso sistema contra novos ataques". (FERRARI, 2017, p.1).

Não bastasse isso, outro ataque de *ransomware*, de proporções maiores, que teve repercussão internacional, foi verificado em 12 de maio de 2017. Acredita-se que nunca antes na história, até o momento, houve um ataque cibernético dessa magnitude. O ataque foi tão bem-sucedido que, segundo o diretor da Europol (Agência Policial da União Europeia), atingiu cerca de 200 mil usuários, em pelo menos 150 países. (DEJONG, 2017).

O código malicioso, precipuamente, ficou conhecido como uma nova família de *ransomwares* chamada de *WannaCry*, também denominada WannaCry 2.0, em sua tradução literal "quero chorar". Ao contrário dos *ransomwares* comuns, além de se espalhar através de *e-mails* ou sites infectados, também infectava através de redes, característica esta similar ao *malware worm*, que ao infectar um computador conectado a uma rede, consegue se mover e atingir todos os dispositivos operacionais

ligados na mesma rede. Segundo Lemonnier (2017, p.1) “os *worms* de computador não se espalham ao infectar arquivos como os vírus, mas através de redes, procurando vulnerabilidades em outros computadores conectados”.

Com essas características o *ransomware WannaCry* espalhou-se para milhares sistemas operacionais em apenas algumas horas, atingindo diversos países. Os alvos principais foram companhias de vários setores, clínicas e hospitais, nos quais o valor dos resgates girava em torno de 300 dólares:

> Iniciado em 12 de maio, um enorme ataque cibernético de ransomware, chamado de WannaCry, se espalhou pela rede, criptografando arquivos de dados de vítimas em 150 países. A extorsão do malware afetou milhares de pessoas e enormes instituições em todo o mundo, como a FedEx ou Serviços de Saúde Nacional da Grã-Bretanha, a Telefonica da Espanha, os carros Renault da França e até a polícia estatal da Índia. (LEMONNIER, 2017, p.1).

Em poucas horas das primeiras ocorrências, o ataque chegou ao Brasil. Por precaução, vários entes públicos desligaram os sistemas eletrônicos, como no caso do Instituto Nacional do Seguro Social (INSS), o qual expediu um comunicado autorizando o desligamento dos servidores, a fim de preservar as informações internas:

> Considerando indícios de ataque cibernético detectado na rede mundial de computadores e a necessidade de preservar os dados pessoais dos cidadãos brasileiros. Considerando que foi autorizado o desligamento dos servidores na Dataprev, de modo a preservar a rede de informações internas. Desta forma, todos so microcomputadores devem ser desconectados da rede. Aqueles microcomputadores que sofreram ataque – os que tiveram tela vermelha – devem ser separados e mantidos desligados. (RODRIGUES; LUIZ, 2017, p.1).

Além disso, cerca de dez tribunais brasileiros desligaram o sistema do ar após as ocorrências que se sucederam em diversos países. Porém, apenas o Tribunal de Justiça de São Paulo confirmou ter detectado máquinas infectadas, nas quais foram recebidas mensagens que fixava o prazo de três dias para proceder ao pagamento do resgate, caso contrário o valor seria dobrado e após de sete dias os arquivos totalmente apagados. Sendo assim, o tribunal suspendeu os prazos processuais e determinou que todos os computadores fossem desligados. (LUCHETE; GALLI, 2017).

Ainda que os ataques atinjam empresas privadas e públicas de variados setores econômicos e jurídicos, nota-se que os golpes visam atingir o maior número

possível de alvos, isto é, espalham seus ataques por todos os mercados, que não poucas vezes são totalmente aleatórios, sem ter um alvo específico. (LISKA; GALLO, 2017).

Atualmente, e conforme verificado até aqui, a conexão virtual está tão interligada no cotidiano das pessoas, que os ataques acabam por ser uma prática rentável, motivo pelo qual houve uma migração das extorsões também para os dispositivos móveis, através da configuração e alteração do código de acesso (PIN) do aparelho, a fim de impedir que a vítima consiga acessa-lo:

> Infecções por *ransomware* em dispositivos móveis continuam a aumentar porque, como no mundo dos microcomputadores, eles são rentáveis. Infecções por *ransomware* em dispositivos móveis geralmente lidam com pouco dinheiro, entre 50 a 100 dólares, e geralmente não exigem uma conta de *bitcoin* para pagamento do resgate. Algumas das equipes de *ransomwares* móveis aceitam vales-presentes do *iTunes* como pagamento, enquanto outras buscam formas criativas para receber o pagamento. Para a maioria dos usuários de celular, pagar o resgate de valor relativamente baixo é mais barato no que diz respeito ao tempo gasto, em comparação a tentar reiniciar o dispositivo e restaurar os dados do *backup*. (LISKA; GALLO, 2017, p. 215).

Nesse sentido, os alvos não se limitam apenas as empresas ou dispositivos móveis, mas também, por exemplo, em dispositivos médicos. Especialmente pela precariedade de recursos financeiros, os hospitais tendem a ter versões desatualizadas de sistemas operacionais, o que acaba gerando uma vulnerabilidade para que os agentes consigam entrar na rede e instalar o programa malicioso. Sem contar que isso pode ir além do esperado, e até resultar em outras práticas criminosas diversas da extorsão digital, como o bloqueio de acesso a equipamentos médicos digitais necessários a própria mantença e sobrevivência de pacientes, podendo ocasionar em casos extremos o delito de homicídio. (LISKA; GALLO, 2017).

Além de tudo, os pedidos de resgates giram em torno de 1 a 5 *bitcoins*, isto é, em torno de R$ 30.000,00 (trinta mil reais) podendo chegar até R$ 150.000,00 mil reais (cento e cinquenta mil reais). São práticas criminosas modernas, que, não poucas vezes, são usadas como forma de levantar dinheiro para organizações criminosas que operam crimes de diversas ordens, por exemplo a lavagem de dinheiro. (GUNS, 2018).

Com efeito, explica a advogada Caroline Teófilo, em uma entrevista prestada para a revista Época, que “[...] os próprios criminosos preferem fazer ataques menos ambiciosos, que gerem um volume menor de denúncias e não chamem a atenção das

autoridades. [...] Eles querem um dinheiro que vem rápido e de diversas fontes". (FERRARI, 2017, p.1).

Os extorsionários, à vista disso, não exigem como resgate grandes quantidades em dinheiro, com algumas ressalvas a grandes empresas. Os criminosos preferem ataques com proporções menores e que não chamem a atenção das autoridades públicas, tornando-se de difícil elucidação e repressão os crimes, uma vez que, na grande maioria, sequer são levadas as investigações a cabo por falta de denúncias:

> 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 as equipes e profissionais preparados para a investigação de um crime virtual. [...]. 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 comercias com 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. (PECK, 2016, p. 382-383).

Por esse motivo, e conforme observado por Marco Antônio Arruda Guns, a elucidação de tal conduta criminosa para os órgãos de segurança pública, notadamente acerca da criptografia utilizada no computador da vítima, é mínima; outras, dependendo do grau de sofisticação utilizada, a desobstrução de acesso aos dados ocorre em minutos por operadores especializados na área da informática. Muitas vezes, como visto, o crime não chega ao conhecimento da autoridade policial, as vítimas preferem negociar diretamente com o extorsionário ou, até mesmo, contratar um profissional da área para descriptografar o acesso dos dados, a fim de evitar o pagamento do resgate:

> [...] Muitas vezes não há registro de boletim de ocorrência policial pelas vítimas terem ou negociado diretamente com o extorsionário ou mesmo a criptografia usada ser mais simples, passível, portanto, de ser aberta por operadoras com algum grau de conhecimento. [...] Dependendo do grau de sofisticação da criptografia, há níveis bastante diversos de criptografia usada. Algumas mais sofisticadas, tornando impossível, por ora, o esclarecimento pela investigação, outras mais simples, cuja desobstrução de acesso aos dados ocorre em minutos por operadores experientes, exemplo técnicos contratados. (GUNS, 2018, p. 1).

Entretanto, apesar da grande dificuldade em se localizar e indiciar os criminosos virtuais que se utilizam de moedas digitais, como o *bitcoins*, para mascarar o proveito econômico adquirido, recentemente, mais de R$ 710 (setecentos) mil *bitcoins* foram recuperados pela Polícia Civil do Tocantins e de Goiás, em uma operação que teve início em maio de 2018, na qual foram cumpridos mais de sete mandados de prisão temporária em face de investigados que são suspeitos de capturar dados bancários de vítimas:

> Mais de R$ 710 mil em bitcoins (moedas digitais), no Brasil e no exterior, foram recuperados pela Polícia Civil do Tocantins e de Goiás, por meio da Operação Ostentação que teve início em maio deste ano. Até agora, sete mandados de prisão temporária foram cumpridos contra investigados de participar das fraudes e foram descobertas 394 possíveis vítimas que tiveram seus dados capturados por hackers. [...] De acordo com a Polícia, a ação tem o apoio da Diretoria de Inteligência da Secretaria Nacional de Segurança, responsável pelo processamento e difusão dos elementos iniciais de informação que deram origem a investigação. Além disso, a operação contou com o apoio de mais de 60 policiais civis, reunindo a Polícia Civil do Tocantins, Diretoria de Inteligência do Ministério Extraordinário da Segurança Pública e Polícia Civil. (SANTOS, 2018, p.1).

À vista disso, a cooperação interestadual e internacional entre órgãos governamentais de segurança pública também é necessária para se buscar a efetividade das investigações policias, a fim de punir os autores que se aproveitam da vulnerabilidade dos usuários, por meio de códigos maliciosos, para praticar crimes em ambientes virtuais:

> Portanto, a adequada vigilância da Internet pela polícia e pelo Poder Judiciário, bem como de todas as tecnologias digitais e convergentes existentes ou a serem inventadas, permite uma ferramenta poderosa para a descoberta de redes criminosa que atuam no mundo real, mas se comunicam virtualmente. (PECK, 2016, p. 388).

A precaução, de igual forma, mostra-se uma maneira alternativa, confiável e segura para prevenção de crimes cibernéticos. Os investimentos em recursos informáticos de segurança são altos, mas sopesando as consequências dos custos de pagar um resgate ou restaurar o sistema após os ataques, torna-se de baixo valor o gasto em métodos de prevenção. (LISKA; GALLO, 2017).

5 CONCLUSÃO

Ao final do estudo, pode-se concluir que a evolução tecnológica fez com que os crimes fossem, gradativamente, adaptados à nova realidade digital, tornando-se um meio favorável à prática de condutas delituosas até então desconhecidas pelos usuários. Por isso, os crimes cibernéticos foram se tornando uma preocupação para o mundo jurídico, tal como ocorre na extorsão digital através do código malicioso *ransomware,* que tem a capacidade de afetar computadores, dispositivos móveis, pessoas físicas ou empresas públicas ou privadas, à medida que vem se transformando em uma técnica cada vez mais sofisticada, capaz de causar impactos em níveis inimagináveis.

À vista disso, três pontos passaram a ser questionados quanto à extorsão digital por meio do *ransomware.* Primeiramente, analisou-se o processo evolutivo da Internet e dos crimes cibernéticos, bem como os respectivos conceitos e classificações pertinentes. Interrogou-se, na sequência, o funcionamento do *ransomware* para a prática da extorsão digital, especialmente a sua integração e estruturação no ordenamento jurídico. Por fim, preocupou-se em demonstrar as particularidades do código malicioso *ransomware,* como uma ferramenta em constante transformação e evolução para a realização de práticas criminosas no ambiente virtual, analisando-se, assim, por meio de casos concretos, as principais incidências ocorridas em âmbito estadual, nacional e internacional.

Nesse contexto, ao longo do desenvolvimento do estudo procurou-se analisar tais apontamentos, com o auxílio de entendimentos doutrinários e legislativos, nacionais e internacionais, que versem sobre a problemática. Dessa forma, proporcionou-se alguns questionamentos importantes, que se fazem necessários dada a gradatividade com que o uso do *ransomware* passou a ser usado como uma ferramenta maliciosa e ilícita no mundo digital.

Constatou-se, portanto, nos últimos anos, que houve um aumento significativo de crimes cibernéticos, os quais são praticados, frequentemente, por meio de *e-mails*, redes sociais, aplicativos ou *sites* falsos, de modo que os agentes se aproveitam da vulnerabilidade de sistemas informáticos, bem como da própria inocência ou falta de conhecimento mínimo de informática da vítima, a fim de infectar o computador dela, através de programas maliciosos desenvolvidos especialmente para a obtenção de informações confidencias ou vantagens financeiras.

Muito embora exista uma série de classificações e espécies de *ransomwares*, observou-se que esse código malicioso serve, precipuamente, para extorquir digitalmente as vítimas, através da criptografia ou bloqueio de acesso aos arquivos pessoais, fazendo-as pagar um determinado valor da forma mais rápida possível, que não poucas vezes, atemorizam o alvo através do aumento progressivo do valor do resgate ou pela eliminação de parte dos arquivos inacessíveis pela demora para efetuar o pagamento. E, mesmo procedendo o pagamento solicitado pelo agente, não há garantia de recuperação dos dados bloqueados, tampouco a identificação do extorsionário, uma vez que o pagamento é exigido por meio de moedas digitais, tais como os *bitcoins*, que garantem o anonimato e a extração dos numerários antes mesmo de serem rastreadas.

Constatou-se que as empresas tendem a ser alvos com maior frequência, dada as melhores chances de obter o pagamento do resgate solicitado, uma vez que a interrupção de serviços internos pode ocasionar danos financeiros imensuráveis para as empresas, especialmente para aquelas que utilizam o banco de dados como principal ferramenta de trabalho, chegando a pagar, dessa forma, milhares de reais, ou até mesmo uma quantia superior, pra recuperar as informações criptografadas.

Acerca dos valores dos resgates, evidenciou-se que, de regra, não são exacerbados, com algumas ressalvas a grandes empresas. Os extorsionários preferem ataques com proporções menores e que não chamem a atenção das autoridades públicas. A vítima, não raras vezes, prefere negociar diretamente com o agente ou acaba contratando um profissional da área para descriptografar o acesso dos dados, a fim de evitar o pagamento do resgate, não chegando sequer ao conhecimento das autoridades policiais.

Por fim, verificou-se que os ataques podem estar fortemente ligados ao financiamento de organizações criminosas, por ser uma prática rentável, anônima e que não exige um conhecimento demasiado de informática. Por isso, observou-se que a cooperação interestadual e internacional entre órgãos governamentais de segurança pública se faz necessária para punir os autores que se aproveitam da vulnerabilidade dos usuários, por meio de códigos maliciosos, para praticar crimes em ambientes virtuais, que muitas vezes não são punidos dadas as barreiras da transnacionalidade criminal. De igual forma, a prevenção com medidas de segurança pode ser tomada para tentar mitigar as possibilidades de ataques cibernéticos, muito embora possa ser, também, um recurso demasiadamente caro.

REFERÊNCIAS

ALMEIDA, Jéssica de Jesus et al. Crimes cibernéticos. **Ciências Humanas e Sociais Unit**. Sergipe, v.2, n. 3, p. 215-346. Disponível em: <https://periodicos.set.edu.br/index.php/cadernohumanas/article/view/2013>. Acesso em: 28 abr. 2018.

A epidemia via internet. **PCWorld**, São Paulo. Disponível em: <http://www.cin.ufpe.br/~rdma/documentos/revistaPCWORLDseguranca.pdf>. Acesso em: 15 mai. 2018.

AVAST. ***Petya***. Disponível em: <https://www.avast.com/pt-br/c-petya#academy>. Acesso em: 08 mar. 2018.

BARRETO, Alesandro Gonçalves; WENDT, Emerson; CASELLI, Guilherme. **Investigação Digital em Fontes Abertas**. 2. ed. Rio de Janeiro: Brasport, 2017.

BRASIL. Decreto n. 2.848, de 7 de dezembro de 1940. **Diário Oficial da República Federativa do Brasil**, Rio de Janeiro, RJ, Poder Executivo, 7 de dezembro, 1940.

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

BRASIL. Portaria nº 148, de 31 de maio de 1995. **Uso da Rede Pública de Telecomunicações para acesso à internet**. Brasília, DF: Agência Nacional de Telecomunicações, 1995.

BORTOT, Jessica Fagundes. Crimes Cibernéticos: aspectos legislativos e implicações na persecução penal com base nas legislações brasileira e internacional. **VirtuaJus**, Belo Horizonte, v. 13, n. 1, p. 338-362, 2017. Disponível em: <http://www. periodicos.pucminas.br/index.php/virtuajus/article/view/15745/15745-56007-1>. Aceso em: 29 fev. 2018.

CERT.BR. **Cartilha de Segurança para Internet**. Versão 3.1. Disponível em: <https://cartilha.cert.br/>. Acesso em: 04 jan. 2018.

COSTA, Fernando José da. ***Locus delicti* nos crimes informáticos**. 2011. 355f. Tese (Doutorado em Direito) – Universidade de São Paulo, São Paulo, 2011.

CRESPO, Marcelo. *Ransomware* e sua tipificação no Brasil. **Canal Ciências Criminais**, 28 out. 2015. Disponível em: <https://canalcienciascriminais.com.br/ransonware-e-sua-tipificacao-no-brasil/>. Acesso em: 16 jun. 2018.

CUNHA, Rogério Sanches. **Manual de direito penal**: parte geral. 4. ed. Salvador: Juspodivm, 2016.

DEJONG, Peter. Diretor da Europol diz que ciberataque atingiu ao menos 150 países. **Folha de São Paulo**, São Paulo, 25 jan. 2016. Disponível em: <https://www1.folha.uol.com.br/mundo/2017/05/1883952-diretor-da-europol-diz-que-cibeartaque-atingiu-ao-menos-150-paises.shtml>. Acesso em: 12 jun. 2018.

FERRARI, Bruno. *Ransomware*: o crime quase perfeito. **ÉPOCA**, São Paulo, 30 mar. 2017. Disponível em: <https://epoca.globo.com/tecnologia/experiencias-digitais/noticia/2017/03/ransomware-o-crime-quase-perfeito.html>. Acesso em: 1 mar. 2018.

GUISSO, Leonardo. **Segurança Digital**: avaliação do nível de conhecimento da população sobre os riscos de segurança atrelados ao uso da internet na região de Bento Gonçalves. [S.l.]: Repositório da UCS, 2017. Disponível em: <http://www.repositorio.ucs.br/xmlui/handle/11338/3081 >. Acesso em: 7 mar. 2018, 17:30:40.

GUNS, Marco Antônio Arruda**. Proposta de perguntas para o Delegado Marco Guns acerca do tema da minha monografia**. Disponível em: <marcoaguns@gmail.com>. Acesso em: 14 jun. 2018.

KAMINSKI, Omar. Conheça o Tratado Internacional contra crimes na Internet. **Consultor Jurídico**, 24 nov. 2001. Disponível em: <https://www.conjur.com.br/2001-nov-24/convencao_lanca_tratado_internacional_cibercrimes>. Acesso em: 04 mai. 2018.

KASPERSKY. **Ransomware móvel triplicou significamente no primeiro trimestre de 2017**, 23 mai. 2017. Disponível em: <https://www.kaspersky.com.br/about/press-releases/2017_kaspersky-lab-ransomware-movel-triplicou-significamente-no-primeiro-trimestre-de-2017>. Acesso em: 28 mar. 2018.

LEMONNIER, Jonathan. *Ransomware WannaCry*: o que você precisa saber. **AVG**, 10 ago. 2017. Disponível em: <https://www.avg.com/pt/signal/wannacry-ransomware-what-you-need-to-know>. Acesso em: 16 abr. 2018.

LIMA, Glaydson de Farias. **Manual de direito digital: fundamentos, legislação e jurisprudência**. 1. ed. Curitiba: Appris, 2016.

LISKA, Allan; GALLO, Timothy. ***Ransomware*: defendendo-se da extorsão digital**. 1. ed. São Paulo: Novatec, 2017.

LUCHETE, Felipe; GALLI, Marcelo. Dez tribunais tiram site do ar após ataque cibernético mundial. **Consultor Jurídico**, 12 mai. 2017. Disponível em: <https://www.conjur.com.br/2017-mai-12/dez-tribunais-tiram-site-ar-ataque-cibernetico-mundial?utm_source=dlvr.it&utm_medium=facebook>. Acesso em: 02 mai. 2018.

MICROSOFT. **Central de Proteção e Segurança: o que é *ransomware*?**. Disponível em: <https://www.microsoft.com/pt-br/security/resources/ransomware-whatis.aspx>. Acesso em: 10 fev. 2018.

MASSENO, Manuel Davi; WENDT, Emerson. O ransomware na Lei: apontamentos breves de Direito Português e Brasileiro. **Direito & TI**, 17 jul. 2017. Disponível em: <https://direitoeti.com.br/artigos/o-ransomware-na-lei-apontamentos-breves-de-direito-portugues-e-brasileiro/>. Acesso em: 02 mai. 2018.

MATEIU, Monica. O guia definitivo para *ransomware*. **AVG**, 7 nov. 2017. Disponível em: <https://www.avg.com/pt/signal/what-is-ransomware>. Acesso em: 16 abr. 2018.

PINHEIRO, Patricia Peck. **Direito Digital**. 6. ed. São Paulo: Saraiva, 2016.

PRADO, Luiz Regis. **Tratado de direito penal brasileiro**, v. 4, 11. ed. São Paulo: Revista dos Tribunais, 2013.

ROLLSING, Carlos; LOPES, Rodrigo. Polícia Civil investiga 40 casos de crimes cibernéticos; saiba como se proteger. **GaúchaZH**, Porto Alegre, 13 abr. 2018. Disponível em: <https://gauchazh.clicrbs.com.br/seguranca/noticia/2018/04/policia-civil-investiga-40-casos-de-crimes-ciberneticos-saiba-como-se-proteger-cjfymg9hl02fx01tgfmqbmdtc.html>. Acesso em: 19 mai. 2018.

RODRIGUES, Mateus; LUIZ, Gabriel. INSS desliga sistemas no DF e libera servidores por ameaça de invasão hacker. **G1**, Distrito Federal, 12 mai. 2017. Disponível em: <https://g1.globo.com/distrito-federal/noticia/inss-desliga-sistemas-no-df-e-libera-servidores-por-ameaca-de-invasao-hacker.ghtml>. Acesso em: 19 mai. 2018.

SAISSE, Renan Cabral. Ransomware: “sequestro” de dados e extorsão digital. **Direito & TI**, 20 nov. 2016 Disponível em: <http://direitoeti.com.br/artigos/ransomware-sequestro-de-dados-e-extorsao-digital/>. Acesso em: 02 mai. 2018.

SANTOS, Lauane dos. Mais de R$ 700 mil bitcoins são recuperados após descoberta de invasão em 394 contas bancárias. **Jornal Do Tocantins**, Tocantins, 09 jul. 2018. Disponível em: <https://www.jornaldotocantins.com.br/editorias/estado/mais-de-r-700-mil-em-bitcoins-s%C3%A3o-recuperados-ap%C3%B3s-descoberta-de-invas%C3%A3o-em-394-contas-banc%C3%A1rias-1.1569676>. Acesso em: 20 jul. 2018.

TRENDMICRO. ***Ransomware*: O que é e como você pode se proteger,** 29 abr. 2015. Disponível em: <http://blog.trendmicro.com.br/ransomware-o-que-e-e-como-voce-pode-se-proteger/>. Acesso em: 25 mar. 2018.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira**. Crimes Cibernéticos: ameaças e procedimentos de investigação**. 2. ed. Rio de Janeiro: Brasport, 2013.

WENDT, Emerson; LOPES, Fábio Motta. **Investigação Criminal: ensaios sobre a arte de investigar crimes**. Rio de Janeiro: Brasport, 2014.