REVISTA THESIS JURIS

http://doi.org/10.5585/rtj.v9i1.16739
e-ISSN: 2317-3580
Recebido: 03 mar. 2020 – **Aprovado:** 25 maio 2020

RANSOMWARE E CIBERSEGURANÇA: A INFORMAÇÃO AMEAÇADA POR ATAQUES A DADOS

RANSOMWARE AND CYBERSECURITY: INFORMATION UNDER THE MENACE OF ATTACKS OF DATA

Mateus de Oliveira Fornasier
Professor do Programa de Pós-Graduação Stricto Sensu (Mestrado e Doutorado) em Direito da Universidade Regional do Noroeste do Estado do Rio Grande do Sul (UNIJUI).
Doutor em Direito pela Universidade do Vale do Rio dos Sinos (UNISINOS), com pós-doutorado em Direito pela University of Westminster (Reino Unido).
mateus.fornasier @unijui.edu.br

Tiago Protti Spinato
Mestrando em Direito pela Universidade Regional do Noroeste do Estado do Rio Grande do Sul (UNIJUI).
tiago.protti.spinato@gmail.com

Fernanda Lencina Ribeiro
Pesquisadora voluntária do Grupo de Pesquisa Direitos Humanos e Novas Tecnologias, do Programa de Pós-Graduacão Stricto Sensu (Mestrado e Doutorado) em Direito da Universidade Regional do Noroeste do Estado do Rio Grande do Sul (UNIJUI).
Advogada.
fehlencina@gmail.com

Resumo: Este artigo objetiva abordar a modalidade de sequestro de dados na internet conhecido como ransomware. Investiga, assim, a possibilidade de ser criada uma regulação jurídica suficiente para ao menos se mitigar esse crime. Como resultados, tem-se que: i) o ransomware representa um grande problema, pois os dados sequestrados são atualmente tão valiosos quanto moeda real, sendo que seu uso tem o poder de influenciar mercados, eleições e vidas humanas de uma forma muito profunda; ii) os pagamentos de resgate se dão mormente por criptomoedas, não reguladas por Estados, o que complexifica o rastreamento dos valores até o criminoso, fazendo com que a punição seja quase inexistente; iii) é necessária, para mitigar a sua ocorrência, a cooperação entre empresas, cidadãos e Estados, pois esse crime não se atém às fronteiras territoriais estatais, sendo praticado em qualquer lugar, com vítimas distantes. Metodologia: método de procedimento hipotético-dedutivo, com abordagem qualitativa e técnica de pesquisa bibliográfico-documental.

Palavras-chave: Ransomware. Cibercrimes. Regulação.

Abstract: This article aims to address the modality of data hijacking on the internet known as ransomware. Thus, it investigates the possibility of creating sufficient legal regulation to at least mitigate this crime. As its results, it could be found that: i) ransomware represents a major problem, as the data hijacked is currently as valuable as real money, and its use has the power to influence markets, elections and human lives in a very profound way; ii) ransom payments are made mainly by cryptocurrencies, not regulated by States, which complicates the tracking of values up to the criminal, making the punishment almost non-existent; iii) cooperation between companies, citizens and States is necessary to mitigate its occurrence, as this crime does not stick to state territorial borders, being practiced anywhere, with distant victims. Methodology: hypothetical-deductive procedure method, with qualitative approach and bibliographic-documentary research technique.

Keywords: Ransomware. Cybercrime. Regulation.

Para citar este artigo (ABNT NBR 6023:2018)

FORNASIER, Mateus de Oliveira; SPINATO, Tiago Protti; RIBEIRO, Fernanda Lencina. Ransomware e cibersegurança: a informação ameaçada por ataques a dados. Revista *Thesis Juris* – RTJ, São Paulo, v. 9, n. 1, p. 208-236, jan./jun. 2020. http://doi.org/10.5585/rtj.v9i1.16739.

Introdução

O advento de uma geração completamente nova de tecnologias rendeu diversos benefícios nas mais diversas áreas práticas e do conhecimento, sendo que mesmo os devaneios mais esdrúxulos das pessoas do passado não previram com precisão o que de fato seria possível para os cidadãos contemporâneos usufruírem. Porém, como há muito demonstrado historicamente, sempre que inovações chegam para colaborar com o conforto humano, existem indivíduos que tentem a subverter a ordem para tirar proveitos financeiros para si, sem qualquer cuidado com a ética ou legalidade de suas ações.

Ilustra essa afirmação um episódio recente. No ano de 2020, os operadores do ransomware Doppelpaymer, que tem foco em empresas, lançaram um site que tem o intuito de expor os dados roubados por eles, e se recusaram a pagar o resgate, podendo causar danos enormes a empresas. Isso demonstra que essas operações são altamente organizadas, e como expõe a notícia, esses ataques infectaram milhares de computadores, roubando uma quantidade muito grande de dados, reforçando assim a necessária busca por regulações eficientes sobre a prática (ABRAMS, 2020).

Justifica-se a relevância da presente pesquisa pela atual reestruturação das comunicações e da produção de bens e serviços na sociedade, o que levará inevitavelmente a mudanças profundas de paradigmas nas mais diversas áreas, sendo que o sistema jurídico tem de se adaptar rapidamente para não cair no atavismo em meio a tantas inovações. Essa reestruturação leva à necessidade de redefinição de várias noções jurídicas basilares: por exemplo, a definição moderna de crime — antes caracterizada, dentre outros fatores, pela presença dos sujeitos a ele relacionados em um meio físico — é atualmente questionável quando contraposta às violações cibernéticas, sendo então necessário que os Estados, em conjunto com a sociedade civil, empresas e indivíduos, possam exercer seu poder para que a tecnologia seja também fruto de discussões, não se quedando alheia ao progresso da humanidade nessas questões, o que poderia gerar o caos e incertezas tamanhas, que desestabilizariam grandes corporações e entidades governamentais, além do cidadão comum médio, que muito têm a perder com os ataques maliciosos.

Ocorre, assim, o uso da tecnologia para fins sombrios, corrompendo-se relações sociais, com o intuito de chantagear, obter vantagens econômicas ou causar constrangimentos na condição de conseguir algum favor ou beneficiamento indevido, sempre pelo meio da força de suas ações. A questão desses crimes virtuais se tornou rapidamente uma séria realidade, levando

os operadores e estudiosos do Direito a empreenderem maiores esforços para abarcar a sua complexidade, que configuraram situações antes sequer consideradas relevantes.

Essas questões são importantes para que se motive uma discussão acadêmica sobre os crimes que assolam a internet, com a intenção de promover maior segurança e acesso ao conhecimento para todos os que assim o busquem no ambiente cibernético. Para a Criminologia, trata-se de uma questão atinente tanto ao perfil dos praticantes de crimes virtuais, quanto das características dos meios onde ocorre, e também, quanto às suas consequências para as vítimas. Já em relação a estudos atinentes ao Direito Penal, a regulação e a tipificação tanto de crimes já estabelecidos nos ordenamentos jurídicos, quanto de novos, relacionados às práticas do ransomware, possui grande relevância para a operabilidade do sistema penal. E para o Processo Penal, há questões relevantes para a punibilidade, a persecução penal, a sua investigação, dentre outras.

Apresenta-se, como problema que guiou a presente pesquisa, a seguinte questão: com a rápida evolução das novas tecnologias, será possível, em um futuro breve, criar uma regulação jurídica suficiente para ao menos se mitigar os crimes digitais? A hipótese trabalhada é a de que a tecnologia é um dos fatores de melhora das condições sociais humanas, mas também gera malefícios quando usada para fins ilícitos como o roubo de dados e a chantagem, e que é necessário que ocorram regulações no ambiente internacional, tanto para regular os crimes, quanto para regular as plataformas de criptomoedas, principais meios de pagamento do resgate (o que caracteriza o ransomware).

O presente estudo tem como objetivo geral abordar o sequestro de dados na internet, conhecido globalmente como ransomware. Para a consecução desse objetivo geral, o artigo possui três objetivos específicos, cada qual correspondente a uma seção sua. A primeira dessas seções apresenta noções gerais sobre essa prática, estabelecendo os fundamentos dessa prática. Em segundo momento, busca entender como as práticas atinentes ao ransomware ocorrem, e que impactos têm para o crescimento da insegurança tecnológica, expondo seus riscos para uma melhor visualização do problema em um âmbito geral. Na terceira parte do trabalho encontram-se parâmetros para uma regulação jurídica que venha a coibir esse tipo de prática, sendo observada também a ocorrência desse tipo de prática delituosa em um ambiente conectado global, onde a questão territorial tem pouca influência prática.

A metodologia utilizada para a conclusão desse estudo se deu pelo método de procedimento hipotético-dedutivo, visto que se utilizou de bibliografias disponíveis para comprovar uma hipótese previamente definida pelo trabalho, com a investigação baseada na tecnologia e em possíveis ataques coordenados que fazem vitimas e movimentam um mercado

paralelo de valores expressivos, com abordagem qualitativa e técnica de pesquisa bibliográfico-documental.

1 Noções gerais acerca dos ataques ransomware

O termo ransomware é utilizado genericamente para que se possa identificar um tipo de malware comumente usados para a prática de crimes de extorsão, quando ameaçam as vítimas por meios digitais, obrigando-as a fazer pagamentos de valores específicos em moedas determinadas em troca de seus dados. (LISKA; GALLO, 2017). Para de fato explicar o que é ransomware, deve-se entender que esse conceito não é algo novo, e podendo suas origens ser encontradas no início da década de 1990, quando Joseph Popp escreveu os primeiros códigos maliciosos que viriam a infectar computadores, com o intuito de criptografar as suas informações, e obter valores financeiros através do desbloqueio das mesmas (LISKA; GALLO, 2016). Obviamente as tecnologias usadas nessa época não podem ser comparadas com o aparato atualmente disponível, o que de fato dificulta de forma hercúlea a tentativa de coibir esses crimes, que ocorrem em crescimento exponencial devido à falta de regulação e à dificuldade de punição de tais práticas maliciosas.

A definição mais aceita nos dias de hoje, e que conceitua bem o que é realmente o ransomware, é que se trata de um tipo especifico de malware que nega o acesso do usuário a seus dados, criptografando conjuntos inteiros de dados e demandando um resgate (*ransom*, em inglês) para que o usuário possa ter o acesso às suas informações restabelecido (HASSAN, 2019). Assim, essa prática também é conhecida chamada de sequestro digital, mudando o alvo que usualmente são pessoas, para os seus dados, que muitas vezes têm informações vitais e importantes para o funcionamento de empresas e outras formas de organização, ou mesmo valor sentimental para o seu dono individual.

Por mais que em um contexto de senso comum, a moral de grande parte da sociedade funciona com a ideia de que pagar resgate para reaver algo que já era seu, e foi tomado de forma ilegal, poderia contribuir para que os crimes continuem acontecendo, pois, usando a lógica, se não houvessem pagadores também não existiriam mais os adeptos da prática. Porém, essa lógica encontra um problema no *modus operandi* dos criminosos, que muito longe de roubarem apenas de grandes corporações, também têm seus alvos em pessoas comuns, que apenas têm seus dados guardados em computadores, discos rígidos e nuvens, que preferem pagar valores baixos, e ter o seu problema sanado logo, o que contribui para o crescimento da prática também entre pessoas comuns, não somente entre os grandes detentores de capital.

Essa problemática cria novos modos de extorsão virtual, gerando um mercado bastante lucrativo e sem precedentes, e que pode gerar inúmeros prejuízos, pois, antigamente, a lógica era a de roubar dados de grandes empresas usando de malwares, para vendê-los aos seus concorrentes como um tipo moderno de espionagem industrial, se valendo de roubo por autônomos, que depois tentavam capitalizar as informações. É impossível afirmar claramente que essa prática foi extinta, porém pensando que as grandes corporações que têm poder econômico são limitadas, e dificilmente incorreriam no erro de ter seus dados roubados de forma sistemática, se apresenta um mercado com mais possibilidades, colocando como vítima qualquer pessoa que faça uso da rede, assim a lógica que legitima o golpe se dá na quantidade de pessoas que podem ser atacadas.

Esse tipo de nova atitude se apresenta como uma facilidade para o criminoso, que vende os dados para os seus próprios detentores, e não precisa correr o risco de negociar com terceiros, que muitas vezes poderiam dificultar o negócio, acabando por expor o esquema, o que sempre é um motivo de preocupação para quem trabalha com atos ilícitos. Assim, esse mercado hoje em dia movimenta fortunas, e se apresenta como uma alternativa interessante para os tecnicamente capacitados que buscam auferir renda nas redes, de forma rápida, deixando a vítima sem qualquer escolha, pois o não pagamento incorrerá a perda dos dados sem qualquer tipo de restituição.

Para demonstrar a gravidade que tais atos estão gerando na sociedade, é possível apresentar alguns dados que corroboram o que foi dito, e demonstram que quantias alarmantes de capital estão sendo despendidas para alimentar essa indústria criminosa e que se apresenta hoje de forma altamente organizada. É importante citar que em torno de algumas semanas, cerca de 22 cidades na Flórida e no Texas desembolsaram entre 460 e 600 mil dólares pelo resgate dos seus dados após sofrerem ataques de ransomware em relação aos seus dados (BRILL, THOMPSON, 2019).

Esses argumentos demonstram que o ransomware possibilita a formação de um mercado ilícito em clara expansão, pelo fato de que apresenta altos índices de lucratividade para os que fazem desse ato uma forma sistemática de ação, com empresas e cidadãos muitas vezes aceitando pagar o resgate pedido, pelo fato de não poderem perder os dados que estão bloqueados. Na atual era de informação, os dados têm um alto valor de mercado, e grandes empresas de tecnologia trabalham monetizando as informações que têm de seus usuários, não podendo correr o risco de ter sua fonte de renda coibida por essas ações; dessa forma, preferem apenas efetuar os pagamentos, pois dessa forma o seu prejuízo ainda poderá ser menor do que se ignorar as ofertas maliciosas.

1.1 Chantagem cibernética e sua aplicabilidade nos tempos atuais

O ransomware não é essencialmente uma prática nova, e como demonstrado anteriormente, remete aos anos de 1990, porém nessa época o grande desafio dos criminosos era receber os valores pagos, pois as transferências de valores na época eram facilmente rastreadas, tornando a prática inviável. Porém com o advento das criptomoedas, os valores passaram a ser transferidos de forma segura e secreta para contas que não podem ser rastreadas, e isso se tornou muito popular nos dias de hoje, facilitando e tornando a prática mais frequente e lucrativa.

Assim, a prática se embasa em um vírus que está em um arquivo, e normalmente o alvo são as pessoas mais curiosas, recebendo o mesmo em e-mails, vídeos ou programas baixados para o uso pessoal. Depois da invasão o programa bloqueia o sistema operacional, fazendo com que a vítima tenha que efetuar um pagamento para que o mesmo seja desbloqueado, sendo importante também mencionar que muitas vezes o criminoso acessa a webcam da vítima e faz imagens de seus momentos íntimos como forma de chantagem (FERREIRA; KAWAKAMI, 2018).

O ransomware pode ser usado de formas distintas, que podem ser divididas em dois tipos que ainda se subdividem. Os primeiros dois tipos principais são aqueles que criptografam os dados, fazendo com que o usuário tenha acesso negado aos seus arquivos, e aqueles que bloqueiam o acesso dos usuários, restringindo o uso dos dados do seu próprio sistema (LISKA; GALLO, 2017). Por mais que sejam parecidos são práticas que usam de subterfúgios e técnicas diferentes, mas que sempre tem o mesmo resultado, a impossibilidade de acesso a dados por parte do seu detentor.

Ainda, qualquer sistema operacional está em risco de invasões por meio de ransomware, seja Windows, Android, iOS, etc. Em cada objeto e em cada sistema particular, o método de ataque utilizado é diferente, fazendo com que se espalhe facilmente e encontre a limitação de cada dispositivo, para assim realizar o ataque com precisão (LISKA; GALLO, 2017). A questão mais importante e que facilita os ataques é descobrir as fragilidades de cada sistema, e focar neles para bloquear os dados do usuário.

Estima-se que aproximadamente entre 2 a 3% da população mundial sofra ataques de ransomware por ano, isso resulta em milhões de casos espalhados, número este que vem crescendo cada vez mais, e essas taxas estão aumentando em um curto espaço de tempo (SIMIOU et al., 2019). Por mais que pareça uma porcentagem baixa se comparado com outros

tipos de crime, ainda assim são inúmeros casos que geram quantidades colossais de dinheiro em posse dos criminosos.

Com o avanço da tecnologia, as formas como os crimes são realizados também avançaram, mas sua tipificação penal continua a mesma, e os crimes tradicionais de roubo, extorsão e chantagem continuam acontecendo, ainda em maior escala — a diferença é que agora esses crimes comuns estão ganhando outras formas de execução, podendo, dessa forma, automatizar seus ataques (O'KANE; SEZER; CARLIN, 2019). Atualmente, os usuários individuais comuns têm sido um grande alvo para os criminosos, não apenas empresas e grandes organizações, pela facilidade de realizar os ataques, pela vulnerabilidade do sistema de internet que cada indivíduo podem possuir na sua residência e no trabalho, sem a segurança necessária para a proteção de dos, alcançando valores próximos a milhões de ataques realizados diretamente em contas privadas.

Outra importante questão é concernente ao modo como a população vai agir frente ao crescimento dos ataques cibernéticos — se ao ver sua empresa, seus familiares e afins sendo atacados, buscarão uma maior proteção contra esses ataques para, assim, barrar o crescimento dos mesmos, ou se as formas de modificação dos ataques vão se dar de forma tão rápida que não será possível controlar os criminosos (SIMIOU et al, 2019). Esse fato é importante para conscientizar também a população, demonstrando que os cidadãos comuns também são responsáveis pela sua própria segurança, devendo ficar atentos a arquivos suspeitos que recebem das redes, mesmo que venha de uma pessoa conhecida, que pode estar contaminada sem saber.

Por ter uma estrutura de propagação com ares pandêmicos, o ransomware pode se propagar irrestritamente, contando com o benefício de não ter limites territoriais, representando uma grave ameaça para a sociedade. A interdependência da estrutura dos Estados com o uso e manutenção de dados e segurança de rede é um fator intrínseco à manutenção da organização social apresentada em uma perspectiva global, podendo-se assim visualizar um grande aumento de crimes digitais, sendo necessário um duro combate para que tais práticas sejam coibidas de forma usual (ATAPOUR-ABARGHOUEI; BONNER; MCGOUGH, 2019).

Um fator importante é que na maioria dos ataques o pagamento é solicitado em criptomoedas, sendo assim, o rastreamento do pagamento para tentar encontrar os criminosos se torna quase impossível, propagando cada vez mais os ataques e tornando mais avançados os modos de ataques, com grande investimento a partir das quantias arrecadadas (AKAY, 2019). Dessa forma, os tanto os dados econômicos, quanto os serviços, infraestrutura, todos estão sujeitos a alguma perda empresarial a partir dos ataques, que estarão cada vez mais recorrentes,

como afirma Akay (2019, p. 12, tradução nossa) "espera-se que uma empresa seja atacada por ransomware a cada 14 segundos até o final de 2019".[1]

Esses dados demonstram que a situação dos ataques ransomware podem tornar as redes algo obsoleto, pois seu uso ficaria completamente prejudicado por esses crimes que continuam a se desenvolver, encontrando novas formas, e também mais refinadas para entrar dentro das redes e sequestrar os seus dados. Por mais que de certa forma, os dados passem um prognóstico deveras apocalíptico, sendo de bom alvitre atentar para que as redes tenham novas formas de combater os ataques, e que existam melhores regulações internacionais que pôr fim a essa prática prejudicial.

1.2 A proteção de dados como fator essencial na sociedade contemporânea

As informações pessoais diariamente despejadas nas redes compartilhadas, são inúmeras e fazem com que bancos de dados tenham uma visão praticamente completa de vidas, interesses, gostos e poder de compra. Isso faz com que esses dados sejam uma moeda muito valorizada no mercado, porque quem detêm a informação também sabe como devem proceder para seu produto vender mais, ou para controlar uma nação em um Estado autoritário.

Frente a isso é possível entender que a moeda mais cara do mercado nos dias de hoje, são os dados que empresas e indivíduos gratuitamente fornecem a organizações que exploram as redes, que de forma peculiar conseguem monetizar os mesmos para auferir lucro e fazer suas ações de marketing para o consumo de massa. Ocorre que existem cada vez mais criminosos que tentam acessar e roubar esses dados, para conseguir, com chantagem e ameaças, que valores sejam pagos para que a vítima tenha novamente acesso ao que já era seu por direito, um verdadeiro sequestro digital de dados, conhecido como ransomware.

Para que a segurança cibernética seja mantida, existem várias formas de blindagem de dados, como a utilização de antivírus, realizar o backup regular dos dados, firewalls de segurança, cópias via e-mail, entre outras formas de proteção importantes, principalmente contra-ataques criminosos realizados por amadores (BRILL; THOMPSON, 2019). Isso faz com que as informações e dados não fiquem restritas a apenas um local, minimizando o dano e retirando o poder do criminoso, que, ao roubar dados duplicados, não causará danos reais a vítima.

Ainda, para grandes empresas e organizações recomenda-se a aquisição de um seguro cibernético, pois nesses casos, o custo de combater um ataque pode ultrapassar US$ 100 mil,

[1] Texto original: "It is expected that a business will be attacked by ransomware every 14 seconds by the end of 2019".

exatamente por ser empresas de grande porte, os criminosos tendem a chantagear solicitando valores muito altos (BRILL; THOMPSON, 2019) — valores esses que são por muitas vezes, apenas uma pequena parcela do que de fato irão perder se não conseguiram novamente o acesso aos dados criptografados. Em razão disso, algumas companhias de seguro oferecem contratos de seguro cibernético, para que seus segurados estejam preparados para ataques e não tenham grandes prejuízos, com uma cobertura variada de acordo com a necessidade de proteção e o risco de violação de cada instituição. Contudo, espera-se que as vítimas aprendam como funcionam os ataques e assim consigam formas de se proteger de novos ataques, e vendo outras vítimas, consigam ter noção do alcance que essas ameaças podem ter, tendo a consciência que terão de decidir se vão ou não pagar pelos seus dados capturados (CARTWRIGHT; CARTWRIGHT, 2019).

Por outro lado, com o tempo e com o aumento dos ataques cibercriminosos, a forma como os criminosos tem se relacionado com as vítimas também evoluiu, com a experiência, foram se tornando cada vez mais profissionais, aprendendo como realizar a chantagem e a encontrar as vulnerabilidades de forma mais sofisticada, esbanjando novas estratégias do crime (CARTWRIGHT; CARTWRIGHT, 2019). E com esse refinamento das ameaças e técnicas de intimidação, ficou ainda mais complicado e danoso a extensão que esses ataques tem, pelo fato de que a profissionalização dos criminosos ocorre em larga escala pelo planeta.

Aqui estão presentes dois grandes extremos: o do usuário, que tenta se proteger buscando novas tecnologias e segurança de informação, e o dos criminosos, que desenvolvem e utilizam novos meios de ataques a esses sistemas, para que a vítima, mesmo quando já sofreu um ataque anterior, e já buscou meios de proteção, esteja novamente correndo risco de perda de dados, e assim, que um novo ataque, agora mais elaborado, tenha sucesso (CARTWRIGHT; CARTWRIGHT, 2019). Isso demonstra uma tentativa vil de adaptação por parte dos infratores, que de fato conseguem atacar com maior refinamento as mesmas pessoas que já foram atacadas e muitas vezes colocaram em prática planos de contenção de danos.

Em resposta a isso, há autores que defendem o desenvolvimento do Direito Criminal Cibernético, para que se possa obter respostas mais eficientes e adequadas aos crimes e assim, proporcionar aos usuários uma maior segurança jurídica ao passarem por esse tipo de situação, com novas garantias além das já constituídas na Constituição (FERREIRA; KAWAKAMI, 2018). Com as transformações ocorridas na última década, o Direito Penal precisa se adaptar as novas condutas, principalmente no que se refere ao uso de dados, aos crimes de chantagem e extorsão de forma cibernética e ainda nos novos crimes. A sociedade precisa de proteção, e espera que o sistema jurídico pena de conta de responder a essas novas formas de pratica de

crimes. No Brasil ainda não há uma legislação específica, para que se possa resolver, investigar e punir os novos ataques, o que resulta em uma necessidade urgente de adaptação tanto de definições criminais quanto de investigação e punição, já que não há como utilizar as soluções presentes no ordenamento jurídico, pois são inadequadas (FERREIRA; KAWAKAMI, 2018).

Para resolver o problema com ataques de ransomware, poderia ser usado um novo sistema baseado em inteligência para o acompanhamento dos pagamentos realizados, uma tentativa de identificar quem está realizando a operação e solicitando o resgate (PAQUET-CLOUSTON; HASLHOFER; DUPONT, 2019). Uma organização, após sofrer vários ataques, com seus dados e recursos limitados, poderia projetar seus recursos para os ataques mais influentes, e ainda, investir na conscientização, na proteção de dados e investir em metodologias eficientes para que se possa lidar com proliferação de ataques.

Com o aumento dos ataques de ransomware, os mesmos estão sendo considerados como uma das ameaças mais graves à segurança cibernética, que tem afetado grandes empresas, o que comprova isso é o fato de que os novos ataques cresceram 30 vezes desde 2015, e estima-se que os ataques estão aumentando de uma taxa de um ataque a cada 40 segundos para um ataque a cada 14 segundos (HASSAN, 2019).

Assim, e como demonstrado por dados reais, os ataques de ransomware estão em franca escalabilidade, com um crescimento exponencial que se apresenta como uma epidemia nas redes de todo o mundo, ocorrendo pelo fato de que a regulação e as punições são quase inexistentes, e o valor recebido nessas operações costuma compensar o esforço realizado. Muitas vezes as pessoas e empresas com medo de perder os seus dados, simplesmente aceitam a chantagem, realizam o pagamento e sequer procuram as autoridades competentes, e devido a isso é possível entender que o número de ataques, que mesmo agora já alarmantes, podem ter um número muito maior que não é conhecido.

Frente a isso a proteção de dados se torna um fator primordial na sociedade contemporânea, que cada vez mais depende das redes para guardar informações importantes e que são relacionadas com a segurança e manutenção da vida humana e da sociedade como conhecida. Então, é necessário que esse assunto seja pautado como algo de extrema prioridade, e que não pode ser vista apenas como um mal menor causado por criminosos, mas sim um caso de pandemia tecnológica.

2 Ransomware e a cibersegurança

No atual contexto social, a internet está cada vez mais presente em vários aspectos da vida em sociedade, desde relações pessoais, passando por relações negociais, de aquisição de adquirir conhecimento, lazer, etc. Em outras palavras, praticamente toda comunicação social pode usar a Internet como substrato, conectado por fio ou não (PRASAD; ROHOKALE, 2020). Dessa forma, é conexão se torna um fator de grande importância, para que cada um tenha acesso a esses serviços, sem conexão, não há como partilhar dados nem realizar tarefas, e é devido a essa conectividade que se torna possível o rastreamento de dados de todos os usuários e objetos por meio do endereço de IP. Pode-se usar de exemplo à formação do estado, onde se permitiu a restrição de certas liberdades, para a confecção de um contrato social que seria benéfico a toda sociedade, e nos novos tempos, abdica-se da privacidade para usufruir das benesses que a tecnologia pode proporcionar a todos.

Nesse momento, os usuários usam a internet constantemente e acreditam que estão seguros, que está sendo respeitadas sua privacidade e segurança, sem se precaver de possíveis vulnerabilidades que possam existir, e então acontecem os ataques, a partir de pequenas portas que ficam entreabertas, gerando um problema inimaginável aos usuários. E como antes referido, os dados que todos armazenam em dispositivos pessoais, são hoje em dia um dos mais valiosos bens que uma grande corporação ou alguém mal-intencionado pode possuir, fazendo assim com que os ataques e fraudes sejam frequentes e sistemáticos.

A previsão é de que em um futuro não muito distante, será utilizada a quinta geração do sistema de comunicação móvel (5G), voltada especificamente para o usuário, fazendo com que os possíveis ataques à segurança cibernética tomarem proporções nunca antes percebidas. O que pode gerar um paradoxo entre a rápida conexão, podendo a mesma ser usada pelas pessoas para fins benéficos, mas que também poderia auxiliar a quem tem planos de fazer ataques ransomware a dados alheios.

Visto isso, compreende-se que a tecnologia surge como uma das principais forças motrizes da sociedade, pois é capaz de expandir, adaptar e atualizar, modificando comportamentos e ambientes, utilizando sensores inteligentes que podem fornecer dados para serem processados e a partir disso serem praticamente infinitas as possibilidades as quais os seres humanos terão de lidar com o advento das novas tecnologias (AKHILESH; MÖLLER, 2020). Por esse motivo se faz importante que uma área tão gigantesca em possibilidades, tenha suas regulações e limites, para que ela não seja um grande espaço de violações e crimes, sendo essa uma luta global e de cooperação entre os países, pois pela primeira vez, as fronteiras foram

derrubadas, e os crimes não têm mais o caráter territorial que antigamente era inerente a eles. Esse progresso está cada vez mais excluindo restrições e alcançando níveis extraordinários, atendendo as particularidades e necessidades de empresas, famílias, negócios, mobilidade, entre outros fatores, o que faz com que a tecnologia tenha um grande impacto principalmente pelos próximos anos, permanecendo cada vez mais na forma de vida do ser humano.

Baseando-se nessa perspectiva, e na realidade de escalabilidade das novas tecnologias nas relações sociais, assim como nos tempos antigos, quando os piratas saqueavam os navios da coroa com seus corsários, hoje há criminosos análogos — porém, que navegam dentro das redes, com a intenção de subtrair os dados e cometer gigantescas fraudes, que podem gerar prejuízos gigantescos. Por isso a discussão sobre a cibersegurança deve ser cada vez mais um tema importante, pois já se entende que a indústria do crime digital movimenta quantidades inacreditáveis de dinheiro no planeta, sendo a fonte de renda de inúmeros piratas modernos.

Não se pode mais falar nos tempos atuais na atuação de grandes empresas e corporações sem o uso das redes, da internet e também da tecnologia, que surge de forma a facilitar as ações corriqueiras, sendo agora um padrão absoluto dentro desses ambientes, o que pode levar a grandes perigos sobre a segurança, pois a quebra de sua privacidade pode afetar diretamente pessoas, instituições e a segurança de inúmeros usuários que tem seus dados expostos às atividades criminosas. As empresas especializadas que utilizam cada vez mais softwares e tecnologia em todos os seus segmentos estão cada vez mais sofrendo ameaças de ataques e sofrem com o constante medo de enfrentar a perda de seus dados e à segurança de seus contratos, equipamentos, e principalmente a todo suporte que a internet e a tecnologia têm representado para grandes empresas (SABHARWAL; SHARMA, 2019).

E não somente falando em grandes empresas, em um futuro próximo, com o advento das casas inteligentes, poderá ocorrer a conexão de todos os sistemas de uma moradia com a tecnologia, permitindo a mesma abrir portas, ligar luzes ou fazer funcionar aparelhos domésticos. Assim grandes partes das residências vão estar cada vez mais conectadas e dependes da tecnologia, com isso é necessário que se desenvolvam pesquisas para auferir o quanto esses dispositivos são frágeis a ataques e como um sistema que consegue realizar tarefas tão complexa não é capaz de identificar ameaças de forma autônoma, e assim diminuir os riscos para os usuários. Solucionar essas questões é imprescindível para se conferir maior segurança na utilização dos dados dos usuários.

2.1 Segurança de dados e o ransomware

O ransomware é o instrumento principal de uma forma de chantagem, mediante a qual indivíduos maliciosos acessam os arquivos do sistema de dados e os capturam e criptografam, tornando quase impossível recuperá-los sem a utilização de uma chave que está sob o seu controle (MAIGIDA et al, 2019). Esse tipo de coação se demonstra como um ótimo meio de auferir ganho para os criminosos, que ao privarem as vítimas de seus dados, muitas vezes as colocam em situações desesperadoras, envolvendo seu trabalho, ou mesmo sua vida pessoal com a perda fotos e lembranças que não poderão ser recuperadas se o pagamento não ocorrer de forma rápida.

Assim, aparece uma mensagem na tela do computador do usuário, cobrando um valor determinado e estabelecendo os passos necessários para que possam recuperar seus dados, mediante pagamento de altos valores para descriptografar os arquivos perdidos. É importante ressaltar que normalmente o criminoso arbitra um tempo muito curto para que o pagamento seja feito, não deixando com que a vítima possa refletir sobre o ataque, e fazendo com que aja de forma impulsiva, para que tenha seus dados devidamente recuperados.

Ainda, é importante mencionar que uma das principais características desse tipo de ataque, é o ambiente, que se torna importante na concretização do crime, e vem sendo utilizado principalmente nas plataformas Windows e Android, por conta das vulnerabilidades destas. Dessa forma os ataques bem-sucedidos vêm servindo de incentivo para outros usuários praticarem os mesmos atos ilícitos, em maior quantidade, nessas plataformas.

Esses sistemas operacionais, são conhecidos pelo seu código, que é aberto para desenvolvedores que podem criar programas e aplicativos, que são vendidos ou distribuídos de forma gratuita nas plataformas e assim, são os sistemas hoje com mais uso no planeta, por serem de certa forma mais intuitivos e simples. Eles também, na maioria dos casos se demonstram populares em números pois, os dispositivos que aceitam esses sistemas muitas vezes podem ser encontrados por valor mais baixos, o que os torna atrativo para grande parte da população mundial.

Os impactos desses ataques são enormes, incluindo a perda de dados, arquivos e informações por meio de criptografia, e pode ir muito além. Como por exemplo com um sistema de desligamento, em locais como hospitais, clínicas entre outros, o ataque pode causar uma perda ou confusão de dados dos pacientes, ou até mesmo desligar equipamentos médicos importantes para a sobrevivência, levando possivelmente o paciente a morte.

Dessa forma, os pesquisadores de segurança e tecnologia vêm buscando meios de solucionar esses ataques, e ainda prevenir os mesmos, para que haja mais segurança entre os usuários e que a solução seja duradoura, visto que a tecnologia está em constante transformação. Pois como se pode constatar, não mais apenas os dados dos seres humanos podem ser bloqueados por esse tipo de ação, mas as consequências podem ir para esferas práticas da sociedade, inclusive podendo causar um sério dano a vida de seres humanos que estão sendo tratados em hospitais com o auxílio de sistemas ligados a redes.

Existem duas principais tendências atualmente, que discutem a segurança cibernética quando utilizadas na área médica, sendo que a primeira aborda o crescimento da utilização da tecnologia por profissionais da saúde, com novos dispositivos e novos usos de sistemas para o benefício dos pacientes. Sistemas, *softwares* e computadores que desempenham funções cada vez mais complexas (WIRTH; GRIMES, 2020). Esses sistemas inovadores podem vir a serem grandes aliados da comunidade médica para mitigar erros e tornar a detecção de doenças uma prática mais célere, sendo uma realidade já nos dias de hoje, e claramente demonstrando que terá um crescimento exponencial com o passar dos tempos.

A segunda discussão revela a forma como os ataques vêm se atualizando e aumentando, se mantendo cada vez mais sofisticados e protagonizando ameaças mais destrutivas, causando prejuízos cada vez maiores para a saúde dos pacientes que necessitam destes dispositivos médicos, os quais enfrentam ameaças que não foram projetados com um sistema de defesa, pois só agora foi possível perceber a vulnerabilidade desses sistemas. Esse erro se deu pelo fato de que os desenvolvedores não conseguiram prever que ataques ransomware poderiam também afetar esse tipo de equipamento, pois na época de seu desenvolvimento, sequer era cogitado que isso poderia ocorrer.

Assim, com base na análise de dados e de ransomware, é possível concluir que a melhor forma de proteção contra os ataques, para prevenir e dessa forma criar um mecanismo de defesa, é realizar um backup dos artigos regularmente, além de buscar novos avanços tecnológicos que possam trazer mais segurança ao usuário, como desenvolvimento de algoritmos para proteção de dados (MAIGIDA et al, 2019). Esses mecanismos de defesa devem ser efetivos, e a prática do *backup* precisa se tornar algo inerente a esses serviços, para que a comunidade tenha mais segurança e possa confiar na tecnologia aliada aos serviços de saúde.

Outro setor que pode ser virtualmente destruído com o advento desses ataques maliciosos, é o das novas moedas digitais, conhecidas como criptomoedas sendo a mais popular e valiosa delas a moeda conhecida como *Bitcoin*. Quantidades astronômicas de dinheiro circulam por esses meios, e elas podem ter a sua segurança corrompida por ataques ransomware

que visariam tornar o acesso do proprietário da moeda impossível, fazendo com que a chantagem possa cobrar valores para que o mesmo tenha novamente sua carteira disponível.

As pesquisas e descobertas avançadas nos garantem que não existe um remédio fácil e específico para todos os casos de ameaça por meio de cripto-ransomware, por ser uma ameaça tão complexa e em constante atualização, com uma capacidade enorme de se adaptar a cada ponto fraco em cada sistema, e ainda, burlar as tentativas de controlar as ameaças (CONNOLLY; WALL, 2019). Assim, não se podem buscar respostas simples para problemas complexos, frente a esse problema, visto que os sistemas estão em constante mutação, mas também os que buscam atacar e se infiltrar nele, gerando assim uma eterna luta para melhorar a segurança, e por outro lado, uma tentativa de quebrar e adentrar em locais privados para se apropriar de dados.

As formas utilizadas de ataques incluem desde truques psicológicos até as pequenas deficiências do sistema, com pequenos erros na proteção de arquivos, na negligência de responsáveis, e na utilização inadequada de serviços (CONNOLLY; WALL, 2019). Fala-se em truques psicológicos, pois muitas vezes o criminoso precisa de um ponto de acesso em um sistema, com a instalação de um malware que pode, por exemplo, ser colocado em um computador, e dele, ser espalhado para os próximos, e faz isso com o uso de e-mails ardilosos ou usando de abuso de confiança.

Com isso, para que se possa proteger o sistema desses ataques, o mecanismo de resposta deve ser dividido em camadas, sem deixar passar nenhuma possível ameaça, para que assim se tornem mais resistentes, impedindo que os ataques de ransomware sejam responsáveis por destruir organizações e serviços — pois ao se dividir em compartimentos há menores chances de que o sistema todo seja bloqueado ou infectado pelo programa malicioso, sendo usado as camadas como barreiras para frear a inserção do vírus, fazendo com que ele não consiga penetrar, ou mesmo seja detectado pela equipe de segurança digital.

2.2 Proteção de dados e o combate ao ransomware

Uma das pautas mais discutidas quando se entra na questão do ransomware e no ataque aos dados de usuários, é a questão da segurança de informação e de que forma se pode, de forma realmente efetiva, tomar medidas para mitigar os danos e o acesso dos criminosos a esses dados. Isso se torna um problema de grande complexidade quando as redes e códigos inerentes ao funcionamento da tecnologia se demonstram como algo mutável onde novos paradigmas vêm sendo desenvolvidos todos os dias, tanto para a proteção, mas também para o uso malicioso.

O usuário comum que usa seu *notebook*, seu celular, tablet e etc, para realizar seu trabalho, comunicar-se com o mundo, para gerenciar equipamentos, estão cada vez mais eufóricos e encantados com as facilidades que a tecnologia vem trazendo, confiando suas senhas e suas informações pessoais em troca de comodidade, sem a menor noção do risco pelo qual estão correndo com tanta exposição (SABHARWAL; SHARMA, 2019). Porém todos devem se preocupar com os riscos que correm, e frente a isso é necessário que existam de fato maneiras de coibir os danos que podem ocorrer a coletividade pelos ataques maliciosos.

Dessa forma, os pesquisadores de segurança e tecnologia vêm buscando meios de solucionar esses ataques, e ainda prevenir os mesmos, para que haja mais segurança entre os usuários e que a solução seja duradoura, visto que a tecnologia está em constante transformação (MAIGIDA et al, 2019). Consequentemente existem esforços globais que tentam frear o uso malicioso de programas, sendo que muitas vezes os estados oferecem aos criminosos remição na sua pena se o mesmo contribuir para esses esforços.

Assim, com base na análise de dados e de ransomware, é possível concluir que a melhor forma de proteção contra os ataques, para prevenir e dessa forma criar um mecanismo de defesa, é realizar um backup dos artigos regularmente, além de buscar novos avanços tecnológicos que possam trazer mais segurança ao usuário, como desenvolvimento de algoritmos para proteção de dados. Ocorre que isso visa apenas mitigar os danos causados pelos ataques, e não tem um papel prático na hora de evitar os mesmos, mas mesmo assim no atual momento se demonstra como a melhor forma de segurança na rede.

Aliados aos pesquisadores, as autoridades policiais também têm um papel importante na investigação dos ataques, para identificar os responsáveis e auxiliar, assim, o Judiciário na sua punição:[2] "juntas, a academia, as autoridades policiais estaduais e locais, a segurança

[2] É interessante, nesse tocante, observar o que comentam Capaz e Prado (2012) em relação ao art. 6º do Código Penal Brasileiro (BRASIL, 1940). Para os comentadores, se um crime for praticado em território brasileiro e o resultado for produzido no estrangeiro, adota-se a *teoria da ubiquidade*, segundo a qual, em tais casos, o foro competente será tanto o do lugar da ação ou omissão como o do local em que se produziu ou deveria produzir-se o resultado. Assim, o foro competente será o do lugar em que foi praticado o último ato de execução no Brasil (conforme o art. 70, §1º, do Código de Processo Penal Brasileiro) (BRASIL, 1941) ou o local brasileiro onde se produziu o resultado. Já no caso de a conduta e o resultado terem ocorrido dentro do território nacional, mas em locais diferentes, aplica-se a teoria do resultado (art. 70 do Código de Processo Penal), e a competência será determinada pelo lugar em que se consumar a infração ou, no caso de tentativa, pelo local em que for praticado o último ato de execução. Complementa o entendimento acima o formulado por Greco (2017), para quem a teoria da ubiquidade resolve problemas de Direito Penal Internacional, pois não se destina à definição de competência interna, mas sim, à determinação da competência do Judiciário Brasileiro. E, nesse mesmo sentido, Nucci (2016) explica que a posição doutrinária majoritária, no Brasil, vê na norma do art. 6º, CP, uma norma de aplicação da lei penal no espaço quando o crime atingir mais de uma nação. Por essa razão, a teoria da ubiquidade adotada pelo Código Penal é reservada para hipóteses em que delitos se iniciam em país estrangeiro e findou no Brasil (e vice-versa). Com isso se tem resguardada a soberania brasileira para julgar o agente, se a sua conduta criminosa houver ocorrido, em qualquer etapa, em território brasileiro.

privada e as agências reguladoras podem estender melhor a segurança pública no mundo cibernético" (LOSAVIO et al, 2019, p. 215, tradução nossa).[3]

Com a crescente ocorrência desses crimes de sistemas cibernéticos, a cibersegurança se tornou uma questão geral de segurança pública, principalmente com a Internet estando cada vez mais presente em todas as relações, transformando até mesmo a forma como crimes são cometidos (LOSAVIO et al, 2019). Isso demonstra que a preocupação em combater esses crimes mesmo que nova, se torna vital para a manutenção da sociedade, visto que os dados hoje são usados como uma moeda poderosa e vital na atual conjuntura social.

Dessa forma, a polícia precisa estar atenta, e em constante atualização e com profissionais dispostos a dominar os novos conhecimentos necessário para desvendar os crimes cibernéticos, que buscam especializações e se comprometem com uma causa muito maior que é proteger os usuários de mais ataques, punindo criminoso responsáveis para que não ocorram mais ataques do tipo (LOSAVIO et al, 2019). Uma forma para proteger esses dados tão necessários a empresas a usuários, e para que todos possam gozar dos benefícios trazidos pela tecnologia, seria uma pre-detecção dos ataques, conhecer como eles funcionam, de que maneira entram no sistema, para que ocorra uma prevenção eficaz (SABHARWAL; SHARMA, 2019).

Por fim, o que o que cabe ao simples usuário fazer para evitar ataques e proteger sus dados é realizar um backup regular dos dados, utilizar sites confiáveis e buscar sempre manter o software utilizado atualizado, criar um ponto de restauração do sistema, são pequenas formas que são fáceis de implementar e pode salvar os usuários de possíveis ataques. Contudo, o backup precisa ser avaliado e formulado para que possa resolver o problema prontamente, para que dessa forma, se consiga uma resposta mais rapidamente perante um ataque ao sistema, passando por avaliação de sua segurança. "Os sistemas de backup são especialmente importantes porque são a base da recuperação e a última linha de defesa de muitas ameaças críticas" (THOMAS; GALLIGHER, 2018, p.14, tradução nossa).[4]

Cumpre destacar o fato de que os impactos de ataques cibernéticos são de grandes proporções, se tratando de uma empresa, por exemplo, as máquinas deixam de operar, os dados são totalmente impossíveis de acessar, fazendo com que o consumidor não receba o produto da forma desejada e não posso utilizar dos serviços como desejado, o que pode acabar com a boa reputação de muitas empresas prestadoras de bens e serviços, que utilizam certas ferramentas

[3] Texto original: "Together, the academy, state and local law enforcement, private security and regulatory agencies can better extend public safety in the cyber realm".
[4] Texto original: "Backup systems are especially important because they are the foundation for recovery and the last line of defense for many critical threats".

que podem ser atacadas em seu processo de produção ou prestação de serviços (THOMAS et al., 2019).

Nesse contexto, o ataque pode interferir tanto na funcionalidade quanto na organização dos dados, fazendo com que o alcance seja ainda maior, dependendo das características e modo de processamento, e para que seja revertido esse ataque é necessária à utilização de aplicativos empregados manualmente ou automatizados, criados por terceiros (THOMAS et al., 2019).

Por esse motivo se necessita que a sociedade crie maneiras de regular esses crimes, e ter mecanismos de mitigação dos danos e punição de seus culpados, pois como anteriormente exposto, o ataque aos dados podem ocasionar danos reais e comprometer até a integridade física de pessoas que se encontram em hospitais conectados a redes.

3 Crimes digitais e a sua regulação

Com o advento das novas tecnologias que permeiam o mundo, criam-se artificialmente milhões de possibilidades diferentes, e com isso encontram-se condições mais cômodas para a vida dos seres humanos, fazendo com que máquinas e programas hoje realizem atividades complexas que antes eram relegadas apenas aos seres humanos, que faziam isso de forma mais lente e menos eficaz. Essa revolução cibernética se apresentou para a sociedade com um viés de transformação tão profundo, como poucas vezes na história foi vislumbrado pelos seres humanos, que hoje têm uma dependência quase vital da rede e das máquinas virtuais.

Porém como a história pregressa demonstra, sempre que surgem inovações na sociedade, que visam apenas o bem-estar humano, também ocorrem a destruição dessas expectativas, frente à subversão da tecnologia, que pode ser usada para fins maliciosos e gerar inúmeros prejuízos para um grande número de pessoas. Nos tempos antigos os crimes eram essencialmente territoriais, e ocorriam no local em que a pessoa estava localizada, sendo assim, as leis e políticas de repressão foram construídas baseadas nesse pressuposto, incluindo-se também as legislações de países e as condições de soberania de territórios, e de condutas praticadas em sua terra física.

Ocorre que, hoje em dia, as fronteiras se tornaram apenas meros locais de controle para pessoas e seus corpos físicos, pois ao se falar das redes e da tecnologia, essas fronteiras foram derrubadas, existindo a ligação global de todas as nações com o uso da internet e das tecnologias, fator esse que veio para aproximar as culturas e difundir a informação, tornando mais fácil o acesso a pesquisas e notícias, como nunca antes tinha sido visto na história da humanidade. E como em toda grande revolução, hoje interagem socialmente pessoas que

viveram a maior parte de suas vidas sem qualquer acesso a essas novas tecnologias, e que somente agora estão sendo expostas a elas; e também há pessoas que já nasceram inseridas nesse contexto e tem grande facilidade em transitar dentro das redes.

Frente a isso existem indivíduos que com o uso da tecnologia, cometem verdadeiros crimes digitais, e por muitas vezes, beneficiados pela fraca legislação que existe sobre o assunto, conseguem ficar impunes auferindo grandes quantidades de dinheiro, e prejudicando milhares de pessoas com as suas ações. Outro problema é que muitas vezes os delitos têm seu dano causado em uma nação, mas foram cometidos em outra, o que faz com que a captura e julgamento dos culpados seja muito difícil, e muitas vezes impossível, pela dificuldade de cooperação entre nações já conflituosas.

Conforme foi anteriormente tratado, com a ocorrência desses crimes cibernéticos, as nações começaram a entender que isso certamente seria uma tendência que veio a se estabelecer nas novas formas de estabelecimento de relações sociais, e que seria necessário um posicionamento do estado para coibir e controlar o esforço maligno de pessoas nas redes. Muitas deliberações ocorreram, e somente nos dias de hoje é que se pode ver de forma realista que as tentativas de regular o que o ocorre no ambiente digital, e também punir seus infratores, começa a ser de fato efetiva.

Pode ser entendido que esses crimes virtuais, em especial o ransomware, são problemas que têm de ser objeto de apreciação internacional, pois o dano gerado por tais práticas pode ser visto em todos os países do mundo, que contam com uma presença massiva de computadores ligados à *internet*. Visto isso, compreende-se que a regulação é algo de vital importância, pois de fato existem grandes trapaceiros que tem como objetivo retirar dinheiro de pessoas, sempre de forma ilegal, usando de subterfúgios virtuais, como o bloqueio de seus dados, exigindo então por chantagem um resgate em dinheiro, sendo que os casos de ocorrência crescem de forma exponencial em todos os países que foram atacados.

Com esse aumento dos crimes cibernéticos, e de chantagens a empresas e usuários, os pesquisadores e especialistas do meio, trabalham exaustivamente para solucionar os ataques, mas nesse tempo os crimes continuam ocorrendo e os sistemas ficando cada vez mais à mercê de criminosos. Existe já um projeto com 13 diretrizes que funcionariam para prevenção dos ataques, porém trata-se apenas de um conjunto de diretrizes básicas de segurança da internet, não tendo a eficácia necessária (MANJEZI; BOTHA, 2019).

Esse sistema de diretrizes demonstra que os especialistas em segurança cibernética não estão preparados para ataques que estão em constante evolução e acreditam que utilizando diretrizes básicas e antigas conseguiriam controlar a disseminação dos ataques, e ressaltando

ainda o baixo nível de conscientização das empresas da existência de ataques, o que faz com que os esforços de treinamento baseados nas diretrizes básicas não sejam eficazes de fato. Assim se faz necessária uma regulação dos crimes digitais com a positivação de suas condutas como crimes, onde possam ser de fato os infratores punidos com o rigor da lei e com efetividade, para que com isso de fato possa existir mais tranquilidade e segurança dentro do ambiente virtual, e também, que a privacidade seja um bem cada vez mais protegido por todos nessa nova era da exposição.

3.1 Regulação das novas tecnologias nos tempos atuais

A efetiva função do estado como regulador das atividades humanas, muitas vezes se dá de forma lenta frente à evolução da sociedade, que de forma exponencial cria soluções e alternativas tecnológicas para resolver os problemas do mundo, e com isso causa danos com sua inércia, e sua inabilidade de regular a sociedade como ela de fato se encontra na época. Esse sempre foi um problema enfrentado pelos ordenamentos jurídico de vários Estados, porém hoje ele se agrava, pois, a velocidade de mudança se apresenta em proporções nunca antes vivenciadas pelos seres humanos em qualquer época.

Segundo Reins (2019) são amplos os questionamentos que surgem quando se trata de um sistema jurídico com normas atualizadas e prontas para as novidades que vem surgindo, com o crescimento constante da tecnologia, esses questionamentos servem para analisar se a o sistema jurídico atual pode se adequar e ser aplicado para as novas formas de comercio de bens e serviços, assim como a novas moedas, ou se será necessárias novas normas.

Contudo o que se questiona é de que forma o atual direito civil e contratual não seria aplicável, se este estaria desatualizado perante a mudança, se o que atualmente existe não é o suficiente para suprir as mudanças da inovação tecnológica (LEENES, 2019, p.11). Assim, frente a perspectivas históricas, o direito normalmente anda a passos lentos frente a mudanças da sociedade, e nesse caso não seria diferente, demonstrando que existe uma grande necessidade de mudar esse fator, tornando a positivação mais célere conforme os pressupostos tecnológicos mudam de forma cada vez mais agressiva.

O crescente aumento no setor de segurança da informação reflete o grave teor dessa ameaça criminosa cibernética no âmbito global, o que resulta em altos custos para a economia mundial. Ainda, as pesquisas sobre como os crimes cibernéticos tem se desenvolvidos estão atrasadas pela dificuldade de compreender o avanço desses ataques. (SCHIRRMACHER, 2018). Dessa forma, para que se diminua os prejuízos causados, é necessária uma maior

investigação relacionada a segurança de informação por agentes capacitados. Para que se possa compreender e assim seja possível antecipar aos ataques cibernéticos, os estudiosos e pesquisadores precisam buscar quais os recursos que são utilizados por esses criminosos para realização dos ataques. Ainda, a origem criminosa dos valores arrecadados pelos cibercriminosos faz com que os mesmos não tenham que pagar impostos, saindo em vantagem econômica e fazendo com que possam investir seus lucros em novos ataques, gerando cada vez mais riqueza para os agentes, que podem investir em novas formas de atividades cibercriminosas.

É importante ressaltar que esses valores, e sendo esse um fator ainda mais complexo para atribuir autoria a esses crimes, nunca são direcionados para contas usuais em bancos tradicionais, pois essas contas pertencem a alguém, o que faria o combate aos crimes ser uma atividade muito tranquila. Os valores normalmente são requisitados por meio de *bitcoins*, que são ferramentas legítimas, mas que tem um forte viés de anonimato e privacidade. Ocorre que as chamadas ciber-moedas acabaram por se tornar ferramentas utilizadas no mercado de bens e serviços ilícitos, servindo como uma moeda de troca comum, no mercado ilegal. Dessa forma, as plataformas disponíveis para troca de mercadorias ilícitas, possibilitam que seus clientes utilizem as criptomoedas com intuito de adquirir substâncias entorpecentes, armas, entre outros itens não permitidos pela legislação (IRWIN; DAWSON, 2019).

Além disso, outro caso frequente é que muitos praticam o cibercrime fazendo uso de ferramentas de *hackers*, tais como o *malware*, para identificar os dados bancários dos usuários, como cartão de crédito e senhas, fazendo combinações e utilizando para chantagear os mesmos, cobrando certa quantia em troca da devolução dos dados, a ser paga em *bitcoins*. Assim se cria um gigantesco mercado, que legitima e fortalece o uso das criptomoedas, porém, quando faz isso de forma ilegal faz com que esse tipo de moeda seja mal vista pelos governos e instituições financeiras do globo. A melhor forma de buscar solucionar esses ataques seria buscar investigar o ransomware, para que possam, de alguma forma, auxiliar as agências policiais a identificar quem são os criminosos que estão utilizando das criptomoedas para realizar ou facilitar ataques e uso de dados ilegais (IRWIN; DAWSON, 2019).

Diversos são os desafios enfrentados a partir do aparecimento do Bitcoin e entre outras criptomoedas, desafios esses que de fato tornam extremamente complexo a determinação de quem são esses ofensores e dessa forma, conseguir diminuir a larga escala desses ataques, o que é imprescindível para a segurança dos usuários. O que se criou foi uma escala em direção a ilicitude, onde, com a movimentação de quantidades gigantescas de capital, as instituições se

dobram frente ao poder econômico, sendo isso um fator impeditivo e que muitas vezes faz as investigações e tentativas de regulação andarem a passos lentos.

As regulações são bastante necessárias, só que elas precisam ser viáveis economicamente, pois em um mundo onde o capital de fato comanda praticamente todas as decisões, quando ele é atacado normalmente sai vitorioso em sua tentativa de se restabelecer. Então, após vários esforços dispensados em torno de implementar regulamentos para a indústria de criptomoedas, se percebeu que se tornava muito caro onde foi introduzindo, criando maiores dificuldades de implementação, com um desequilíbrio entre o custo, tornando caro demais para funcionar. Assim, as criptomoedas ainda são antros de inúmeras fraudes e local do pagamento de resgate dos ransomwares, com pouca efetividade no tocante a regulação das mesmas e tentativa de identificar os agentes causadores do mal.

Para vencer a guerra contra-ataques cibernéticos é preciso avaliar todos os recursos utilizados pelos agentes criminosos, alcançado uma estratégia favorável para um futuro próximo, para uma maior proteção dos estados e privada, superando as dificuldades encontradas como natureza de dados e etc. (SCHIRRMACHER, 2018). Porém para isso precisa-se que existam políticas reguladoras próprias para lidar com esses ataques, primeiramente tentando causar danos no recebimento de dinheiro conseguido com os ilícitos, sendo esse o caminho que de fato poderá coibir a prática de forma efetiva e real.

3.2 Ransomware e regulação da prática do ilícito

O ransomware, como devidamente explicado na parte introdutória do presente trabalho, se apresenta nada mais do que como uma chantagem intencional feita por intermédio de computadores, e que visa bloquear dados de pessoas físicas ou jurídicas com a intenção de pedir resgate pelos mesmos, o que caso contrário não ocorra, culminaria com a exclusão de todos os dados de forma permanente. Porém atualmente se está no limiar das regulações efetivas, e diversos empecilhos são encontrados para a efetiva e devida punição dos crimes relacionados ao ransomware.

Existe ainda, uma grande dificuldade em estabelecer normas e regulamentos para desvendar e punir esses crimes, e mais ainda ao executar a lei, identificando os usuários que estão utilizando somente para atividades ilícitas e separando os que utilizam para atividades diversas desse fim. (IRWIN; DAWSON, 2019). Como exposto anteriormente, uma das maneiras desse negócio ilegal ser realmente viável é por meio das criptomoedas, sendo seu uso amplamente difundido no meio do ransomware como principal forma de cobrança dos resgates.

Ainda, cabe ressaltar que o uso do *bitcoin* como moeda será cada vem mais semelhante ao uso da moeda fiduciária utilizada tradicionalmente ao redor do mundo. "Isso ocorre porque o Bitcoin tem um valor que é transferível para moeda fiduciária e é utilizado da mesma maneira quando se trata de comprar bens e serviços" (IRWIN; DAWSON, 2019, p. 18, tradução nossa).[5]

Esse fator é muito importante para entender o porquê dos ataques serem economicamente possíveis, e acontecerem com uma grande frequência, pois, ao se demonstrarem satisfatórias na aquisição de capital, atraem cada vez mais pessoas, que não tem dificuldades em transformar o *bitcoin* em moeda oficial. Esse é um dos principais fatores que levam os criminosos a investir em inovações frente a essas tecnologias para sempre estarem a um passo a frente das leis e regulações.

Portanto, é indispensável a regulamentação para garantir que transações que possam ser consideradas de risco, imediatamente sejam visíveis para que o usuário tenha tempo suficiente para identificar o indivíduo responsável pela atividade, e ainda, que o mesmo recurso esteja disponível para os usuários padrão e também para a polícia, que por sua vez pode encontrar os usuários que praticam atividades ilícitas, investigá-los e processá-los.

Ocorre que isso se torna um problema que afeta diretamente o conceito pelos quais as moedas cripo estão fundados, sendo o cerne de sua atividade e fundamentação, que é o conceito de ser uma moeda anárquica que não necessita do estado, e que preza pela privacidade total. Assim existe um paradoxo entre o real posicionamento, inclusive político dessas moedas, com a necessidade de regulação do estado para coibir crimes, criando assim um problema, pois sem regulação as infrações nunca vão parar de ser cometidas, porém, com a regulação, o espírito e função das criptomoedas perdem seu real valor e efetividade. Porém, ao se colocar a questão em análise, tem-se de entender que a regulação se faz necessária, e que essa é a única forma de coibir os danos causados pelos ataques, sendo então preciso que existam maneiras de aliar a questão da privacidade com a questão do poder efetivo de buscar soluções para crimes.

A preocupação em estabelecer um sistema de identificação de *bitcon* e outras cibermoedas, e em fazer com que esse sistema funcione efetivamente, precisa ser global, estabelecida a partir da cooperação entre todos os países — até porque o *bitcon* é transnacional, não regulada por ordenamentos contidos em fronteiras. Assim, com a regulamentação em todos os países e jurisdições, o sistema terá completa eficácia, com a uma maior probabilidade de punição aos responsáveis e redução de crimes. Do contrário, os crimes de uso indevido de *bitcon* e cibermoedas simplesmente se concentraram em jurisdições que não contemplam a

[5] Texto original: "this is because Bitcoin has value that is transferable to fiat currency, and is utilised in much the same way when it comes to purchasing goods and services".

regulamentação. Esse sistema seria formado de três pontos principais, sendo esses a consistência, a clareza, o, e o custo benefício na implementação, elementos que serão essenciais em qualquer sistema visando barrar cibercrimes e buscar uma maior segurança para os usuários. Dessa forma, a atenção encontra-se voltada para solucionar as dificuldades em estabelecer e implementar um sistema eficaz e global para combater as cibermoedas e crimes relacionados a lavagem de dinheiro e terrorismo, financiados por meio de Bitcoin e os usuários. Para que assim, seja possível concretizar uma cooperação necessária para o combate dessa indústria de crimes.

Ainda é de se considerar a disparidade entre as sociedades, em que muitas trabalham com diferentes formas de controle de mercadorias, bens e serviços, enquanto outras tendem a manter certo equilíbrio, como as sociedades democráticas, que buscam diferentes objetivos sociais, com uma regulamentação diversa das demais no que concerne ao uso da tecnologia (REINS, 2019). A humanidade em constante evolução sempre buscará por melhorias na tecnologia e isso é algo que deve ser já tratado como uma realidade sem volta, pois o progresso tende a tentar sanar os problemas da sociedade. Ocorre que a regulamentação dessas tecnologias precisa passar por um exercício a favor de ponderar e equilibrar os objetivos e interesses sociais conflitantes, para conseguir construir estruturas viáveis e que possam de fato serem cumpridas. Desse modo, na realidade não há uma forma ideal de regulamentação para todos os tipos de tecnologias que possa abranger toda a sociedade, e sim a busca deve ser para encontrar uma regulamentação que possa ser abordada por cada ordenamento jurídico, com toda sua especificidade, buscando os interesses globais, mas atendendo as necessidades locais. “Os processos regulatórios das novas tecnologias sejam capazes de capturar essas preferências — muitas vezes concorrentes — sem, ao mesmo tempo, sufocar a inovação no processo. Isso é ainda mais crucial nos tempos incertos em que estamos atualmente” (REINS, 2019, p. 313 tradução nossa).[6]

O desenvolvimento tecnológico vem aumentando da mesma forma que o mundo vem enfrentando graves problemas geopolíticos, transformações climáticas e um crescimento exponencial no fluxo da migração, desafios enfrentados diretamente pela sociedade, que estão dependentes de regulamentação (REINS, 2019). Por diversas vezes a regulamentação é essencial para proteger o ser humano das transformações tecnológicas que possam causar algum prejuízo à população, dessa forma, uma estrutura regulamentar que funcione de maneira eficaz

[6] Texto original: “The regulatory processes for new technologies are capable of capturing these — often competing — preferences, without — at the same time — stifling innovation in the process.This is all the more crucial in the uncertain times that we are currently”.

se faz essencial para que esse desenvolvimento aconteça de forma lícita, sempre buscando o melhor para a sociedade.

Com isso, pode-se vislumbrar um futuro deveras incerto, pois as condições de regulação para os ataques cibernéticos se baseiam em uma cooperação internacional que muitas vezes é inexistente, e perpassa a questão da privacidade da regulação das criptomoedas. Assim, enquanto não existirem políticas reais com a intenção de punir os criminosos, eles continuarão atuando, pois existem grandes potenciais de lucro nessa atividade, e pouco risco de sofrerem sanções, comparados a outros tipos de crimes mais tradicionais.

Conclusão

Assim como a tecnologia se aprimora, ocorre o mesmo com os crimes que são inerentes a elas, que também estão em constante evolução e aprimoramento. O ransomware é um grande problema, nesse sentido, pois os dados são atualmente tão valiosos quanto a moeda real, sendo que seu uso tem o poder de influenciar mercados, eleições e vidas humanas de uma forma muito profunda. Então, seu sequestro mediante paga de resgate restringe o seu uso pelo legítimo dono.

Muitas empresas que são atacadas não hesitam, assim, em fornecer o pagamento solicitado, pois a perda dos dados que estão em jogo as levaria a prejuízos muito maiores do que o resgate requisitado por eles. Isso cria uma gigantesca relação de dependência com o criminoso, que tem em seu poder os dados e certamente pode com uma simples ação, apagar ou criptografar para sempre toda informação, gerando muito dano as vítimas. Porém, o ransomware também é direcionado a indivíduos, que também sofrem esses ataques, e muitas vezes cedem à chantagem, para não perder algum dado importante que tenha em seu sistema. Essa é, de fato, uma das desvantagens do avanço tecnológico, que se demonstra danoso nesses casos concretos, aumentando a sensação de insegurança populacional frente ao arquivamento de seus dados na rede.

O que se demonstra necessário para, pelo menos, mitigar a ocorrência de tal prática maliciosa é a cooperação entre empresas, cidadãos e Estados, para que os ataques sejam cada vez menos frequentes e eficazes, e os criminosos possam ser identificados e punidos. Essa identificação muitas vezes carece de eficácia pelo fato de que esse crime não se atém às fronteiras territoriais estatais, sendo praticado em qualquer lugar, com o alvo estando muitas vezes países ou continentes distantes.

Outro fator importante, é que a maioria dos pagamentos de resgate feitos para os criminosos, não se demonstra em moeda corrente, em bancos tradicionais e operações

financeiras comuns, mas sim nas criptomoedas, oriundas de um projeto de distanciamento entre economia e Estado a fim de se configurar um modelo sigiloso de movimentação de capital. Isso faz com que seja muito complexo rastrear o caminho que esses valores trilham para chegar até o criminoso, fazendo com que sua punição seja quase inexistente.

Em razão de todos os argumentos acima apresentados, foi parcialmente confirmada a hipótese de que a tecnologia pode, concomitantemente, gerar a melhora das condições sociais humanas (melhorias nas formas de comunicação, de produção, de relações econômicas em geral, dentre outras não contempladas neste trabalho, tais como novas formas de cura, de aquisição cultural, etc.), e malefícios quando usada para fins ilícitos — como a chantagem online mediante o pagamento de resgate (*ransomware*). Essa prática, assim, pode ser reconhecida como um malefício atinente ao desenvolvimento tecnológico, que se vale de ótimas promessas atendidas pelo desenvolvimento tecnológico (comunicações transfronteiriças rápidas e relativamente baratas, criptomoedas que não necessitam da burocrática centralização estatal para funcionar, manutenção da privacidade em meios online, dentre outras) para causar prejuízos a empresas e a pessoas físicas mediante extorsão. Como vários aspectos dessa prática fogem ao domínio estatal nacional (por se darem em ambientes muito mais voláteis e abrangentes do que os limites politicamente estabelecidos pela soberania estatal), tem-se que uma regulação em ambiente internacional é necessária para se conter práticas nocivas realizadas pela internet. Contudo, para além de tratados e outras formas de convenção estabelecidas pelos Estados, outras formas de regulação — tais como medidas técnicas atinentes ao próprio fluxo de pagamentos por criptomoedas, que de alguma forma venham a impedi-los quando referentes a crimes — devem ser estudadas e propostas.

Referências

ABRAMS, Lawrence. DoppelPaymer ransomware sells victims' data on darknet if not paid. **Bleeping Computer**, [s. l.], 3 fevereiro 2020. Disponível em: https://www.bleepingcomputer.com/news/security/doppelpaymer-ransomware-sells-victims-data-on-darknet-if-not-paid/. Acesso em: 02 mar 2020.

AKAY, Meltem. **Detecting cryptographic ransomware by examining file system activity**. 2019. Tese (Mestrado em Engenharia de Cibersegurança) — Graduate School of Natural and Applied Sciences, Seri University, Istanbul, 2019. Disponível em: http://earsiv.sehir.edu.tr:8080/xmlui/handle/11498/56626. Acesso em: 28 mar 2020.

AKHILESH, K. B. Smart Technologies—Scope and Applications. In: AKHILESH, K. B; MÖLLER, Dietmar P. F. (eds.). **Smart Technologies**. Singapore: Springer, 2020, p. 1-16.

ATAPOUR-ABARGHOUEI, Amir; BONNER, Stephen; MCGOUGH, Andrew Stephen. Volenti non fit injuria: Ransomware and its Victims. **arXi.org**, p. 1-7, 2019. Disponível em: https://arxiv.org/abs/1911.08364. Acesso em: 28 mar 2020.

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940.** Código Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 28 mar 2020.

BRASIL. **Decreto-Lei nº 3.689, de 3 de outubro de 1941.** Código de Processo Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 28 mar 2020.

BRILL, Alan; THOMPSON, Eric. Ransomware: Believe the Risk and Be Ready for It. **Corporate Compliance Insights**, 2019. Disponível em: https://ssrn.com/abstract=3464842. Acesso em: 28 mar 2020.

CAPEZ, Fernando; PRADO, Stela. **Código Penal Comentado.** 3 ed. São Paulo: Saraiva, 2012.

CARTWRIGHT, Anna; CARTWRIGHT, Edward. Ransomware and reputation. **Games**, v. 10, n. 2, p. 26-40, 2019. DOI: https://doi.org/10.3390/g10020026.

CONNOLLY, Lena Y.; WALL, David S. The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. **Computers & Security**, v. 87, p. 1-18, 2019. DOI: https://doi.org/10.1016/j.cose.2019.101568.

EICHENSEHR, Kristen. The Law & Politics of Cyberattack Attribution. **UCLA Law Review**, v. 67, p. 1-63, 2020. Disponível em: https://ssrn.com/abstract=3453804. Acesso em: 28 mar 2020.

FERREIRA, Márcio Ricardo; KAWAKAMI, Cynthia. Ransomware-Kidnapping personal data for ransom and the information as hostage. **ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal**, v. 7, n. 3, p. 5-14, 2018. DOI: http://dx.doi.org/10.14201/ADCAIJ201873514.

GRECO, Rogério. **Código Penal Comentado**. 11 ed. Niterói: Editora Impetus, 2017.

HASSAN, Nihad A. Endpoint Defense Strategies. In: HASSAN, Nihad A. **Ransomware Revealed**. Berkeley: Apress, 2019, p. 71-114.

IRWIN, Angela S.M.; DAWSON, Caitlin. Following the cyber money trail: global challenges when investigating ransomware attacks and how regulation can help. **Journal of money laundering control**, v. 22, n. 1, p. 110-131, 2019. DOI: https://doi.org/10.1108/JMLC-08-2017-0041.

LEENES, Ronald. Regulating New Technologies in Times of Change In: REINS, Leonie (ed.). **Regulating new technologies in uncertain times**. The Hague: T. M. C. Asser Press, 2019, p. 3-18.

LISKA, Allan; GALLO, Timothy. **Ransomware:** Defending against digital extortion. Sebastopol: O'Reilly Media, 2016.

LOSAVIO, Michael et al. STEM for Public Safety in Cyber: Training for Local Law Enforcement and Cyber Security. In: IEEE. **2019 IEEE Integrated STEM Education Conference (ISEC).** Princeton: IEEE, 2019, p. 215-221.

MAIGIDA, Abdullahi Mohammed et al. Systematic literature review and metadata analysis of ransomware attacks and detection mechanisms. **Journal of Reliable Intelligent Environments**, v. 5, n. 2, p. 67-89, 2019. DOI: https://doi.org/10.1007/s40860-019-00080-3.

MANJEZI, Zandile; BOTHA, Reinhardt A. Preventing and Mitigating Ransomware. In: VENTER, H.; LOOCK, M.; COETZEE, M.; ELOFF, M.; ELOFF, J. (eds.). **Information Security. ISSA 2018. Communications in Computer and Information Science**, v. 973. Cham: Springer, 2019, p. 149-162.

NUCCI, Guilherme de Souza. **Código de Processo Penal Comentado**. 15 ed. Rio de Janeiro: Forense, 2016.

O'KANE, Philip; SEZER, Sakir; CARLIN, Domhnall. Evolution of ransomware. **IET Networks**, v. 7, n. 5, p. 321-327, 2018. DOI: 10.1049/iet-net.2017.0207.

PAQUET-CLOUSTON, Masarah; HASLHOFER, Bernhard; DUPONT, Benoit. Ransomware payments in the bitcoin ecosystem. **Journal of Cybersecurity**, v. 5, n. 1, p. 1-11, 2019. DOI: 10.1093/cybsec/tyz003

PRASAD, Ramjee; ROHOKALE, Vandana. **Cyber Security:** The Lifeline of Information and Communication Technology. Springer, 2020.

REINS, Leonie. Regulating New Technologies in Uncertain Times — Challenges and Opportunities In: REINS, Leonie (ed.). **Regulating new technologies in uncertain times**. The Hague: T. M. C. Asser Press, 2019, p. 19-29.

SABHARWAL, Simran; SHARMA, Shilpi. Ransomware Attack: India Issues Red Alert. In: MANDAL, Jyotsna Kumar; BHATTACHARYA, Debika (eds.). **Emerging Technology in Modelling and Graphics**. Singapore: Springer, 2020, p. 471-484.

SCHIRRMACHER, Nina-Birte; ONDRUS, Jan; TER CHIAN FELIX TAN. Towards a Response to Ransomware: Examining Digital Capabilities of the WannaCry Attack. In: **Pacific Asia Conference on Information Systems (PACIS) 2018 Proceedings**, 2018, p. 210-217. Disponível em: https://aisel.aisnet.org/pacis2018/210. Acesso em: 28 mar 2020.

SIMOIU, Camelia et al. "I was told to buy a software or lose my computer. I ignored it": A study of ransomware. In: **Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)**, [s. l.], 2019. Disponível em: https://www.usenix.org/conference/soups2019/presentation/simoiu. Acesso em: 28 mar 2020.

SLAYTON, Thomas B. Ransomware: The Virus Attacking the Healthcare Industry. **Journal of Legal Medicine**, v. 38, n. 2, p. 287-311, 2018. DOI: https://doi.org/10.1080/01947648.2018.1473186.

THOMAS, Jason; GALLIGHER, Ryan P.; THOMAS, Macalah L., GALLIGHER, Gordon. Enterprise Cybersecurity: Investigating and Detecting Ransomware Infections Using Digital Forensic Techniques. **Computer and Information Science**, v. 12, n. 3, p. 72-80, 2019. DOI:10.5539/cisv12n3p72.

THOMAS, Jason; GALLIGHER, Gordon. Improving backup system evaluations in information security risk assessments to combat ransomware. **Computer and Information Science**, v. 11, n. 1, p. 1-11, 2018. Disponível em: https://ssrn.com/abstract=3095629. Acesso em: 28 mar 2020.

WIRTH, Axel; GRIMES, Stephen L. Medical device cybersecurity — At the convergence of CE and IT. In: IADANZA, Ernesto (ed.). **Clinical Engineering Handbook**. Academic Press, 2020, p. 253-258.