Aspectos Jurídicos no Combate e Prevenção ao *Ransomware*

Fábio Lucena de Araújo*

Sumário

Resumo

A evolução tecnológica fez surgir novos crimes cibernéticos, entre eles, o ataque por *ransomware*. Prática cada vez mais recorrente, onde o criminoso, através de criptografia, impossibilita o acesso à máquina infectada, cobrando um valor em dinheiro (geralmente em moeda virtual) para liberar o acesso ao usuário. Nesse contexto, o presente artigo tem como objetivo analisar a prevenção e a atuação da polícia judiciária no combate ao *ransomware*, discorrendo sobre seus limites jurídicos e observando os mecanismos de cooperação internacional, utilizando-se da pesquisa bibliográfica, bem como da exegese dos diplomas legais.

Abstract

Technological evolution has given rise to new cyber crimes, including the ransomware attack. Increasingly recurring practice, where the criminal through encryption, makes it impossible to access the infected machine, charging a cash value (usually in virtual currency) to release access to the user. In this context, this article aims to analyze the prevention and action of the judicial police in the fight against "ransomware", discussing its legal limits and observing the mechanisms of international cooperation, using bibliographical research, as well as the exegesis of legal diplomas.

Palavras-chave: Aspectos jurídicos. Combate e prevenção. *Ransomware*.

Keywords: *Legal aspects. Combat and prevention. Ransomware.*

* Graduado em Direito pela Universidade Estácio de Sá (UNESA). Tecnólogo em Gravação e Produção Fonográfica pela Universidade Estácio de Sá (UNESA). Advogado.

1. Introdução

O acesso às novas tecnologias em um mundo cada vez mais conectado tem garantido diversos avanços nas relações sociais e econômicas. Entretanto, toda essa tecnologia também pode ser utilizada para a prática de crimes. Os crimes cibernéticos são uma realidade, várias espécies de crimes se originaram e outros já conhecidos ganharam uma nova roupagem diante do avanço tecnológico.

Nesse artigo, trataremos do tema *ransomware*, chamado popularmente de *sequestro digital* ou *sequestro de dados*. Em síntese, trata-se de uma espécie de vírus de computador, em que o cibercriminoso, após conseguir infectar a máquina desejada através de criptografia, impossibilita o acesso à máquina já infectada, cobrando um valor em dinheiro (geralmente em moeda virtual) para liberar o acesso ao usuário.

É de especial relevância o estudo do tema, tendo em vista os prejuízos políticos, econômicos e sociais oriundos de um ataque virtual nesse sentido. O mundo tem assistido, ultimamente, a uma ameaça crescente desses ataques, o que nos leva a um questionamento imediato. A legislação pátria e as ferramentas de informação são eficientes na prevenção e combate ao *ransomware*?

Nessa esteira, busca-se, com o presente artigo, dissecar o tema, analisando a prevenção e a investigação da polícia judiciária no combate ao *ransomware*, discorrendo sobre seus limites jurídicos e observando os mecanismos de cooperação internacional, bem como na especial exegese da Lei nº 12.737, de 30 de novembro de 2012.

Os ataques dos cibercriminosos têm se expandido dos usuários particulares para as grandes corporações e até mesmo governos. Através de diversas táticas, eles têm conseguido grande percentual de sucesso, gerando lucros exorbitantes para essas organizações criminosas. Por consequência, essas ações geram graves reflexos nos campos social, econômico e governamental.

Indubitável a necessidade de uma análise criteriosa sobre o tema, discorrendo sobre a legislação pertinente e a cooperação internacional na busca da prevenção e combate a essa ameaça que põe em risco o mundo inteiro em ataques cada vez mais danosos.

2. *Ransomware*

Chamado comumente de *ransomware*, este vírus faz parte de uma classe específica de *malwares*[1] que é utilizada nas chamadas *extorsões digitais*, pois obriga suas vítimas a pagarem determinado valor em troca do completo controle de seus dados. Essencialmente, existem duas classes: a *Locker*, que impede que a vítima acesse o equipamento infectado, praticamente inutilizando-o, e a *Crypto*, que bloqueia o acesso aos dados armazenados no equipamento infectado, utilizando criptografia.

[1] *Malware* – É a combinação das palavras inglesas *malicious* e *software*, ou seja, programas maliciosos. São programas e comandos feitos para diferentes propósitos: apenas infiltrar um computador ou sistema, causar danos e apagar dados, roubar informações, divulgar serviços etc.

Sua origem tem início em 1989, com o nome de *AIDS*, criado por Joseph L. Popp, um biólogo com PhD em Harvard. Na época, bem menos danoso do que o próprio vírus cujo nome se originou. Este *malware* mantinha, em seus ataques, uma contagem específica de reinicializações do sistema para, posteriormente, ocultar todos os diretórios. Entretanto, por conter uma criptografia básica, ele era facilmente removido.

Após um breve período de hibernação, em meados da década de 2000, diante dos novos avanços tecnológicos, da capacidade cada vez maior de processamento dos computadores e diante de formas mais complexas de criptografia, voltaram a aparecer ataques cada vez mais elaborados e diversas variantes de *ransomware*.

Hodiernamente, estes ataques têm se tornado cada vez mais frequentes e tendo como vítimas não só o usuário particular, mas também pessoas jurídicas de direito privado e de direito público. Os cibercriminosos têm expressivo sucesso nesses ataques, conseguindo quantias vultosas, chegando ao ponto de terceirizar seus vírus na *deep web*[2], no serviço chamado de *RaaS – Ransomware as a Service*, ou seja: *Ransomware* como um serviço, cobrando um percentual sobre os ataques bem-sucedidos. Essas empreitadas se espalham tanto pelos computadores pessoais, bem como para os das grandes corporações, seus servidores e até os dispositivos móveis.

Em maio deste ano (2017), o mundo presenciou um dos maiores ataques cibernéticos, o vírus chamado *WannaCry* afetou mais de 150 países, fazendo aproximadamente 200.000 vítimas[3]. A maioria dos ataques foi contra empresas, acendendo uma luz de alerta ao mundo sobre a vulnerabilidade dos nossos sistemas. Torna-se deveras preocupante a quantidade de dados confidenciais aos quais estas organizações criminosas conseguiram ter acesso. E este é apenas um dos milhares de *malwares* espalhados pela rede.

3. Dinâmica dos Ataques

A análise sistemática dos ataques cibernéticos é de extrema importância para o desenvolvimento de mecanismos de defesa, bem como para o aperfeiçoamento legislativo no sentido de combater tais práticas. Percebe-se que o comportamento dos criminosos tende a mudar de acordo com o alvo escolhido. Existem ataques mais simples e outros mais complexos, estes ocorrem quando existe um alvo específico, seja pessoa física, pessoa jurídica de direito privado ou até mesmo de direito público. As abordagens se desenvolvem de diversas formas, seja explorando as falhas dos sistemas ou também por meio de engenharia social, explorando as nossas vulnerabilidades sociais. Diante do exposto, trataremos tais etapas como: Implantação; Instalação; Comando e Controle; Destruição e Extorsão, conforme classificação elencada por Allan Liska e Timothy Gallo.[4]

---

[2] *Deep Web* – É o nome dado para uma zona da internet que não pode ser detectada facilmente pelos tradicionais motores de busca, garantindo, *em tese,* privacidade e anonimato para os seus navegantes.

[3] CEBRIÁN, Belén Dominguez. *Cibertaque*: o vírus *WannaCry* e a ameaça de uma nova onda de infecções. *El País*. Madri. 15 mai. 2017. Disponível em: <http://brasil.elpais.com/brasil/2017/05/14/internacional/1494758068_707857.html>. Acesso em: 20 mai. 2017.

[4] *Cf.* LISKA, Allan; GALLO, Timothy. Ransomware *(Defendendo-se da Extorsão Digital)*. 1ª ed. São Paulo: Novatec Editora Ltda., 2017. p.19.

3.1. A Implantação do *Malware*

Num primeiro momento, há necessidade de o cibercriminoso ter acesso à máquina-alvo, com o fito de adicionar as partes integrantes do *malware*. Diante dessa etapa, eles se utilizam dos chamados *download drive-by*[5]. Exemplificando: ao visitar páginas da internet já infectadas e aproveitando-se das falhas de segurança da máquina-alvo, quando o usuário final acessa um desses *sites*, *downloads* automáticos são efetuados pela máquina sem que este usuário perceba. Diante de diversas técnicas, os componentes do *malware* são instalados sem que o antivírus da máquina perceba. Outra forma de ataque complexo é o *watering hole attack*[6]. Esse procedimento consiste na busca de diversas informações coletadas sobre a vítima, como os *sites* que ela visita, as permissões que ela tem de autorizar em sua navegação, os aplicativos necessários para acessar determinado local, os tipos de *e-mails* que podem ser trocados, entre outras formas. Assim, os cibercriminosos podem executar um ataque específico. Trata-se de um ataque personalizado.

3.2. A Instalação do *Malware*

Diante de um ataque bem-sucedido, o qual pode ter se efetivado pelas diversas ferramentas utilizadas para esse propósito, uma parte do *malware* acessa a máquina. Nesse momento inicial, o programa é executado no sentido de fazer o *download* do *ransomware* completo. Após esse estágio, ocorrerá uma gradativa dependência da máquina em relação ao criminoso, o qual passa, literalmente, a "varrer" a máquina na busca de suas principais diretrizes de comando. Essa conexão entre criminoso e máquina infectada passa a trazer diversos riscos, não só para essa máquina, mas para toda a estrutura à qual eventualmente ela esteja conectada.

As palavras de Allan Liska e Timothy Gallo[7] são cristalinas em definir esta etapa:

> Em um ataque com alvo específico, as técnicas para instalar, ofuscar, compactar o código e explorar falhas podem ser mais nefastas na tentativa de maximizar o resgate (*ransom*). O *ransomware* pode usar essa instalação inicial para se espalhar lentamente pela rede afetada, instalando-se em vários sistemas e abrindo compartilhamentos de arquivos que, por sua vez, serão simultaneamente criptografados quando instruções forem enviadas na próxima fase.

Após essa varredura, o vírus passará a desabilitar todo e qualquer procedimento que venha permitir que o usuário o acione para tentar reverter a situação atual, como

[5] Qualquer *download* que acontece sem o conhecimento da pessoa, geralmente um vírus de computador, um *spyware* ou um *malware*.

[6] Temos diversas analogias esquisitas no mundo da informática, *Watering Hole Attack* é mais uma delas. Nesse caso *Watering Hole* seria uma analogia a uma fonte d´água na África, onde os animais param para beber água e ficam vulneráveis aos predadores que ficam à espreita, no aguardo de uma presa fácil.

[7] *Cf.* LISKA, Allan; GALLO, Timothy. Ransomware *(Defendendo-se da Extorsão Digital)*. 1ª ed. São Paulo: Novatec Editora Ltda., 2017. p.22.

funcionalidades padrão, recuperação do sistema, *logins* e antivírus. Vencida esta etapa, haverá a necessidade de se estabelecer uma nova troca de informações entre criminoso e máquina infectada para o comando e controle.

3.3. O Controle da Máquina

A partir da execução, o vírus passará a buscar na máquina diversas informações importantes, como sistemas instalados, protocolo de internet (IP), tipos de antivírus, navegadores, entre outras informações, para ter a ciência se a máquina infectada é realmente importante para os criminosos ou não, continuando, assim, com as outras fases do ataque.

3.4. Destruição de Dados e "Extorsão" das Vítimas

De posse de tais informações, os arquivos serão criptografados ou bloqueados, tendo em vista que estes já foram identificados pela fase anterior. Normalmente, os arquivos mais procurados são os arquivos de texto, planilhas, arquivos de programas de imagens, de áudio e vídeo. Exemplo de extensões desses arquivos: *pdf, mp3, rtf, txt, bmp, zip, jpg, xls, exe, ppt, gif, docx, avi, html, mpeg*, *avi, jpeg,* entre outros.

O processo de criptografia destes arquivos utiliza chaves simétricas ou assimétricas, as quais movem e embaralham estes arquivos. Entretanto, diante do rápido desenvolvimento desses vírus, os ataques têm, cada vez mais, utilizado as duas técnicas. A chave simétrica é uma chave única que serve para criptografar, bem como para descriptografar os dados da máquina. Em sua funcionalidade, ela usa menos recursos do sistema da máquina infectada, podendo criptografar de forma mais rápida, mesmo quando o computador estiver *offline*. Entretanto, o criminoso somente terá as informações sobre a conclusão do ataque quando a máquina se reconectar à internet. É também chamada de *criptografia de chave secreta*.

Quanto à chave assimétrica, esta traz uma criptografia mais complexa, tendo o invasor uma chave pública que serve para criptografar os arquivos e uma chave privada, que será usada no processo de descriptografia. A criptografia assimétrica necessita de maior processamento da máquina, mas garante maior segurança no ataque, uma vez que apenas a chave pública transita entre o criminoso e a máquina-vítima. Após esta etapa, a vítima terá seu acesso limitado ou não terá nenhum acesso ao computador, o qual apresentará uma tela com instruções para o pagamento do resgate de seus dados.

O pedido de pagamento ocorre nesse momento: diante da máquina infectada, a vítima não terá acesso aos seus dados e será compelida a pagar um valor, que aumentará com o passar do tempo, dependendo do tipo de ataque. Um usuário particular não é tão importante para os cibercriminosos quanto governos ou grandes corporações. Normalmente, os valores são cobrados em moeda virtual (geralmente o *bitcoin*[8]).

[8] *Bitcoin* é uma tecnologia digital que permite reproduzir em pagamentos eletrônicos a eficiência dos pagamentos com cédulas descritas acima. Pagamentos com *bitcoins* são rápidos, baratos e sem intermediários. Além disso, eles podem ser feitos para qualquer pessoa que esteja em qualquer lugar do planeta, sem limite mínimo ou máximo de valor.

A partir de uma infecção, pagar ou não o valor pedido pelos criminosos?

A orientação dos órgãos de segurança é não pagar. Entretanto, cabe fazermos uma análise sobre a extensão do dano sofrido. Se a vítima possui dados importantes que venham a trazer altos prejuízos a si quanto a terceiros, talvez a melhor opção seja pagar o resgate. Mas é importante frisar que o pagamento desses valores não será a garantia de que o criminoso enviará a chave que irá descriptografar os arquivos.

3.5. A Criptomoeda

Normalmente, os cibercriminosos têm utilizado o *bitcoin* (criptomoeda) para o pagamento dos resgates por dificultar o rastreamento das transações. O *bitcoin* consiste em uma moeda digital descentralizada, ou seja, ela não depende de um emissor central e pode ser transacionada para qualquer pessoa em qualquer parte do planeta sem intermediários e, inclusive, sem limite de valor. Sem muito aprofundamento, para utilizá-la, cada usuário terá de criar uma "carteira" (um programa). Ela serve para acumular os seus endereços *bitcoin*. Assim, ao criar uma carteira, o usuário receberá duas chaves: uma chave criptografada pública e outra privada. A chave pública é aquela em que o usuário informará aos outros e utilizará para efetuar suas transações e a chave privada é como se fosse a "senha" da chave pública. Como as chaves públicas são muito extensas, utiliza-se muito nessas transações o chamado *QR Code*[9], que é a representação da chave pública em forma de imagem.

Quando ocorrem essas transações, é gerada uma corrente de blocos (*blockchain*[10]), que é basicamente um banco de dados. Cria-se, então, um bloco inicial que, a cada 10 minutos, é ampliado e um novo bloco é gerado, de modo que cada bloco posterior possui informações de seu antecessor. Assim ocorre até o final da transação.

Como forma de proteção, cada transação efetuada é impressa na rede *bitcoin*, de modo que não há possibilidade de tentar gastar aquela moeda em mais de uma transação. As transações são públicas, mas ninguém sabe quem são as pessoas que estão por trás dos pontos de início e fim, em tese, garantindo o anonimato. Por óbvio que usuários comuns podem deixar outros rastros em suas transações, como, por exemplo, seu número de IP. Sabemos que os criminosos facilmente podem mascarar seu IP original. Por tais fatores, os cibercriminosos preferem essa moeda em suas empreitadas.

4. Prevenção

Um dos principais fatores de sucesso dos ciberataques é a exploração das vulnerabilidades do usuário final. Os usuários particulares ainda não se deram conta

[9] Código *QR* (sigla do inglês *Quick Response*) é um código de barras bidimensional que pode ser facilmente escaneado usando a maioria dos telefones celulares equipados com câmera. Esse código é convertido em texto (interativo), um endereço de internet, um número de telefone, uma localização georreferenciada, um *e-mail*, um contato ou um SMS.

[10] A cadeia de blocos, ou *blockchain*, é o sistema de registros que garante a segurança das operações realizadas por criptomoedas – as *bitcoins*.

das ameaças que se escondem por trás de uma simples visita à internet. As empresas e os governos devem investir pesado em campanhas de conscientização de seus funcionários para a execução de uma navegação segura. Visando à prevenção e à minimização dos danos, é de extrema importância fazer uma cópia periódica (*backup*) de todos os dados das máquinas em mídia física externa. Noutro ponto, outras medidas simples, porém não menos importantes, como a ativação da extensão dos arquivos, bem como o monitoramento dos anexos dos *e-mails*, para evitar que um arquivo executável malicioso seja ativado.

Manter os programas sempre atualizados, porque estes estão sempre em desenvolvimento de proteção para novas ameaças. Importante baixar aplicativos apenas de fontes confiáveis, verificando se as permissões de instalação e execução são coerentes e desabilitar a autoexecução de mídias removíveis e de arquivos que estejam anexados. Algumas empresas de cibersegurança também desenvolvem ferramentas gratuitas para descriptografar dados infectados por *ransomware*, tendo como exemplo o *site www.nomoreransom.org*.

As equipes de segurança da informação também utilizam a chamada *sandbox* (caixa de areia), que é uma ferramenta capaz de executar os programas suspeitos de forma isolada, num ambiente virtual dentro da própria máquina, possibilitando ao usuário analisar seus procedimentos de forma segura, num perímetro limitado e sem afetar a máquina. Outro procedimento utilizado é o chamado método *honeyfile* ou *honeypot* (arquivo de mel ou pote de mel), onde se apresenta um sistema exposto como uma isca para um ataque. Diante desse ataque, a equipe de segurança da informação poderá estudá-lo, podendo desenvolver novos mecanismos de defesa para novos vírus.

Por óbvio que os procedimentos de prevenção não se esgotam aqui, diversos procedimentos técnicos são utilizados, mas não caberia maior aprofundamento, tendo em vista correr o risco de desviarmos da análise jurídica do presente estudo.

5. A Polícia Judiciária e o Combate ao *Ransomware*

Em nosso ordenamento jurídico, a competência para a apuração das infrações penais cabe às Polícias Civis dos Estados e à Polícia Federal, conforme preceitua o artigo 144 da Constituição da República, bem como aos membros do Ministério Público[11]. Diante da evolução tecnológica, a prática de crimes cibernéticos se tornou uma realidade, havendo uma constante necessidade dos órgãos de investigação acompanharem essa evolução. As organizações criminosas têm explorado esse mercado cada vez mais lucrativo e interessante, onde a busca pelo anonimato tem dificultado a atuação desses órgãos de investigação.

Ao tratarmos de crimes cibernéticos, precisamos também entendê-los como uma ameaça real à segurança dos países. Diante disso, também há necessidade de planejamento para a construção de uma defesa cibernética com a finalidade de proteger

[11] (STF. Plenário. RE nº 593727/MG, Rel. Orig. Min. Cezar Peluso, red. p/ o acórdão Min. Gilmar Mendes, julgado em 14/5/2015) (repercussão geral) (Info nº 785) – (Resolução nº 13/2006 do CNMP).

áreas importantes como a energia, finanças, transporte, telecomunicações, informação, entre outras. O *Livro Verde* – Segurança Cibernética no Brasil assim dispõe[12]:

> Em decorrência de tais avanços tecnológicos e da velocidade com que os mesmos vêm ocorrendo, é possível verificar um movimento acentuado de rearranjo das proposições das nações em termos de segurança e defesa. Tal está sendo propiciado, quer seja por meio da revisão e/ou reforço de suas políticas, estratégias e normas, quer seja pela atualização e/ou reformulação das competências essenciais de órgãos chave de governo, visando, principalmente, a criar as condições necessárias de segurança e defesa do espaço cibernético, notadamente no que diz respeito ao entendimento das novas exigências para a proteção de uma nação.
>
> (...)
>
> A Política Nacional de Segurança Cibernética deverá ter como uma de suas premissas a sua construção a partir de visão multidisciplinar, interinstitucional, em que múltiplas competências se complementam na solução de problemas e na identificação de oportunidades.

Diante dessas circunstâncias, pode-se inferir que as despesas com segurança digital se tornarão cada vez mais caras, bastando analisarmos o fato de que estes ataques já causaram, em 2016, um prejuízo de mais de 05 cinco bilhões de dólares[13].

Oportuno dizer que, dentro do contexto supracitado, a definição de cibercrime se traduz em qualquer crime perpetrado com o uso de redes ou da internet e este termo teve origem no final da década de 1990, em Lyon (França), onde um subgrupo do G-8 (grupo dos países mais ricos e influentes do mundo) se reuniu para tratar dos crimes praticados pela Internet[14].

Não obstante o aludido conceito, diante da nova realidade tecnológica, crimes já conhecidos ganharam nova roupagem e novos tipos penais foram criados. A partir dessa situação, para uma melhor análise técnico-jurídica, se faz necessária a divisão em crimes cibernéticos próprios, impróprios e mistos, nas palavras de Stenio Santos Sousa[15]:

---

[12] BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. *Livro verde:* Segurança cibernética no Brasil / Gabinete de Segurança Institucional, Departamento de Segurança da Informação e Comunicações; organização Claudia Canongia e Raphael Mandarino Junior. Brasília, 2010. p.63.

[13] FELIPE, Leandra. Cibercrimes causaram prejuízos de bilhões de dólares no mundo em 2016. *Agência Brasil*. Estados Unidos. 31 mai. 2017. Disponível em: <http://agenciabrasil.ebc.com.br/geral/noticia/2017-05/cibercrimes-causaram-prejuizos-de-bilhoes-de-dolares-no-mundo-em-2016>. Acesso em: 05 jun. 2017.

[14] BARBAI, Marcos A. *A criminalidade no espaço digital*: a formulação do sentido. *In*: DIAS, Cristiane. *Formas de mobilidade no espaço e-urbano*: sentido e materialidade digital [*online*]. Série e-urbano. Vol. 2, 2013. Consulta no Portal Labeurb – http://www.labeurb.unicamp.br/livroEurbano/ Laboratório de Estudos Urbanos – LABEURB/ Núcleo de Desenvolvimento da Criatividade – NUDECRI, Universidade Estadual de Campinas – UNICAMP.

[15] SANTOS, Stenio Sousa *et al*. *Combate ao Crime Cibernético*. Contribuição crítica ao processo de investigação criminal da fraude bancária eletrônica: *Ubi societas, ibi criminis*? 1ª ed. Rio de Janeiro: M. Mallet Editora Ltda., 2016, p.52.

> Na primeira hipótese, diz-se do crime que tem como objetivo o ataque ao próprio sistema computacional. É exemplo dessa conduta a invasão de computadores, a disseminação de vírus e o ataque de negação de serviços, entre outros.
>
> Da segunda espécie, encontram-se todos os que são praticados por meio ou com o auxílio da tecnologia. Ainda que não houvesse o sistema computacional, o delito continuaria evidenciado, posto que existente em formato tradicional. A tecnologia apenas facilita a conduta ilícito-típica, mas não é sua *conditio sine qua non*.
>
> (...)
>
> Crimes cibernéticos mistos são aqueles em que não apenas se utiliza a tecnologia para a comissão delitiva, mas onde esta se torna imprescindível ou ao menos torna o delito particularmente ofensivo ou lesivo. Crimes como os de pornografia infantil pela internet e as fraudes bancárias eletrônicas exemplificam essa classificação.

Outra frente de combate advém do Poder Legislativo na produção de legislação específica, uma vez que ataques cibernéticos, geralmente, dão acesso a informações confidenciais de grandes corporações e até mesmo de importantes órgãos estatais. Cumpre trazer à baila a lembrança do ataque mundial ocorrido em maio deste ano, que atingiu, inclusive, Tribunais de Justiça[16] e o Ministério Público do Estado de São Paulo[17].

Nesse contexto, importante citar a Resolução nº 1, de 15 de julho de 2009, editada pelo Poder Executivo, através do Ministério da Justiça, a qual regulamenta o Subsistema de Inteligência de Segurança Pública (SISP), que tem como objetivo fornecer informações aos governos no auxílio à tomada de decisões na seara da segurança pública, através da obtenção, análise e compartilhamento de informação útil e salvaguarda da informação contra acessos não autorizados. A presente norma visa à preservação e defesa da sociedade e do Estado, bem como das instituições, observando a responsabilidade social e ambiental, a dignidade da pessoa humana, a promoção dos direitos e garantias individuais e do Estado Democrático de Direito, o SISP integra o Sistema Brasileiro de Inteligência (SISIBN).

Além da Lei nº 9.296/96 (Lei da Interceptação Telefônica), da Lei nº 12.850/13 (Lei das Organizações Criminosas) e da Lei nº 13.441/2017 (Infiltração de agentes nos crimes contra a dignidade sexual de crianças e adolescentes), outro diploma relevante é a Lei nº 12.965/2014, denominada "Marco Civil da Internet", que tem grande importância na investigação destes crimes cibernéticos, uma vez que veio trazer maior luz à lacuna

[16] LUCHETE, Felipe; GALLI, Marcelo. Dez tribunais tiram site do ar após ataque cibernético mundial. *Revista Consultor Jurídico*. 12 mai. 2017. Disponível em: <http://www.conjur.com.br/2017-mai-12/dez-tribunais-tiram-site-ar-ataque-cibernetico-mundial>. Acesso em: 17 mai. 2017.

[17] NÚCLEO DE COMUNICAÇÃO SOCIAL. Nota de Esclarecimento sobre a rede de computadores do MP-SP. *Ministério Público do Estado de São Paulo*. São Paulo. 12 mai. 2017. Disponível em: <http://www.mpsp.mp.br/portal/page/portal/noticias/noticia?id_noticia=16942683&id_grupo=118>. Acesso em: 17 de maio de 2017.

legislativa sobre o grande fluxo de informações na rede. Isto porque ainda há uma grande dificuldade das autoridades em obterem acesso às fontes fechadas, diante da desobediência de alguns provedores de serviços de internet. Em seu artigo 3º, a presente Lei dispõe sobre os princípios:

> Art. 3º – A disciplina do uso da internet no Brasil tem os seguintes princípios:
>
> I – garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
>
> II – proteção da privacidade;
>
> III – proteção dos dados pessoais, na forma da lei;
>
> IV – preservação e garantia da neutralidade de rede;
>
> V – preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
>
> VI – responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
>
> VII – preservação da natureza participativa da rede;
>
> VIII – liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.

Entretanto, sabemos que, no ordenamento jurídico pátrio, não há direito absoluto, devendo o Poder Judiciário ponderar esses princípios dentro de cada caso concreto. No que corresponde ao armazenamento e à disponibilização das informações, em seu artigo 10, estabeleceu-se que os provedores de acesso e aplicativos da internet devem: guardar os registros de conexão e acesso; informar os dados de cadastro às autoridades, mediante requisição das autoridades administrativas competentes; disponibilizar os registros de conexão e acesso de forma autônoma ou associados a dados pessoais, ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, bem como disponibilizar o conteúdo das comunicações privadas, diante de ordem judicial.

A obtenção dessas informações pelas autoridades requer a observância de determinados quesitos elencados no parágrafo único do artigo 22, *in verbis*:

> Art. 22 – A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet.

> Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade:
>
> I – fundados indícios da ocorrência do ilícito;
>
> II – justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e
>
> III – período ao qual se referem os registros.

No procedimento investigativo dos crimes de informática, em que pese a tentativa do anonimato, evidencia-se que estas atividades criminosas deixam rastros e, em obediência ao comando disposto no artigo 158 do Código de Processo Penal[18], as autoridades dispõem de diversos mecanismos para a coleta destes dados. Eles podem ser obtidos através da análise das fontes abertas e fontes fechadas. Segundo Alessandro Gonçalves Barreto[19], as chamadas fontes abertas são aquelas de livre acesso, sem obstáculo à obtenção dos dados e conhecimentos. As fontes fechadas são aquelas cujos dados são protegidos ou negados, necessitando de um credenciamento, uma operação de busca para sua obtenção.

A busca e coleta de dados em fontes abertas propicia uma análise sem a necessidade de autorização judicial. Desta forma, os investigadores têm acesso a informações contidas em banco de dados públicos, livros, revistas, artigos científicos, programas, *sites*, redes sociais, *blogs*, entre outros meios, sem maiores dificuldades. Especificamente, ressaltamos que os dados cadastrais não necessitam de autorização judicial porque representam requisitos mínimos da vida em sociedade.

Os dados podem se dividir em humanos e eletrônicos: o primeiro privilegia o homem, o investigado; o último se atém às ferramentas e aos equipamentos utilizados para a prática do crime. A utilização das fontes abertas traz maior celeridade ao procedimento investigativo, não havendo necessidade das autorizações judiciais, bem como dá maior robustez aos elementos de prova dentro do inquérito.

As fontes fechadas trazem maior complexidade na obtenção de suas informações, uma vez que restam protegidas pela Constituição Federal/88, justamente por estarem vinculadas a direitos fundamentais como: a intimidade, a honra, a vida privada (art. 5º, X, CF/88), o sigilo das correspondências e das comunicações telegráficas, de dados e das comunicações telefônicas (art. 5º, XII, CF/88). Diante disso, justifica-se a autorização judicial, conforme o art. 10 c/c art. 22 da Lei nº 12.965/2014, sob pena de agirem ao arrepio da lei.

Importante salientar que as informações mínimas em uma requisição, seja aos provedores de acesso bem como às companhias telefônicas, devem, no mínimo,

---

[18] Art. 158 Quando a infração deixar vestígios será indispensável o exame de corpo de delito, direto ou indireto, não podendo supri-lo a confissão do acusado. (Decreto-Lei n° 3.689, de 03/10/41 – Código de Processo Penal).

[19] BARRETO, Alessandro Gonçalves; WENDT, Emerson; CASELLI, Guilherme. *Investigação digital em fontes abertas*. 1ª ed. Rio de Janeiro: Brasport Editora, 2017. p.16.

conter: o número do IP; a data em que ocorreu a comunicação; e o horário, indicando qual o fuso horário utilizado (GMT ou UTC).

5.1. Principais Mecanismos de Investigação

O combate aos diversos crimes praticados na grande rede mundial de computadores deve observar diversos fatores, entre eles o aspecto jurídico, quanto à eventual necessidade de autorização judicial, e o técnico, no que tange aos equipamentos e à capacitação dos profissionais envolvidos nesse mister. A Polícia Federal mantém, em suas superintendências, Grupos de Repressão a Crimes Cibernéticos (GRCC) e, em âmbito estadual, particularmente no Rio de Janeiro, a Polícia Civil possui a especializada Delegacia de Repressão aos Crimes de Informática (DRCI).

Cumpre observar que, nesse tipo de crime, as evidências apresentam características diversas, possuindo diversos formatos, pois podem dizer respeito a imagens, vídeo, áudio, planilhas, documentos, seja de forma isolada ou em conjunto. Estas evidências, por serem facilmente destruídas ou alteradas, devem ser de pronto preservadas. Tais evidências estão misturadas a outros dados, obrigando os investigadores e técnicos a fazerem uma análise mais apurada durante a sua obtenção.

Na apuração desses crimes, cada área tem seus procedimentos específicos, por exemplo: análise dos dados registrados nos servidores; análise dos pacotes de dados contidos na transferência de informações dentro da rede; quanto à investigação relacionada a *websites*, é necessária a guarda de todos os seus componentes e, para isso, existem programas específicos como: *HTTrack, Express WebPictures, Grab-a-Site, WebLooper, WebReaper.*

Além disso, há necessidade da descoberta do servidor que faz a hospedagem desses *websites* e, para isso, é importante saber se o *website* em questão é nacional ou não. Através da ferramenta *whois*[20], bem como do *site* (www.registro.br), o qual é o responsável pelo registro dos domínios das páginas no Brasil, é possível ter acesso ao nome do responsável administrativo pelo domínio; ao contato de incidentes de segurança (responsável pelo Setor de Tecnologia de Informação) e ao provedor de *backbone*[21] (empresa que detém blocos de endereços IP's).

Caso o domínio seja estrangeiro, ainda há possibilidade de obtermos estas informações por outros serviços de *whois*, tais como: http://www.internic.net/whois.html; http://lacnic.net/; http://www.arin.net/ e http://www.netoworksolutions.com.

Em que pese o fato de os crimes cibernéticos deixarem rastros, sabemos que os cibercriminosos também utilizam de ferramentas para buscar o anonimato

[20] A ferramenta *WHOIS* é utilizada para se obter informações sobre um determinado domínio. Através do *WHOIS,* podem-se obter informações sobre os servidores DNS, estado do domínio (ativo, expirado etc.), informações sobre a empresa de hospedagem de sites, entre outros dados.

[21] O *backbone*, tradução de "espinha dorsal", é uma rede principal por onde passam os dados dos clientes da internet. Todas essas vias [ou pequenas redes] estão conectadas à estrada principal [*backbone*].

em suas ações. Um exemplo disso é o navegador *TOR*[22], um dos mais utilizados para acessar a *deep web* para a prática de crimes. Ele mascara o IP original e a localização, embaralhando as informações e dificultando a identificação. Isso ocorre por causa de seu complexo mecanismo, que utiliza uma rede de transmissão de dados baseada em múltiplas máquinas. Assim, ao enviar uma mensagem, ela passa não por apenas uma, mas por inúmeras máquinas até chegar ao destinatário. O objetivo é dificultar o acesso indevido ao computador, confundindo quem tenta invadir a sua privacidade para ter acesso às suas informações.

Ressalte-se que não há crime perfeito, pois, ainda que esteja anônimo, quem navega pela *deep web* e troca mensagens produz pacotes (unidades de dados) e, ao monitorar a rede, esses dados podem dar aos agentes indícios de atividades ilícitas através da análise do tempo dos dados transmitidos. Registre-se que a Polícia Federal desenvolveu uma tecnologia inédita na América Latina, que possibilitou efetuar o monitoramento da *deep web*, o que resultou na operação *Darknet* em 2014. Segundo o Professor Rafael de Souza, em matéria publicada na Associação Nacional dos Delegados da Polícia Federal[23]:

> Uma das formas de se investigar a rede secreta, segundo o professor, é estudando o tráfego da internet. Embora com IP escondido, quem troca mensagens pela *deep web* ainda produz pacotes (como são chamadas as unidades de dados) visíveis. Um dos indícios de que existiria uma atividade ilícita seria a troca de pacotes entre um pequeno grupo de usuários sem localização de IP definida.
>
> Tráfego de dados constante entre computadores ocultos é um sinal mais do que suspeito.
>
> Quem monitora esse trânsito consegue, também, verificar o formato das mensagens partilhadas.
>
> Geralmente, grupos de pedofilia na *deep web*, por exemplo, trocam fotos, identificadas pelo formato, que pode ser jpg, jpge, entre outros.

A partir de nossa pesquisa sobre o *ransomware*, percebemos que parte relevante do sucesso nos ataques está na falta de informação/cuidado do usuário final na administração de seus *e-mails* pessoais e profissionais. Portanto, a abordagem abaixo trata do mecanismo de investigação no que tange aos *e-mails*.

Quando um *e-mail* é enviado, aparece o endereço do remetente e do destinatário no chamado "cabeçalho" da mensagem (os navegadores dispõem

[22] *TOR (The Onion Router*) é uma rede de túneis virtuais que dificulta e embaralha a identificação dos equipamentos ao acessarem determinado conteúdo na rede.

[23] GUIMARÃES, Fabiane. *A internet que ninguém via. Metro*. Associação Nacional dos Delegados de Polícia Federal. 30 dez. 2014. Disponível em: <http://www.adpf.org.br/adpf/admin/painelcontrole/materia/materia_portal.wsp?tmp.edt.materia_codigo=7235&tit=A-internet-que-ninguem-via#.WVsS6YjyvIV>. Acesso em: 03 jul. 2017.

dessa função, geralmente, na aba opções). O objetivo é ter acesso a todos os códigos da mensagem para descobrir a numeração do IP, a data e a hora da mensagem. Numa primeira análise de conteúdo, busca-se a palavra *received* (recebido), essa palavra aparece em ordem decrescente e indica por quantas estações (servidores) a mensagem passou antes de chegar ao destinatário final. Assim, na última palavra *received,* podemos encontrar quem foi o remetente.

Ao localizar o IP, a autoridade interessada deverá efetuar a pesquisa nos mecanismos *whois* para ter acesso aos dados do provedor de acesso e, a partir daí, a pedido dela, o juiz oficiará esse provedor no sentido de quebrar o sigilo dos dados telemáticos com a finalidade de acessar as informações do usuário vinculado ao IP em uma determinada data e horário.

Caso não consiga localizar o número do IP, a partir do *e-mail* do remetente, pode-se requerer judicialmente a quebra do sigilo de dados telemáticos ao provedor deste *e-mail* para que ele informe o número do IP da máquina que autenticou a conta na data e horário do *e-mail* enviado.

Outro procedimento é o monitoramento de *e-mail* de alvos suspeitos (mediante autorização judicial). Dessa forma, o juiz pode determinar que o provedor responsável pela conta desvie as mensagens enviadas ou recebidas para uma conta de monitoramento, possibilitando que as mensagens sejam analisadas. Assim, será possível saber com quem o alvo se corresponde e de onde realiza os acessos.

6. Mecanismos de Cooperação Internacional

O Estado brasileiro é signatário de diversos tratados internacionais e, diante das conexões político-econômicas, a República Federativa do Brasil se comporta nas relações internacionais na forma do artigo 4º da Constituição Federal, sendo regida pelos seguintes princípios, *in verbis*:

> Art. 4º – A República Federativa do Brasil rege-se nas suas relações internacionais pelos seguintes princípios:
>
> I – independência nacional;
>
> II – prevalência dos direitos humanos;
>
> III – autodeterminação dos povos;
>
> IV – não intervenção;
>
> V – igualdade entre os Estados;
>
> VI – defesa da paz;
>
> VII – solução pacífica dos conflitos;
>
> VIII – repúdio ao terrorismo e ao racismo;
>
> IX – cooperação entre os povos para o progresso da humanidade;

> X – concessão de asilo político.
>
> Parágrafo único. A República Federativa do Brasil buscará a integração econômica, política, social e cultural dos povos da América Latina, visando à formação de uma comunidade latino-americana de nações.

A dificuldade encontrada pelas autoridades na apuração dos crimes cibernéticos está na característica transnacional destes, havendo grande obstáculo na obtenção de provas ou indícios, tendo em vista não haver uma legislação unificada, considerando-se a soberania dos países. Diante da inexistência de poder coercitivo na esfera internacional, os países estabelecem tratados internacionais e acordos de cooperação. Nessa atuação, há necessidade de uma combinação entre os tratados, os princípios do direito internacional e a legislação que regulamenta as empresas privadas que atuam na internet.

Importante instrumento em âmbito global no combate aos crimes cibernéticos é a Convenção de Budapeste (Convenção sobre o Cibercrime), firmada pelo Conselho Europeu em 23/11/2001 na Hungria. Entretanto, o Brasil pode assinar mesmo não tendo participado de sua redação da época. Em seus quarenta e oito artigos, acreditando que uma luta efetiva contra a cibercriminalidade requer uma cooperação internacional em matéria penal, rápida e eficaz, ela disciplina procedimentos como: medidas legislativas a serem tomadas a nível nacional entre os membros; a manutenção dos dados informáticos; a interceptação e o recolhimento em tempo real dos dados de tráfego; estabelece os princípios gerais relativos ao auxílio mútuo, entre outros.

Ao tomar como exemplo o fato de que a maioria das empresas privadas que atuam na internet possuem suas sedes nos Estados Unidos da América e que existe acordo de cooperação internacional entre Brasil e EUA, discorreremos sobre os principais procedimentos utilizados na investigação de crimes transnacionais em relação aos dois países. Numa investigação nesse sentido, a Constituição Federal, em seu artigo 144, §1º e §4º, c/c o art. 2º da Lei nº 12.830/2013, confere aos delegados de polícia federal e delegados de polícia civil dos estados a competência para requerer estes dados. O Ministério Público, amparado pelo artigo 8º da Lei Complementar nº 75/93 c/c o artigo 62 da Lei nº 8.625/93 c/c Resolução nº 13/2006 CNMP e diante do entendimento do STF, no julgamento do RE nº 593727/MG em 2015, também é autoridade competente nesse sentido. No entanto, ressaltamos que, diante destes pedidos, o Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional do Ministério da Justiça (DRCI/MJ) é o órgão competente para auxiliar estas autoridades nesse mister, conforme o art. 10, V, do Decreto nº 8.668, de 11 de fevereiro de 2016. Estas autoridades atuam em conjunto com outros países e com instituições como a Interpol, Europol, Ameripol, FBI, entre outras.

O Marco Civil da Internet (Lei nº 12.965/2014), no §2º do artigo 11, estabelece que a legislação brasileira deverá ser aplicada às empresas estrangeiras sediadas no exterior, desde que estas ofertem serviços ao público brasileiro ou que pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil. Noutro ponto, também estabelece que se aplica a lei brasileira aos dados coletados em

território nacional desde que pelo menos um dos terminais esteja localizado no Brasil. No entanto, diante das dificuldades na obtenção destes dados, em investigações sobre cibercrimes de ordem transnacional, as autoridades fazem uso do *MLAT* (*Mutual Legal Assistance Treaty*), que é um acordo mútuo de assistência legal firmado entre países. Ressalte-se que o Ministério Público Federal (MPF) defende o entendimento do Marco Civil, que não exige o *MLAT* (*Mutual Legal Assistance Treaty*) quando a empresa presta serviços no Brasil. O governo do Brasil e o dos Estados Unidos da América firmaram esse acordo de assistência judiciária em matéria penal em outubro de 1997 e está representado em nosso ordenamento pelo Decreto nº 3.810/2001.

Para a obtenção dos dados não amparados pelo manto constitucional, as autoridades lançam mão do documento chamado *Subpoena*, que, parafraseando José Augusto Campos Versiani[24], este termo tem como tradução literal "intimação", mas pode ser entendido como uma requisição que deve ser preenchida em inglês, assinada, digitalizada e encaminhada à empresa detentora da informação. No que tange aos dados protegidos, as autoridades valem-se do *MLAT*, devendo, também, observar o princípio da dupla-incriminação.

O acordo de cooperação internacional deve obedecer a requisitos de ordem formal e material, partindo-se de uma base legal como uma convenção, um acordo internacional e o princípio da reciprocidade, devendo passar, obrigatoriamente, pela autoridade central designada para esse fim. Ressalte-se que serve tanto para a cooperação ativa ou passiva e que, em nosso caso, é o Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional do Ministério da Justiça (DRCI/MJ)[25]. As solicitações devem ser produzidas em duas vias, tomando como exemplo investigações originadas aqui no Brasil; a primeira via será original na língua portuguesa e a segunda via, traduzida para o idioma do Estado requerido.

No que tange aos requisitos materiais, obrigatoriamente, a autoridade requerente deverá endereçar o pedido ao correto destinatário da solicitação, que, em nosso exemplo, é o Departamento de Justiça dos Estados Unidos da América. Noutro ponto, é importante indicar o órgão e a autoridade competente responsável pelo inquérito policial ou qualquer outro procedimento de investigação criminal, ou, ainda, pela ação penal em curso, informando o número do inquérito ou da ação penal, o cargo e o nome completo das autoridades, bem como os dados de contato, tais como *e-mails* ou telefone.

Não menos importante é a descrição narrativa completa, clara e objetiva dos fatos, discorrendo sobre os elementos essenciais dos acontecimentos, as circunstâncias sobre o lugar, a data e a maneira pela qual a infração foi cometida, esclarecendo detalhadamente o nexo causal entre a investigação ou processo em curso, seus suspeitos ou réus e a assistência jurídica solicitada.

---

[24] VERSIANI, José Augusto Campos *et al*. *Combate ao Crime Cibernético*. Cooperação Internacional na Investigação de Crimes Cibernéticos. 1ª ed. Rio de Janeiro: M. Mallet Editora Ltda., 2016. p.156.

[25] BRASIL. Secretaria Nacional de Justiça. Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional. *Manual de cooperação jurídica internacional e recuperação de ativos*: cooperação em matéria penal/Secretaria Nacional de Justiça. Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional (DRCI). 3ª ed. Brasília: Ministério da Justiça, 2014. p.56.

6.1. Territorialidade

A necessidade de combate aos cibercrimes, em especial ao *ransomware*, invariavelmente, transita pelo assunto da territorialidade/extraterritorialidade. Em que pese o fato de existirem diversos mecanismos de investigação, inclusive com colaborações em tempo real, como é o caso do sistema mundial de informação (I-24/7)[26], da Interpol, o qual funciona 24 horas nos 07 dias da semana, sabemos que os cibercriminosos utilizam ferramentas que camuflam sua identidade, dificultando a análise de seus rastros, conforme já ventilado em tópicos anteriores.

Exemplo importante de toda essa complexidade é o fato de que um criminoso em um determinado país pode infectar uma máquina em um outro, utilizando-se de um servidor que se encontra em um terceiro país. Em outra forma de ataque, criminosos também podem infectar determinada máquina, valendo-se de outra máquina (zumbi)[27], situada em qualquer outro país.

Nesse contexto, salientamos o status residual da competência da justiça estadual em relação à Justiça Federal em seu artigo 109, IV e V, da Constituição Federal. Diante da controversa doutrina, imaginemos um cibercrime: um ataque de *ransomware* ocorrido em território brasileiro, porém em estados diferentes, o chamado "crime plurilocal". Tomando como exemplo, um criminoso situado no estado do Rio de Janeiro infecta um computador de um usuário residente no estado de São Paulo, passando a exigir que este deposite certa quantia em moeda virtual para liberar o acesso à máquina infectada, conduta tipificada no artigo 154-A do Código Penal.

Numa primeira análise, percebemos que tal crime possui pena de até 02 anos, submetendo-se à Lei nº 9.099/95 (Juizado Especial Criminal), a qual adota, em seu artigo 63, a teoria da ubiquidade, competindo ao órgão judicial do lugar em que foi praticada a infração penal julgá-la (Justiça Estadual do Rio de Janeiro). Em uma análise prática, percebe-se que, ao adotar tal teoria, em alguns casos, ela atentaria contra os próprios princípios norteadores da Lei nº 9.099/95, em seu artigo 2º: a economia processual e a celeridade, uma vez que obrigaria a vítima a se deslocar até outro estado (Art. 154-B), podendo inviabilizar a prestação jurisdicional.

Ressalte-se que, a depender do caso concreto, tal conduta poderá ultrapassar os 02 anos, não mais se enquadrando como de menor potencial ofensivo, submetendo-se à Vara Criminal. Nesse sentido a competência será determinada pelo lugar em que se consumou a infração, com fulcro no artigo 70 do Código de Processo Penal, consagrando a teoria do resultado.

---

[26] BLAT, Erick Ferreira *et al*. *Combate ao Crime Cibernético*. Ferramentas de investigação nos crimes cibernéticos utilizadas pela Polícia Federal. 1ª ed. Rio de Janeiro: M. Mallet Editora Ltda., 2016. p.78

[27] Computador zumbi é um termo empregado para classificar computadores utilizados para envio de *spam* e ataque a *sites*, sem que o dono do computador saiba de tal atividade.
Para que isso aconteça, o invasor precisa instalar um programa no computador-alvo, normalmente através de *e-mails*, redes ponto-a-ponto (*peer-to-peer*) ou mesmo através de *sites* com links onde o invasor disfarça o programa para que o usuário não saiba de que se trata. Após a instalação do programa, o invasor passa a utilizar esse computador (juntamente com todos os outros computadores infectados) para enviar *e-mails* em série (*spam*) com diversas finalidades, ou mesmo para atacar *sites*, com intuito de criar danos ao *site* ou deixá-lo lento.

Ponto importante é a análise da redação contida no artigo 5º do Código Penal, que dispõe aplicar-se a lei brasileira, sem prejuízo das convenções, tratados e regras de direito internacional ao crime praticado no território nacional. Adotando, assim, a teoria da territorialidade temperada, onde o Brasil abre uma lacuna à sua exclusividade em prol da cooperação internacional.

Diante dessa abordagem, quanto aos crimes a distância que se iniciam em um país e terminam em outro, tratando-se da aplicação da norma penal no espaço, a aplicabilidade do artigo 6º do Código Penal se vislumbra a mais adequada. Ele considera praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado, adotando, assim, a teoria da ubiquidade.

7. Análise Legislativa (Lei nº 12.737/2012)

A evolução das relações econômicas e tecnológicas condicionou a sociedade a depender cada vez mais da internet e, hoje em dia, nos grandes centros, é praticamente impossível haver pessoas físicas ou jurídicas que não possuam um computador, um *tablet* ou um celular que lhes auxilie nas relações de trabalho ou simplesmente de lazer. Diante desse crescente fluxo de dados, a tecnologia da informação se mostra de extrema importância para nos auxiliar nessa nova realidade, seja na melhora da produtividade, dando mais eficiência às relações, bem como na proteção estratégica de informações pessoais, empresariais e/ou governamentais.

Dentro desse contexto, os crimes praticados pela internet cresceram e disseminou-se uma silenciosa guerra por importantes informações sigilosas. Entre outros projetos que tramitavam no Poder Legislativo, em 30 de novembro de 2012, foi sancionada a Lei nº 12.737/2012[28] (Projeto de Lei nº 2.793/2011).

Apelidada de "Lei Carolina Dieckmann", ela entra no ordenamento jurídico de forma muito rápida e leva esse apelido por manter relação com o episódio do furto de fotos íntimas do computador da supracitada atriz, a qual teve tais fotos divulgadas na internet[29]. Entre outros tipos penais criados pela Lei, consta o art. 154-A, que altera o Código Penal com o *nomen iuris* de "invasão de dispositivo informático", o qual tipifica a conduta apresentada no presente estudo. Com o fito de analisarmos o aludido artigo, é necessário transcrevê-lo abaixo:

> 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

[28] BRASIL. *Lei nº 12.737*, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal – e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 30 jul. 2017.

[29] Carolina Dieckmann fala pela 1ª vez sobre fotos e diz que espera *justiça*. *G1*. São Paulo. 14 mai. 2012. Disponível em: <http://g1.globo.com/pop-arte/noticia/2012/05/carolina-dieckmann-fala-pela-1-vez-sobre-roubo-de-fotos-intimas.html>. Acesso em: 30 jul. 2017.

> 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.

Os cibercriminosos que se utilizam do *ransomware* praticam a conduta prevista no referido artigo, mas, para melhor examinarmos, é importante fracioná-lo: *invadir / dispositivo informático alheio / conectado ou não à rede de computadores / mediante violação indevida de mecanismo de segurança / 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.*

Em análise, conforme já ventilado no tópico 4 (Dinâmica dos Ataques) do presente estudo, os criminosos invadem dispositivo informático alheio, normalmente conectado à internet, assim considerados os *smartphones*, computadores, *tablets*, *ipads*, *ipods* etc. Importante observarmos o termo "mediante violação indevida de mecanismo de segurança" e por mecanismo de segurança podem ser considerados *antimalware*[30], *backups*, *login*/senha, certificado digital[31], *firewall*[32], entre outros.

Sabemos que existem diversas possibilidades de invadir e infectar a máquina e, a título de exemplo, ainda que o usuário execute um *malware "*camuflado" anexado ao seu *e-mail* (prática descrita como *phishing*), ainda configurar-se-á o crime, uma vez que existirá um vício de vontade (dolo) que faz o criminoso enganar o usuário e o *malware*, após instalado, ainda irá burlar os mecanismos de segurança da máquina.

Outro ponto é o especial fim de agir descrito no tipo penal: "com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo". Perceba que, no crime em comento, a conduta dos criminosos subsome-se ao tipo penal, tendo em vista que o *ransomware,* em sua silenciosa atuação, ao criptografar os arquivos, ele altera os dados, embaralhando as informações, obtendo-as em seus servidores de controle e comando, podendo, também, destruí-las se assim quiser o criminoso.

Ao final do tipo penal, "(...) ou instalar vulnerabilidades para obter vantagem ilícita", a parte final trata-se de mero exaurimento, mas ainda assim constitui uma finalidade específica de um ataque por *ransomware*. Uma das etapas é a instalação do programa, o qual irá modificar e explorar as vulnerabilidades do sistema para, na etapa final, forçar a vítima a pagar um valor para obter novamente o controle de seu sistema.

---

[30] Ferramentas *antimalware* são aquelas que procuram detectar e, então, anular ou remover os códigos maliciosos de um computador. Antivírus, *antispyware, antirootkit e antitrojan* são exemplos de ferramentas deste tipo.

[31] Certificado Digital – É um arquivo eletrônico que funciona como se fosse uma assinatura digital, com validade jurídica, e que garante proteção às transações eletrônicas e outros serviços via internet, de maneira que pessoas (físicas e jurídicas) se identifiquem e assinem digitalmente, de qualquer lugar do mundo, com mais segurança e agilidade.

[32] *Firewall* pode ser definido como uma barreira de proteção, que controla o tráfego de dados entre seu computador e a Internet (ou entre a rede onde seu computador está instalado e a Internet). Seu objetivo é permitir somente a transmissão e a recepção de dados autorizados.

> §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*.

No parágrafo primeiro, temos a figura da equiparação, o que demonstra que o legislador estava atento, pois se adequa perfeitamente à figura das organizações de cibercriminosos que disponibilizam os códigos maliciosos em fóruns de internet, terceirizando os ataques e cobrando um percentual sobre o valor recebido.

> §3º – Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
>
> Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

Temos no parágrafo terceiro a modalidade qualificada, dobrando a pena estipulada no primeiro parágrafo. Ciberataques vinculados à espionagem industrial e governamental são uma realidade[33], os ataques de *ransomware* geram grandes prejuízos[34], afetando a economia dos países. Uma questão gira em torno do que significa "informações sigilosas", discorrendo sobre o assunto, Rogério Grego[35] traz à baila o conceito de informação sigilosa para a administração pública, disposto no inciso III do artigo 4º da Lei nº 12.527/11 (Lei de Acesso à Informação), *in verbis*:

> Art. 4º – Para os efeitos desta lei, considera-se:
>
> (...)
>
> III – informação sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado.

Ponto relevante é se organizações criminosas em ciberataques conseguirem informações sigilosas sobre o Estado brasileiro. Nesse caso, aplicaremos o §3º do artigo

[33] GROSSMANN, Luís Oswaldo. Symantec *identifica ciberataques em 16 países com* malware *da CIA*. Convergência Digital. 10 abr. 2017. Disponível em: <http://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=44938&sid=18>. Acesso em: 06 ago. 2017.
[34] SANTANA, Felipe. 60% das pequenas empresas atingidas por vírus nos EUA vão à falência. *G1*. Nova Iorque, EUA. 13 mai. 2017. Disponível em: <http://g1.globo.com/mundo/blog/direto-de-nova-york/post/60-das-pequenas-empresas-atingidas-por-virus-nos-eua-vao-falencia.html>. Acesso em: 06 ago. 2017.
[35] GRECO, Rogério. *Código Penal Comentado*. 7ª ed. Niterói, RJ: Impetus, 2013. p.447.

154-A do Código Penal ou tal conduta se adequa ao crime tipificado no parágrafo único, inciso IV do artigo 13 da Lei nº 7.170/83 (Lei de Segurança Nacional), *in verbis*:

> Art. 13 – Comunicar, entregar ou permitir a comunicação ou a entrega, a governo ou grupo estrangeiro, ou a organização ou grupo de existência ilegal, de dados, documentos ou cópias de documentos, planos, códigos, cifras ou assuntos que, no interesse do Estado brasileiro, são classificados como sigilosos.
>
> Pena: reclusão, de 3 a 15 anos.
>
> Parágrafo único – Incorre na mesma pena quem:
>
> (...)
>
> IV – obtém ou revela, para fim de espionagem, desenhos, projetos, fotografias, notícias ou informações a respeito de técnicas, de tecnologias, de componentes, de equipamentos, de instalações ou de sistemas de processamento automatizado de dados, em uso ou em desenvolvimento no País, que, reputados essenciais para a sua defesa, segurança ou economia, devem permanecer em segredo.

O artigo 154-A protege a intimidade, a liberdade individual e a segurança da informação. Em estudo, sob o prisma do princípio da especialidade, percebe-se que sua redação traz diversos elementos que podem ser utilizados para a prática do delito. Entretanto, importante observarmos a expressão em seu §3º: "se a conduta não constitui crime mais grave".

Nessa esteira, trazemos à baila a Lei de Segurança Nacional (Lei nº 7.170/83), que, no inciso IV do parágrafo único do artigo 13, traz condutas que também se enquadram aos ataques por *ransomware*, punindo-as com reclusão de 03 a 15 anos. A referida lei tutela os interesses do Estado brasileiro no que tange à sua independência, segurança e integridade de seus órgãos supremos.

Não se pode olvidar que algumas agências de inteligência governamentais exploram e armazenam as vulnerabilidades dos sistemas operacionais utilizados na internet, criando *exploits*[36] para monitoramento em massa. Essas ferramentas podem ser utilizadas tanto pelos governos como por cibercrimonosos[37] em ataques com motivações políticas, religiosas ou econômicas. Desta feita, em um ataque por *ransomware*, dados sigilosos que são importantes para nosso país podem chegar às mãos dos criminosos através dos servidores de comando e controle que se comunicam com a(s) máquina(s) infectada(s).

[36] Um *exploit* geralmente é uma sequência de comandos, de dados ou uma parte de um *software* elaborados por *hackers* que conseguem tirar proveito de um defeito ou vulnerabilidade.

[37] HIGA, Paulo. Microsoft reclama de governos que *colecionam* falhas de segurança do Windows. *WannaCry* surgiu de uma vulnerabilidade descoberta pela agência de segurança dos EUA (e que foi vazada por *hackers*). *Tecnoblog*. 15 mai. 2017. Disponível em: <https://tecnoblog.net/214665/microsoft-nsa-cia-vulnerabilidades-windows-wannacry/>. Acesso em: 07 ago. 2017.

Em remate, no que tange à supracitada indagação, salientamos que em que pese o fato de o artigo 154-A do Código Penal trazer condutas mais específicas e adequadas à nova realidade social, amparado pela parte final da sanção prevista no §3º do aludido artigo, entendemos ser perfeitamente aplicável o parágrafo único do inciso IV do artigo 13 da pretérita Lei nº 7.170/83, tendo em vista a maior abrangência do bem jurídico tutelado por esta.

> §2º – Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
>
> §4º – Na hipótese do §3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
>
> §5º – Aumenta-se a pena de um terço à metade se o crime for praticado contra:
>
> I – Presidente da República, governadores e prefeitos;
>
> II – Presidente do Supremo Tribunal Federal;
>
> III – Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
>
> IV – dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

Nos aludidos parágrafos, temos as causas especiais de aumento de pena e em relação ao §2º, este apenas terá relação com o *caput* e o §1º do artigo 154-A, devendo ser aplicado na forma do artigo 68 do Código Penal. Quanto aos §§ 4º e 5º, estes são autoexplicativos. Os crimes do artigo 154-A se procedem mediante representação, salvo se o crime for cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios, ou empresas concessionárias de serviços públicos. Fator importante na referida lei é que a conduta em estudo diz respeito a um crime de menor potencial ofensivo. No entanto, diante da gravidade da conduta, há entendimento no sentido da aplicabilidade do crime de extorsão (art. 158 do CP)[38], com a devida vênia, não conjugamos com tal entendimento por entendermos que o art. 154-A é mais específico, tutelando bens jurídicos direcionados, e seria forçoso entender que há grave ameaça na estudada conduta.

Apesar de a Lei nº 12.737/12 ter adentrado em nosso ordenamento jurídico, temos assistido a ataques cada vez mais complexos, trazendo resultados desastrosos em diversos países, sem a devida identificação e punição desses cibercriminosos. O problema é global e a constante evolução tecnológica trará novos desafios aos

[38] CRESPO, Marcelo. *Ransonware e sua tipificação no Brasil*. Canal Ciências Criminais. 28 out. 2015. Disponível em: <http://canalcienciascriminais.com.br/ransonware-e-sua-tipificacao-no-brasil/>. Acesso em: 07 ago. 2017.

países, a conexão entre *ransomware* e IOT[39] (internet das coisas) ampliará o espectro criminal dessas organizações. A título de exemplo, citamos o ataque ao metrô de São Francisco, nos Estados Unidos, em 2016, onde criminosos invadiram o sistema, liberando as catracas e também furtando dados[40]. No mesmo ano, um hospital em Kansas (EUA) sofreu dois ataques que impediram os funcionários de terem acesso aos arquivos, prontuários médicos e arquivos financeiros do hospital[41]. No início deste ano (2017), um hotel na Áustria sofreu um ataque que invadiu o sistema de fechaduras eletrônicas, impedindo os clientes de entrarem ou saírem de seus quartos[42].

Em análise, percebemos que o tipo penal do art. 154-A descrito na Lei nº 12.737/2012 não alcança a realidade fática, uma vez que traz penas inexpressivas, em completa discrepância em relação aos danos causados. Noutro giro, percebe-se que o legislador pátrio ainda não se ateve à problemática em comento, pois em que pese ter criado no anteprojeto do novo Código Penal (PLS 236/2014) uma parte especial para os crimes cibernéticos (Título IV), o anteprojeto ainda se mostra desproporcional ao tamanho dos lucros auferidos e dos danos causados por um ataque de *ransomware*.

8. Conclusão

No presente estudo, pôde-se discorrer sobre a complexidade dos avanços tecnológicos, seus reflexos na vida social atual e como isso propiciou o aparecimento de novas condutas criminosas, bem como velhos tipos penais que ganharam novas roupagens. Aproveitando-se da rapidez tecnológica e da lentidão burocrática dos órgãos repressivos governamentais, organizações de cibercriminosos se estruturaram e passaram a movimentar vultosos valores com a conduta perpetrada no presente estudo.

Hodiernamente, ataques globais põem em risco todos os países em uma guerra silenciosa e, não obstante os ataques aos usuários privados, dados importantes de empresas e governos são coletados para os mais diversos fins. Percebeu-se que diversos mecanismos que propiciam o anonimato e a falta de informação dos usuários finais contribuem para o maior sucesso dos ataques por *ransomware*.

Noutro ponto, os tratados e acordos de cooperação internacional conjugados aos métodos de investigação das polícias judiciárias são importantes vetores no combate ao crime cibernético. No entanto, diferente do que ocorre com outros crimes

---

[39] A Internet das Coisas (do inglês, *Internet of Things*) é uma revolução tecnológica a fim de conectar dispositivos eletrônicos utilizados no dia-a-dia (como aparelhos eletrodomésticos, eletroportáteis, máquinas industriais, meios de transporte etc.) à Internet, cujo desenvolvimento depende da inovação técnica dinâmica em campos tão importantes como os sensores *wireless*, a inteligência artificial e a nanotecnologia.

[40] ROHR, Altieres. Metrô de São Francisco libera catracas após ataque por vírus de resgate. *G1*. 28 nov. 2016. Disponível em: <http://g1.globo.com/tecnologia/blog/seguranca-digital/post/metro-de-sao-francisco-libera-catracas-apos-ataque-por-virus-de-resgate.html>. Acesso em: 07 ago. 2017.

[41] Hospital de Kansas atingido por *ransomware,* extorquido duas vezes. *Blog Trend Micro.* 30 mai. 2016. Disponível em: <http://blog.trendmicro.com.br/hospital-de-kansas-atingido-por-ransomware-extorquido-duas-vezes/>. Acesso em: 07 ago. 2017.

[42] DEMARTINI, Marina. *Hackers* trancam quartos de hotel e exigem resgate em *bitcoin*. *Revista Exame*. São Paulo. 01 fev. 2017. Disponível em: < http://exame.abril.com.br/tecnologia/hackers-trancam-hospedes-em-hotel-e-exigem-resgate-em-bitcoin/>. Acesso em: 07 ago. 2017.

cibernéticos como a injúria racial praticada pela internet e a pornografia infantil, a prática do *ransomware* ainda não resultou em importantes condenações em nosso país.

Em análise, concluiu-se que a tipificação do ataque por *ransomware* disposta na Lei nº 12.737/2012 não se mostrou eficaz em combater o referido crime. Percebeu-se que o legislador pátrio ainda não está afinado com as transformações tecnológicas e suas implicações dentro do cibercrime. Ainda que o legislador tenha disponibilizado um título para os crimes cibernéticos no anteprojeto do novo Código Penal, as penas aplicáveis à estudada conduta são mínimas e não correspondem à gravidade dos danos causados, tanto às pessoas físicas e jurídicas, bem como à segurança político-econômica do país.

Referências

BARBAI, Marcos A. A criminalidade no espaço digital: a formulação do sentido. *In*: DIAS, Cristiane. *Formas de mobilidade no espaço e-urbano*: sentido e materialidade digital [*online*]. Série e-urbano. Vol. 2, 2013. Consulta no Portal Labeurb – http://www.labeurb.unicamp.br/livroEurbano/ Laboratório de Estudos Urbanos – LABEURB/ Núcleo de Desenvolvimento da Criatividade – NUDECRI, Universidade Estadual de Campinas – UNICAMP.

BARRETO, Alessandro Gonçalves; WENDT, Emerson; CASELLI, Guilherme. *Investigação digital em fontes abertas*. 1ª ed. Rio de Janeiro: Brasport Editora, 2017.

BLAT, Erick Ferreira *et al*. *Combate ao Crime Cibernético*. Ferramentas de investigação nos crimes cibernéticos utilizadas pela Polícia Federal. 1ª ed. Rio de Janeiro: M. Mallet Editora Ltda., 2016.

BRASIL. Secretaria Nacional de Justiça. Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional. *Manual de cooperação jurídica internacional e recuperação de ativos:* cooperação em matéria penal/Secretaria Nacional de Justiça, Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional (DRCI). 3ª ed. Brasília: Ministério da Justiça, 2014.

_____. *Lei nº 12.737*, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 30/jul./2017.

_____. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. *Livro verde*: Segurança cibernética no Brasil/Gabinete de Segurança Institucional, Departamento de Segurança da Informação e Comunicações; organização Claudia Canongia e Raphael Mandarino Junior. Brasília, 2010.

Carolina Dieckmann fala pela 1ª vez sobre fotos e diz que espera *justiça*. *G1*. São Paulo. 14/maio/2012. Disponível em: <http://g1.globo.com/pop-arte/noticia/2012/05/carolina-dieckmann-fala-pela-1-vez-sobre-roubo-de-fotos-intimas.html>. Acesso em: 30/jul./2017.

CEBRIÁN, Belén Dominguez. *Cibertaque*: o vírus *WannaCry* e a ameaça de uma nova onda de infecções. *El País*. Madri. 15 mai. 2017. Disponível em: <http://brasil.elpais.com/brasil/2017/05/14/internacional/1494758068_707857.html>. Acesso em: 20/maio/2017.

CRESPO, Marcelo. *Ransonware* e sua tipificação no Brasil. *Canal Ciências Criminais*. 28/out./2015. Disponível em: <http://canalcienciascriminais.com.br/ransonware-e-sua-tipificacao-no-brasil/>. Acesso em: 07/ago./2017.

DEMARTINI, Marina. *Hackers* trancam quartos de hotel e exigem resgate em *bitcoin*. *Revista Exame*. São Paulo. 01/fev./2017. Disponível em: <http://exame.abril.com.br/tecnologia/hackers-trancam-hospedes-em-hotel-e-exigem-resgate-em-bitcoin/>. Acesso em: 07/ago./2017.

FELIPE, Leandra. Cibercrimes causaram prejuízos de bilhões de dólares no mundo em 2016**.** *Corresp. Agência Brasil*. Estados Unidos. 31 mai. 2017. Disponível em: <http://agenciabrasil.ebc.com.br/geral/noticia/2017-05/cibercrimes-causaram-prejuizos-de-bilhoes-de-dolares-no-mundo-em-2016>. Acesso em: 05/jun./2017.

GRECO, Rogério. *Código Penal Comentado*. 7ª ed. Niterói, RJ: Impetus, 2013.

GROSSMANN, Luís Oswaldo. *Symantec* identifica ciberataques em 16 países com *malware* da CIA. *Convergência Digital*. 10 abr. 2017. Disponível em: <http://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=44938&sid=18>. Acesso em: 06/ago./2017.

GUIMARÃES, Fabiane. *A internet que ninguém via*. Metro. Associação Nacional dos Delegados de Polícia Federal. 30 dez. 2014. Disponível em: <http://www.adpf.org.br/adpf/admin/painelcontrole/materia/materia_portal.wsp?tmp.edt.materia_codigo=7235&tit=A-internet-que-ninguem-via#.WVsS6YjyvIV>. Acesso em: 03/jul./2017.

HIGA, Paulo. Microsoft reclama de governos que *colecionam* falhas de segurança do Windows. *WannaCry* surgiu de uma vulnerabilidade descoberta pela agência de segurança dos EUA (e que foi vazada por *hackers*). *Tecnoblog*. 15 mai. 2017. Disponível em: <https://tecnoblog.net/214665/microsoft-nsa-cia-vulnerabilidades-windows-wannacry/>. Acesso em: 07/ago./2017.

Hospital de Kansas atingido por *ransomware*, extorquido duas vezes. *Blog Trend Micro*. 30 mai. 2016. Disponível em: <http://blog.trendmicro.com.br/hospital-de-kansas-atingido-por-ransomware-extorquido-duas-vezes/>. Acesso em: 07/ago./2017.

JESUS, Damásio de; MILAGRE, José Antônio. *Manual de Crimes Informáticos*. 1ª ed. São Paulo: Editora Saraiva, 2016.

LISKA, Allan; GALLO, Timothy. Ransomware *(Defendendo-se da Extorsão Digital).* 1ª ed. São Paulo: Novatec Editora Ltda., 2017.

LUCHETE, Felipe; GALLI, Marcelo. Dez tribunais tiram *site* do ar após ataque cibernético mundial. *Revista Consultor Jurídico.* 12 mai. 2017. Disponível em: <http://www.conjur.com.br/2017-mai-12/dez-tribunais-tiram-site-ar-ataque-cibernetico-mundial>. Acesso em: 17/mai./2017.

NÚCLEO DE COMUNICAÇÃO SOCIAL. Nota de Esclarecimento sobre a rede de computadores do MP-SP. *Ministério Público do Estado de São Paulo*. 12/maio/2017. Disponível em: <http://www.mpsp.mp.br/portal/page/portal/noticias/noticia?id_noticia=16942683&id_grupo=118>. Acesso em: 17/maio/2017.

ROHR, Altieres. Metrô de São Francisco libera catracas após ataque por vírus de resgate. *G1*. 28/nov./2016. Disponível em: <http://g1.globo.com/tecnologia/blog/seguranca-digital/post/metro-de-sao-francisco-libera-catracas-apos-ataque-por-virus-de-resgate.html>. Acesso em: 07/ago./2017.

SANTANA, Felipe. 60% das pequenas empresas atingidas por vírus nos EUA vão à falência. *G1*. Nova Iorque, EUA. 13 mai. 2017. Disponível em: <http://g1.globo.com/mundo/blog/direto-de-nova-york/post/60-das-pequenas-empresas-atingidas-por-virus-nos-eua-vao-falencia.html>. Acesso em: 06/ago./2017.

SANTOS, Stenio Sousa *et al*. *Combate ao Crime Cibernético*. Contribuição crítica ao processo de investigação criminal da fraude bancária eletrônica: *Ubi societas, ibi criminis*? 1ª ed. Rio de Janeiro: M. Mallet Editora Ltda., 2016.

VERSIANI, José Augusto Campos *et al*. *Combate ao Crime Cibernético*. Cooperação Internacional na Investigação de Crimes Cibernéticos. 1ª ed. Rio de Janeiro: M. Mallet Editora Ltda., 2016.