Organização Comitê Científico
Double Blind Review pelo SEER/OJS
Recebido em: 29.11.2017
Aprovado em: 30.12.2017

Revista de Direito Penal, Processo Penal e Constituição

CIBERATAQUES EM MASSA E OS LIMITES DO PODER PUNITIVO NA TIPIFICAÇÃO DE CRIMES INFORMÁTICOS

Gladstone Avelino Britto[1]

Maristella Barros Freitas[2]

RESUMO

Um poderoso ciberataque desferido contra corporações em 2017 atingiu 99 países, Brasil incluído. Para liberar os sistemas afetados, o vírus gerou uma nota de resgate contendo instruções para pagamento aos cibercriminosos em Bitcoin, moeda digital cujo possuidor não pode ser rastreado. Investigações policiais para descobrir a autoria do crime foram frustradas. O artigo busca compreender, mediante uso da hermenêutica jurídica e da técnica de pesquisa bibliográfica de cunho exploratório com abordagem qualitativa, como o direito penal reagir a essa nova forma de criminalidade, respeitando os fundamentos constitucionais do poder punitivo.

Palavras-chave: crimes informáticos; Malware; Ransomware Petya

MASS CYBERATTACKS AND THE LIMITS OF PUNITIVE POWER IN THE LEGAL FRAMEWORK OF COMPUTER CRIMES

ABSTRACT

A powerful cyberattack against corporations in 2017 reached 99 countries, including Brazil. To release the affected systems, the virus generated a ransom note containing instructions for payment to cybercriminals in Bitcoin, a digital currency whose possessor cannot be traced. Police investigations to find out the perpetrator were thwarted. Cybercrime deflects more than $ 600 billion in fraud every year. The article seeks to understand, using legal hermeneutics and the technique of exploratory research with a qualitative approach, how criminal law reacts to this new form of crime, respecting the constitutional foundations of punitive power.

Keywords: computer crimes; Malware; Ransomware Petya

[1] Universidade Federal de Mato Grosso, Aluno do Programa de Mestrado em Economia pela UFMT
[2] Unicamp, Doutora em Política Científica

INTRODUÇÃO

De acordo com uma teoria que ficou conhecida como Lei de Moore, a cada 18 meses dobra a eficiência dos processadores de computadores. Esse extraordinário avanço técnico permitiu expandir os sistemas corporativos a partir do desenvolvimento em software (programas de computador, homepage, sistemas operacionais), que podem automatizar e interferir em praticamente todas as atividades sujeitas ao trabalho humano. O lado preocupante dessa tendência é que aumentou o risco de colapso na execução dessas atividades em decorrência de falhas que ocorrem por razões técnicas ou, principalmente, que possam ser induzidas dolosamente nos sistemas computacionais.

Entre maio e junho de 2017 um poderoso ciberataque atingiu 99 países. Pelas características do código malicioso introduzido nos computadores afetados, tem havido dificuldades para as autoridades policiais apresentarem elementos conclusivos de autoria nas investigações abertas para a identificação dos culpados. De concreto, sabe-se que a ação criminosa afetou o funcionamento de empresas e organizações estatais, hospitais, serviços de telefonia e grandes indústrias, atingindo, apenas no Brasil, um total de 15 estados. Tais ciberataques fizeram com que sites do Ministério Público Federal e do Tribunal de Justiça de São Paulo fossem afetados, o que motivou o desligamento de todas as máquinas do TJ no auge dos ataques, em maio. O mesmo ocorreu com os sistemas do Instituto Nacional do Seguro Social, também foram desligados preventivamente, prejudicando o atendimento aos segurados.

Dada a relevância do tema e a escassa produção acadêmica direcionada especificamente para essa nova forma de criminalidade, o objetivo da pesquisa foi investigar os aspectos técnicos e jurídicos envolvidos na temática, contribuindo com a epistemologia sobre esse aspecto de investigação criminal. E a metodologia empregada faz uso da técnica de pesquisa bibliográfica, de cunho exploratório e de abordagem qualitativa, visando analisar a questão proposta a partir dos aspectos do direito penal e de criminologia indicados no problema de pesquisa.

Diante de uma realidade que se manifesta hostil e potencializa os efeitos de ameaças virtuais, a partir de crimes cibernéticos que se praticam a todo o momento e colocam em risco o desenvolvimento das relações pessoais e comerciais, os problemas de pesquisa que motivam este trabalho foram direcionados para esclarecer: a) quais os meios utilizados nos ciberataques e suas características técnicas? b) Como o direito penal brasileiro e o internacional estão se instrumentalizando para a repressão penal de cibercrimes?

1 CONFIGURAÇÃO TÉCNICA EM CIBERATAQUES

A arquitetura da Internet, criada em 1969, tem sido consistentemente ampliada visando possibilitar o acesso rápido e fácil às informações disponibilizadas por servidores de dados do mundo inteiro para qualquer usuário, o que tem favorecido o anonimato de indivíduos que cometem crimes e conseguem escapar com facilidade da persecução penal.

Pode-se dizer que somente a partir dos anos 1990, com o desenvolvimento de softwares e computadores de mesa e, depois, laptops e dispositivos móveis de telefonia celular com melhorias significativas em capacidade de transmissão de dados e na adoção da tecnologia de pacotes, permitiu multiplicar exponencialmente o uso da Internet.

No entanto, ainda existe uma certa dificuldade técnica de se rastrear e localizar certos delinquentes cibernéticos, sobretudo aqueles capazes de ocultar os rastros de seu IP (Internet Protocol), o endereço capaz de identificar cada equipamento que acesse a Internet.

Diante de uma dura realidade em que se encontram instituições policiais, ministeriais e judiciarias, muitas das quais desprovidas de equipamentos de informática modernos e ou de quadro de pessoal capacitado e suficiente para a tarefa de perseguir e coibir o crime, há um certo prejuízo na instrução processual penal que conduziria à autoria do delito virtual (MALAQUIAS, 2015).

Nesse contexto, Roberto Antônio Darós Malaquias (2015) aponta para o prejuízo mundial anual da ordem de 575 bilhões de dólares causados pelos crimes cibernéticos, que figuram como um dos delitos que mais causam prejuízos à sociedade, equivalentes a 0,8% do PIB mundial, superados apenas pelo tráfico internacional de drogas, com 600 bilhões de dólares (MALAQUIAS, 2015).

1.1 Ataques de negação de serviço e softwares maliciosos

Causaram perplexidade, tanto a duração continuada do ciberataque de 2017 (dois meses até ser detido), quanto o fato de estar integrado com motivação financeira. Até aqui, a satisfação dos hackers estava centrada no status conquistado nos grupos de que fazem parte derivado de sucesso na derrubada dos sistemas operacionais e servidores de grandes corporações, muitas das quais fazem grandes investimentos em segurança digital.

O fato, supostamente, foi engendrado por hackers russos, hipótese levantada pela evidência de que os ataques foram disparados em horários compatíveis com o fuso horário comercial naquele país e, sobretudo, pelo fato de ter afetado mais severamente a Ucrânia, país com recente histórico de beligerância contra a Rússia (UNTERSINGER, 2017). Essa hipótese, contudo, é frágil, já que a própria Rússia também teve empresas afetadas pelo evento.

O que o recente ciberataque teve de inovador, em relação a outros atos dessa natureza, foi que aliou o típico objetivo dos hackers de derrubar sistemas à motivação em obter vantagens financeiras, bastante comum nos casos de criminosos voltados para lesar pessoas físicas. Quando a ação delituosa se volta apenas para dificultar o funcionamento de computadores pessoais ou de aparelhos de telefonia celular de particulares, nem sempre isso resulta em vantagem pecuniária para o infrator, pois há a possibilidade de substituição do equipamento travado, não tendo o agente criminoso como valorar os efeitos do dano, para fins de pedido de resgate.

Contudo, derrubar um sistema informatizado de uma empresa ou apagar seus registros de dados pode gerar danos econômicos severos, havendo alta probabilidade de que as exigências dos autores dos ataques sejam atendidas, conferindo maior eficácia na ação criminosa.

A derrubada temporária de sites na Web de grandes empresas ou de órgãos da administração pública se revelou como uma das primeiras manifestações dos hackers de que se tem notícia. Um ataque de negação de serviço, mais conhecida pela sigla em inglês DoS (*Denial of Service*) se caracteriza pela tentativa de interromper o fornecimento dos serviços virtuais. Basicamente, os hackers procuram exaurir algum recurso crítico associado ao serviço, tal como inundar um servidor de um gigantesco volume de requisições, a tal ponto que ele se torna incapaz de responder às requisições dos demais usuários.

Outra modalidade, derivado da primeira, são os ataques de negação a serviços distribuídos DDosS (*Distributed Denied of Service*), que é um sistema computacional estruturado em rede e que provoca perda de serviço por parte dos usuários.

A frequência e a sofisticação dos Ataques de Negação de Serviço têm aumentado exponencialmente, não obstante os esforços dos Fornecedores de Serviço das empresas e órgão públicos para controlarem e mitigarem ataques de DoS e DDoS. Sendo a Internet parte de uma infraestrutura internacional, sua característica de não ter fronteiras inviabiliza a completa proteção contra os ataques. Esses ataques podem ser diretos, de origem remota, ataques reflexivos, por meio de vermes (worms) ou de vírus.

A diferença entre esses últimos é que o vírus é um pedaço de código nocivo que reproduz na forma de outro código de máquina executável. Para que haja a infecção é preciso que haja a intervenção humana, do operador da máquina, para ser executado, enquanto que o verme roda automaticamente, pois o programa procura ativamente novas máquinas conectadas em rede para se infectar (STALLINGS, 2014).

Os ataques dos tipos DoS e DDoS tornam-se cada vez mais sofisticados à medida em que aumenta o nível de automação das máquinas. Os softwares (programas de computador) encontrados na Internet são frequentes hospedeiros de conteúdos infectados. Nos casos de computadores controladas remotamente a partir de redes de bots (robôs), centenas de computadores infectados pertencentes a terceiros podem ser usados, sem que seus usuários percebam.

Toda essa rede pode ser direcionada, por exemplo, para enviar milhares de e-mails simultaneamente a um determinado servidor, contribuindo para derrubá-lo. Os desenvolvedores voltados para atividades criminosas têm se esforçado para otimizar as características dos worms, no que diz respeito à sua propagação e rapidez de contágio (GRAÇA, 2013).

Conforme Pedro José Bentes Graça (2013), no caso dos ataques por meio de DoS ou DDoS e que visam restringir acesso de usuários por meio da Internet, isso ocorre porque várias máquinas saturam a largura de banda da vítima derrubando um ou mais servidores. Esses ataques assumem duas formas distintas: os ataques lógicos e os ataques com exaustão de recursos causados pela inundação de pedidos.

Os ataques lógicos exploram falhas de segurança que tornam o servidor ou o serviço em causa substancialmente mais lento. Já em ataques por inundação, os pacotes de dados enviados pelo agente criminoso são refletidos em outras máquinas infectadas, programadas para enviar os dados para a vítima multiplicados centenas de vezes, o que acarreta na derrubada dos sistemas (GRAÇA, 2013).

Os eventos aqui relatados são viabilizados pela propagação anterior de programas maliciosos, referido em inglês *Malicious Software* (Malware), que podem assumir a forma de

spammers, que atua faz a vítima atuar como robô, para o envio de grandes volumes de e-mail; Cavalo de Troia (Trojan), que executa aos olhos dos usuários uma função e, de modo oculto, captura autorizações legítimas e as envia ao criminoso; Spyware, o software espião, que coleta teclas digitadas e dados de tela e as envia ao criminoso, dentre outros.

Para realizar ataques do tipo DoS, o Malware opera um código que o ativa, com vistas maximizar o uso do processador, evitando que a vítima consiga fazer algum trabalho. Ao mesmo tempo, desencadeia erros no sistema operativo da máquina ou na ordem de sequência das instruções a serem executadas pelo CPU. Cria-se, assim, instabilidade do equipamento do usuário robô, levando-o à paralisia total (GRAÇA, 2013).

1.2 Atuação do vírus Ransomware Petya nos ciberataques de 2017

Nos ataques recentes foi utilizada uma espécie de vírus eletrônico, denominado de Ransomware Petya, na modalidade WannaCryptor, que explora falhas nos sistemas operacionais Windows e incorpora um vírus de resgate, que indica à corporação vítima o caminho para efetuar o pagamento do valor exigido pelos criminosos.

Caso a empresa afetada não pagasse uma quantia em Bitcoins, moeda digital utilizada em pagamentos eletrônicos e cuja titularidade não pode ser facilmente rastreada, estando cotada em agosto em, aproximadamente, US$ 600,00 por unidade, estaria a vítima afetada (em geral, pessoa jurídica) sujeita a ter inutilizados seus sistemas operacionais ou de dados.

O vírus Petya, que afetou grandes empresas de todo o mundo em 28 de junho de 2017 é mais perigoso e mais sofisticado que o vírus WannaCry, mas usa o mesmo princípio de propagação maciça através das redes locais. Apesar de ainda não se saber com certeza qual foi o primeiro equipamento infectado, nem como se infectou, sabe-se que esse novo malware usa a vulnerabilidade denominada de “EternalBlue”.

O desenvolvimento atual não só procura equipamentos vulneráveis, como também emprega ferramentas de administração para infectar todos os equipamentos de uma rede se, por acaso, encontra uma máquina com esses privilégios (PALAZUELOS, 2017).

Ransomware é um vírus de resgate, que embaralha os arquivos do computador, impedindo seu funcionamento normal. Para restaurar os arquivos e recuperar o sistema, a vítima precisa fazer um pagamento. De acordo com Aliaksandr Trafimchuk, da empresa israelense de desenvolvimento de softwares Check Point, o vírus utilizado na prática criminosa, denominado Petya, é uma espécie do gênero Ransomware que apareceu pela primeira vez na cena do crime cibernético no início de 2016. Embora o Petya não tenha uma taxa de infecção impressionante como outros recursos de armazenamento, como CryptoWall ou TeslaCrypt, foi imediatamente marcado como o próximo passo na evolução do Ransomware.

Os criminosos que desenvolveram o Petya não se contentaram com apenas criptografar todos os arquivos importantes encontrados nos discos rígidos das vítimas, mas também decidiram manter o conteúdo do disco rígido completo, criptografando sua tabela de arquivos mestre (MFT), de modo a tornar o sistema de arquivos completo inútil até que o resgate fosse pago (TRAFIMCHUK, 2016).

O Petya pode ser melhor descrito como um sistema de Ransomware de três estágios, onde cada etapa possui sua própria funcionalidade dedicada:

Quadro – rotina operacional de acionamento do vírus Petya

ETAPA	COMANDO	ROTINA
0	MBR Overwrite	Substituir o registro de inicialização mestre do disco rígido e implanta o boot-loader personalizado
1	MFT Encryption	Usar o carregador de inicialização personalizado introduzido no estágio 0 para criptografar todos os registros da Mestre-Tabela de arquivos (MFT), o que torna o sistema de arquivos completamente ilegível.
2	Ransom Demand	Exibe o logotipo da Petya e a nota de resgate detalhando o que deve ser feito para descriptografar o disco rígido.

Fonte: TRAFIMCHUK (2016) Decrypting the Petya Ransomware

No estágio inicial, o Petya gera um vetor de inicialização de 8 bytes, bem como uma chave aleatória de 16 bytes que é expandida para uma chave de criptografia de 32 bytes com um algoritmo simples. Se for possível parar o processo de execução depois que Petya é executado, mas antes que o sistema tenha reiniciado completamente, ainda é possível simplesmente reverter as operações que a Petya executou e restaurar a unidade para o estado anterior.

No estágio 1 é carregado o código de inicialização implantado no estágio 0. Se esta verificação retornar um valor positivo, o Petya começa a enumerar os registros da Módulo de arquivos mestre da unidade (MFT), enquanto se disfarça como um aplicativo legítimo de reparo de arquivos.

A etapa 2 da execução do vírus Petya ocorre quando a codificação MBR e MFT estiver concluída e o computador inicializa e exibe o logotipo do crânio assustador visto abaixo.

Depois que a vítima pressiona qualquer tecla, a nota de resgate que contém as instruções de pagamento e descriptografia é exibida.

Figura Estágio 2 "Demanda de resgate"

Fonte: TRAFIMCHUK (2016) Decrypting the Petya Ransomware

Temos aqui uma conduta que consiste em constranger a vítima, mediante grave ameaça (causar mal sério e verossímil). O constrangimento deve ser para coagir a fazer certa coisa (pagamento de resgate). O comportamento tem o intuito de obter indevida vantagem econômica.

A vantagem que o agente pretende conseguir deve ser indevida, como prevista no elemento normativo, e ter conteúdo econômico, o que caracteriza, também, o crime previsto no artigo 158 do Código Penal Brasileiro.

2 TIPOLOGIA JURÍDICA EM CRIMES CIBERNÉTICOS

Os aspectos da segurança de sistemas informatizados pressupõem a adoção ações de detecção, prevenção e recuperação de ataques a computadores e redes no nível operacional. Isso não prescinde a importância de adoção de ferramentas jurídicas e legais, sendo uma das mais importantes o fator de intimidação das leis. Os crimes de computador, ou cibercrimes, são nomes usados para descrever atividades criminosas nas quais as redes de computadores são uma ferramenta importante.

Tais crimes, basicamente, ocorrem tendo por alvo os computadores em si, em geral a partir de ataque à integridade de dados, confidencialidade e privacidade dos usuários; como fonte de armazenamento de arquivos pornográficos ou softwares pirateados; ou como ferramentas auxiliares para a prática de outros crimes, como a fraude de dados, interferência em sistemas ou falsificação de documentos.

2.1 Natureza e sujeitos do crime cibernético

Keniche Guimarães Matsuyama e João Ademar de Andrade Lima (2016) classificam os crimes cibernéticos nos tipos puros, mistos e comuns. Para os autores, o crime cibernético puro é aquele que descreve comportamentos ilícitos cujo objetivo é atacar o sistema computacional e seus componentes.

Conhecido pela palavra em inglês *hardware*, o sistema computacional é a parte física do equipamento, incluindo a Unidade Central de Processamento (CPU, que é o computador em si) e periféricos, e o *Software*, constituído pelos programas que executados pelos computadores. *Hardware* ainda abarca os dados e os sistemas em si. No crime cibernético puro, a investida do agente tem por objetivo atingir o equipamento físico, o sistema informático e as informações dos bancos de dados. Nessa modalidade, exemplificativamente, temos a invasão de servidores e sites.

No crime cibernético misto a ação criminosa está voltada para prejudicar o uso da Internet para que o intento delituoso possa se efetivar, conquanto o infrator vise bem jurídico distinto do informático. O agente não busca causar danos físicos ao sistema computacional ou a seus componentes. Nesse caso, o uso da tecnologia é ferramenta primordial para a concretude da ação delinquente, como dos ataques de negação de serviço.

Por fim, a conduta do agente que se vale da rede mundial de computadores tão somente como instrumento para efetivação de um crime já devidamente tipificado no Código Penal, caracterizando a modalidade de crime cibernético comum, como a fraude a contas bancárias ou cartões de crédito (MATSUYAMA, 2016).

De acordo com Carlos Araújo (2015), tem havido "*uma crescente preocupação da comunidade mundial com o abuso e a apropriação de informações eletrônicas e o uso de computadores para cometer crimes*". Em parte, isso deriva da tendência da substituição de documentos de papel (o processo eletrônico judicial, por exemplo), o que causa, para o autor, um grande impacto na natureza de crimes como o roubo, a fraude e a falsificação, com a

introdução do dinheiro eletrônico, das compras on-line a partir de sistemas de computadores privados.

Nesse ambiente, o autor sustenta que a disponibilidade de computadores e a confiança da comunidade no sistema de informações constituem valiosos recursos para que organizações criminosas potencializem o uso de tais equipamentos na prática de crimes, tais como os de fraude, a pornografia, as drogas, a pedofilia, os direitos autorais, a espionagem, transferências de tecnologias e o terrorismo eletrônico visando à derrubada de sistemas (ARAÚJO, 2015).

Há três formas de crimes praticados contra vítimas individuais: a primeira, tendo por objetivo de causas danos ou impedir o uso do equipamento, o que pode ocorrer sem que o criminoso obtenha vantagem financeira. A satisfação do criminoso ocorre no plano pessoal ou, provavelmente, dentro do círculo de relacionamentos que o cercam, com o reconhecimento por ter desenvolvido um programa destruidor.

Muitos ataques dirigidos a vítimas individuais têm um potencial destruidor além dos danos transmitidos ao equipamento, pois visam extrair informações, mensagens eletrônicas ou imagens pessoais da vítima, nos quais o objetivo do agente pode ser praticar extorsão ou cometer ações imputando fato ofensivo à reputação ofendido a partir da divulgação dos dados extraídos. Nesse segundo caso, a ação visa objetivos profissionais, comerciais ou eleitorais do autor ou do mandante do crime.

A terceira natureza de ação do invasor pode se dar por meio da obtenção de dados financeiros do agente passivo, constantes de suas contas correntes ou de cartões de crédito que estiverem armazenados em memórias de computadores pessoais, em tablets ou em dispositivos móveis de telefonia, proporcionando a prática de fraudes mediante saques indevidos.

Quanto aos crimes praticados contra sistemas de pessoas jurídicas, destacam-se, além das mesmas possibilidades previstas nas ocorrências com pessoas físicas, ações visando à "interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública, conforme assim o definiu o Art. 2º da Lei nº 12.737/2012, que inseriu no Código Penal parágrafo 1º do Art. 266, destinado a estabelecer punição para "*quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento*", que é o ato consistente a derrubar a rede telemática (Internet) em órgão que faça a prestação de serviço de público.

Há duas naturezas de agentes criminosos nos delitos de natureza cibernética. Conforme MALAQUIAS (2015) o primeiro tipo, denominado como Hacker, busca, por razões pessoais, demonstrar capacidade técnica em provocar danos com repercussão econômica ou midiática, sem buscar, necessariamente, obter intenção de obter vantagens financeiras ilícitas.

Outro tipo de agente provocador desses atos é denominado de Cracker, grupo constituído por exímios operadores de equipamentos de informática e profundos conhecedores de redes de comunicação e sistemas de segurança, como firewall ou criptografia e que podem atuar como piratas virtuais, penetrando remotamente em computadores integrados à rede (MALAQUIAS, 2015).

Em sua maioria, os crackers estão direta ou indiretamente ligados a estruturas de corporações, à contra inteligência de governos, atuam no campo da espionagem ou em empresas do ramo de produção de software para informática.

2.2 Marco legal na repressão para os crimes cibernéticos no Brasil

Os governos têm se mobilizado para deter ações terroristas, por meio de aperfeiçoamento em suas técnicas de investigação de delitos. Sobretudo, por uma maior rigidez na legislação, permitindo ações que produzem fortes restrições em garantias fundamentais, a exemplo da recente lei alemã que permitiu à polícia infiltrar vírus em equipamentos de indivíduos suspeitos, independentemente de autorização judicial. Essa tendência foi inaugurada pelos Estados Unidos, por meio da Patriot Act, no rescaldo dos ataques de 11 de setembro de 2001.

No Brasil, duas são as leis com impacto no sistema regulatório da informática. No plano da legislação civil, destaque para a Lei nº 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet.

No plano da legislação penal, a Lei nº 12.737, de 30 de novembro de 2012, que dispõe sobre a tipificação criminal de delitos informáticos, alterando o Decreto-Lei nº 2.848, de 7 de dezembro de 1940, o Código Penal vigente, não fez a distinção entre as formas entre crimes com objetivos coletivos e os crimes com alvos individuai. Tanto em um caso quanto no outro, o crime ocorre quando o agente:

> *Art. 154-A Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita*.

A respeito do artigo do Código Penal introduzido com a Lei nº 12.737/2012, o Juiz Federal Márcio Cavalcanti indagou em artigo que, "*se o agente invade o computador da vítima, lá instala um Malware (programa malicioso), descobre sua senha e subtrai valores de sua conta bancária, comete qual delito?*"

O magistrado defende que a lei não alterou o entendimento precedente que se trata de crime de furto mediante fraude, previsto no art. 155, § 4º, II, do Código Penal, uma vez que o art. 154-A prevê como crime invadir computador, mediante violação indevida de mecanismo de segurança, com o fim de instalar vulnerabilidades para obter vantagem ilícita, enquanto que o art. 155, § 4º, pune a conduta de subtrair coisa alheia móvel, no caso um valor monetário, mediante fraude perpetrada por meio virtual, uma vez que a finalidade do agente era a subtração, não tendo por objetivo a simples invasão. Aplica-se, no caso, o princípio da consunção, de forma a que a punição do agente ocorrerá apenas pelo crime de furto, ficando a invasão absorvida (CAVALCANTE, 2012).

Um aspecto controverso do tipo penal introduzido está na falta de adequada técnica criminal quando o legislador utilizou o verbo "invadir" para descrever a ação do agente. A palavra invadir, segundo consta do Dicionário Aurélio, significa penetrar de forma violenta em um determinado lugar e ocupá-lo pela força, ou seja, ocupar um lugar de forma maciça e abusiva. (HOLANDA, 2017). É certo que a invasão de um sistema informatizado não se faz com o uso da violência, o que agregaria um, fator de imprevisibilidade jurídica em termos de condenação baseada nesse tipo penal.

Ademais, observa-se no texto legal a ausência de definição de diversos termos técnicos inseridos na lei, dificultando a aplicação do tipo penal adequado. Em outra falha nessa

legislação, observa-se que somente disciplina as figuras típicas, ainda que de forma imprecisa, mas não contempla os meios processuais, o que prejudica a eficácia da norma.

Ciberataques, embora não tenham sido mencionados com tal nome na tipificação contida no Código Penal, artigo 154-A, constituem "Invasão de dispositivo informático", podendo ser considerados espécies do gênero crime cibernético, caracterizados pela ação típica, antijurídica e culpável e que necessitam de espaço virtual para serem praticados, sendo o computador pessoal ou a estação de trabalho do agente criminoso o instrumento para a prática do delito.

Preliminarmente, propõe-se estabelecer duas categorias de crimes cibernéticos, os primeiros aqueles ocorrem no plano coletivo, afetando muitas vítimas ao mesmo tempo, sendo dimensionados para superar defesas de sistemas corporativos, que possuem mecanismos de defesa antivírus mais potentes, o que gera efeitos mais impactantes. Essas ações são denominadas de ciberataques

Outro tipo de invasão a sistemas informatizados visam o usuário pessoa física, que pode ou não ter sistema antivírus instalado (dado o custo desses aplicativos, muitos usuários pessoas físicas não possuem). O usuário individual também não costuma seguir protocolos de segurança mais rígidos.

O mecanismo utilizado para a prática de ambas as formas de crimes, coletivos e contra particulares, também é o mesmo e consiste em introduzir vírus, códigos maliciosos hospedeiros, spam, mail-bomba, trojan horse para fins de praticar a captura de informações ou sua destruição, ou, simplesmente, para afetar o sistema operacional de modo a inviabilizar o uso do equipamento do usuário vítima.

Qual é, então, a utilidade de distinguir crimes cibernéticos cometidos contra particulares em pequena escala, daqueles praticados coletivamente, em geral quebrando defesas de sistemas corporativos robustos?

A razão é que os crimes cibernéticos coletivos ou ciberataques podem, em muitos casos, serem enquadrados na Lei nº 13.260, de 16 de março de 2016, que, regulamentando o disposto no inciso XLIII do art. 5o da Constituição Federal, disciplina o terrorismo, trata de disposições investigatórias e processuais e reformula o conceito de organização terrorista a partir da alteração das Leis nº 7.960, de 21 de dezembro de 1989, e nº 12.850, de 2 de agosto de 2013.

Desse modo, são considerados atos de terrorismo:

> *IV - **sabotar o funcionamento** ou apoderar-se, com violência, grave ameaça a pessoa ou **servindo-se de mecanismos cibernéticos**, do controle total ou parcial, ainda que de modo temporário, de meio de comunicação ou de transporte, de portos, aeroportos, estações ferroviárias ou rodoviárias, hospitais, casas de saúde, escolas, estádios esportivos, instalações públicas ou locais onde funcionem serviços públicos essenciais, instalações de geração ou transmissão de energia, instalações militares, instalações de exploração, refino e processamento de petróleo e gás e instituições bancárias e sua rede de atendimento.*

Cabe ressaltar que a Constituição Federal em seu artigo 5º, estabelece a existência de cinco tipos de crimes inafiançáveis, dentre os quais consta o terrorismo, no inciso XLIII. Como consequência, não se cogita o pagamento de fiança e consequente liberdade provisória do

envolvido em delito. Assim, o acusado por crime inafiançável deve, necessariamente, ficar preso durante toda a instrução processual.

Em relação às práticas de cibercriminosos de exigir pagamento das vítimas para a liberação de sistemas obstruídos, tal conduta, além de violar a Lei nº 12.737/2012 configura extorsão, que é o ato de obrigar alguém a tomar um determinado comportamento, por meio de ameaça ou violência, com a intenção de obter vantagem, recompensa ou lucro. É um crime assim tipificado no artigo 158 do Código Penal Brasileiro:

> *Art. 158 - Constranger alguém, mediante violência ou grave ameaça, e com o intuito de obter para si ou para outrem indevida vantagem econômica, a fazer, tolerar que se faça ou deixar fazer alguma coisa:*
>
> *Pena - reclusão, de 4 (quatro) a 10 (dez) anos, e multa.*

Conforme sustentam William Stallings e Laurie Brawn (2014), existe um ciclo vicioso que alimenta o cibercrime relacionado à relativa falta de sucesso dos titulares do poder repressivo do Estado, das polícias, do Ministério Público e do Poder Judiciário, expressa no relativamente baixo número de condenações criminais, frustrando um dos objetivos do direito penal, que é levar os criminosos a pagar pelos seus erros.

Aliado à globalização cibercrime, que permite a difusão internacional dos softwares maliciosos por meio das redes de grandes corporações multinacionais, observa-se um aumento na percepção de sucesso por parte dos cibercriminosos. Isso, aliado aos conhecimentos técnicos adquiridos pelos cibercriminosos com a experiência na prática delituosa e da relativa incompetência do Estado em acompanhar em tempo real o desenvolvimento de novas tecnologias no cibercrime, alimentam o ciclo vicioso que transmite a percepção e impunidade e ajuda a perpetuar as ocorrências criminosas (STALLINGS, 2014).

Por isso, Alessandra Mara de Freitas Silva e Cristian Kiefer da Silva (2013) defendem que a legislação penal no Brasil é incipiente, deixando de tutelar os bens jurídicos ameaçados (por exemplo, os dados armazenados). Portanto, é necessária a atuação eficaz dos órgãos competentes no enfrentamento dessa nova modalidade delitiva. Para os autores, enquanto houver falhas na legislação penal, não esses tipos penais não serão considerados crimes. Isso faz com que os cibercriminosos sejam "agraciados com o benefício da impunidade, pois no direito penal não se pode atribuir uma pena, ou impor uma sanção a uma conduta que o ordenamento penal não considere expressamente como criminosa", ainda que a conduta tenha como resultados prejuízos financeiros à vítima ou atente contra a integridade humana (SILVA, 2013).

2.3 Legislação internacional e proteção de garantias fundamentais

Christiano German (2002) sustenta que, como decorrência dos ataques ocorridos em 11 de setembro de 2001, foram introduzidas medidas por meio do US Patriot Act, o conjunto de leis americanas de reforço no combate ao terrorismo, em que foi implantado uma espécie de direito penal do inimigo, reforçando a competência dos serviços de inteligência na vigilância das pessoas e obtenção de dados que trafeguem na rede informatizada de dados.

No Título VIII do Patriot Act, que trata de Direito Penal e Terrorismo (Strengthening The Criminal Laws Against Terrorism), foram previstas penalidades aos que danifiquem

sistemas ou computadores governamentais ou façam acesso não autorizado a um computador protegido. Os ciberataques apresentam agravantes quando levam uma pessoa a ser ferida; promovam ameaça à saúde pública ou à segurança pessoal; afetem a administração da justiça, a defesa nacional ou a segurança nacional.

Também foi severamente tipificada a prática de atos de extorsão através de um computador protegido de empresas, associações, instituições educacionais, financeiras, entidade governamental ou outra entidade jurídica. A penalidade pela tentativa de danificar computadores protegidos através do uso de vírus ou outro mecanismo de software foi fixada em prisão fechada de 10 anos. Havendo reincidência, a nova pena se eleva para até 20 anos de prisão. Na seção 816, Development and support of cybersecurity Forensic capabilities. (Desenvolvimento e suporte da segurança cibernética - Capacidades forenses), o Ato também especificou o desenvolvimento e o suporte de capacidades de segurança cibernética. Além disso, a lei criou laboratórios forenses de computador regionais com a capacidade de realizar exames de evidências computadorizadas interceptadas relacionadas com atividades criminosas e ciberterrorismo, facilitando a partilha de conhecimentos técnicos dos funcionários públicos e de informações sobre a investigação, análise e repressão de crimes cibernéticos (UNITED STATES, 2001).

Outro marco legal internacional é a Convenção de Budapeste contra o Cibercrime, de 23 de novembro de 2001, com a adesão dos Estados Unidos e de grande parte dos países europeus, cujo tratado ainda não ratificado pelo Brasil. A Convenção estabeleceu instrumentos para proteger a sociedade das nações que a ela aderiram mediante a adoção de normas com foco na cooperação internacional, na convergência dos interesses comunitários europeus e na adoção de medidas destinadas a reduzir o risco de que a informação digital seja utilizada para o cometimento de delitos.

Alguns aspectos da Convenção giram em torno de tipificação de infrações cometidas contra a confidencialidade, a integralidade e a disponibilidade de dados em sistemas informáticos; a infrações relacionadas com computadores; preceitos de Direito Processual, considerando a adoção de medidas técnicas e legais para a preservação de dados. O principal ponto trata de conceder maior facilidade às investigações criminais, garantindo medidas cautelares e produção antecipada de prova.

Em Portugal a Lei nº 109, de 15 de setembro de 2009 estabeleceu as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas ao combate ao cibercrime. Além estabelecer, no artigo 2.º as definições dos termos utilizados, possibilitando dar mais clareza ao entendimento da lei (o que não ocorreu com a lei brasileira), tratou de aspectos relativos a falsidade cometida com uso da informática; às punições para quem praticar danos em dados informatizados; às ações de sabotagem com o uso de meios informatizados; acesso ilegal; reprodução indébita de programa protegido por direitos autorais; além das disposições processuais para a punição dos crimes nela previstos.

Em junho de 2017 o Bundestag (parlamento alemão) aprovou uma lei que permite às autoridades policiais instalar um sistema de escuta nos dispositivos móveis de suspeitos de terrorismo e atividade ilegais, para monitorar conversas em aplicativos de mensagens. Um dos principais aplicativos utilizados atualmente, WhatsApp, criptografa as mensagens enviadas, codificando o conteúdo e tornando-o indecifrável, inclusive pela polícia. A solução para que as autoridades alemãs antecipem os atos criminosos foi permitir a instalação remota, nos

smartphones dos suspeitos, de uma espécie de vírus que funcionaria como um programa espião, capaz de interceptar as mensagens enquanto forem digitadas, a intrusão (BLEIKER, 2017).

Na decisão do parlamento alemão, relator do projeto fez consignar que "a tarefa do processo penal é a comprovação (ou não) das alegações do Estado, legitimado para atuar na proteção dos interesses dos indivíduos que compõem a população, por meio de um processo capaz de garantir os direitos fundamentais, sem deixar de lado a preocupação central do julgamento criminal, que é a investigação dos fatos, sem a qual o princípio substantivo da culpa não pode ser realizado" (DEUTSCHLAND, 2017). Por isso, o projeto contém numerosas propostas para simplificar as exigências judiciais no processo de investigação, sem contaminar o processo penal por nulidades, e, ao mesmo tempo, garantir velocidade na aplicação da justiça.

Contudo, conforme alertam Harold Abelson *et al* (2015), os mecanismos do mesmo recurso utilizado pelas autoridades policiais podem ser usados pelos cibercriminosos. Os autores entendem que, mesmo que os cidadãos necessitem de uma aplicação da lei para se protegerem no mundo digital, todos os decisores políticos, (governos, legisladores e aplicadores do direito) têm a obrigação de trabalhar para tornar a nossa infraestrutura de informação global mais segura, confiável e resiliente.

Os autores entendem que a aplicação de lei que permita acesso excepcional a comunicações privadas e dados mostra abrirá portas através das quais criminosos e estados-nação mal-intencionados também possam atacar os próprios indivíduos que a lei busca defender. Os custos seriam substanciais, o dano à inovação severa e as consequências para o crescimento econômico difícil de prever (ABELSON, 2015).

Ainda que a lei alemã não tenha ordenado a quebra da criptografia dos comunicadores, não há como garantir que essa possibilidade esteja fechada aos criminosos (BLEIKER, 2017).

Assim, os que promovem decisões no plano políticos precisam ser claros na avaliação dos prováveis custos e benefícios. Quando se pensam em modificações na lei para os fins de aperfeiçoar a investigação criminal com acesso excepcional a dados protegidos por sigilo, os autores sugerem que as autoridades forneçam robustas evidências para documentar seus pedidos e, em seguida, apresentem detalhamento do que a autoridade policial espera com os mecanismos de acesso excepcional de que farão uso (ABELSON, 2015).

Ao estudar as circunstâncias que amparam a adoção de medidas excepcionais, Sérgio Moccia sustentou que a ideia de emergência pode ser atrelada à de urgência e de crise, colocando em xeque os padrões normais de comportamento e a possibilidade de manutenção das estruturas. Nesse sentido, a emergência requer uma resposta pronta, imediata e que, substancialmente, deve durar enquanto o estado emergencial perdurar (MOCCIA. 1999).

Para Luigi Ferrajoli (2010), a emergência que ampara as medidas excepcionais pode ser apresentada de duas formas distintas e simultâneas: a legislação de exceção no que diz respeito à Constituição e as mutações legais das leis do jogo. A jurisdição de exceção, por sua vez, deriva da legalidade alterada. Para o autor, em ambas se percebe que os valores dominantes em face da suposta necessidade de resposta ao fenômeno emergente, com a implícita insinuação da fraqueza da cultura da normalidade. Com efeito, o Sistema Garantista defendido por Ferrajoli tem pilares firmados sobre dez axiomas fundamentais, que, ordenados, conectados e harmonizados sistemicamente, determinam as "regras do jogo fundamental" de que se incumbe o Direito Penal e, também, o Direito Processual Penal.

Contrapondo-se a isso, CALABRICH *et al* (2010) defendem que o garantismo, que é uma visão do Direito Constitucional aplicada no Direito Penal e Direito Processual Penal, deve ser aplicado de uma forma ampliada, sendo equivocado quando enxerga apenas os direitos fundamentais do réu, ou seja, priorizando apenas um lado do processo. Contra isso propõem um Garantismo penal Integral, que visa resguardar os direitos fundamentais não só dos réus, mas também das vítimas.

CONSIDERAÇÕES FINAIS

Os crimes cibernéticos não são um fenômeno jurídico recente, mas seu volume e consequências tem se tornado cada vez maior, acompanhando a própria evolução da Internet e dos sistemas de automação na sociedade.

O cibercriminoso, antes um agente apenas motivado pelo prazer em burlar esquemas de segurança computacional, hoje descobriu um filão para ganhar dinheiro fácil. Com isso, travam uma guerra silenciosa contra os programadores das corporações financeiras, empresariais e dos governos, além dos desenvolvedores de programas de combate a Malware.

A cada falha descoberta em sistemas pelos hackers, os responsáveis pela atualização de sistemas operacionais e aplicativos buscam um remédio para corrigi-la. A impunidade nesse campo gera efeitos econômicos adversos e desafia a ação de governos no sentido de aperfeiçoamento da legislação repressora das condutas criminosas, além de exigir aparelhamento técnico e capacitação dos agentes do estado para enfrentar esse desafio.

O que existe na legislação penal brasileira ainda é incipiente para um combate eficaz, faltando no ordenamento jurídico penal elementos para preencher lacunas legislativas ou melhorar a qualidade técnica da legislação. Se a Lei n° 12.737/2012 representou um avanço na atualização dessa legislação, tipificando novas condutas, não o fez adequadamente, inclusive mostrando-se carente de elementos do direito processual penal que possam dar efetividade aos parcos tipos de direito material nela inseridos.

Assim, existe uma demanda da sociedade brasileira por eficiência no processo de persecução dos atos praticados pelos cibercriminosos, inclusive por meio do monitoramento antecipado das ações dos criminosos, de modo a evitar o mal maior do fato consumado. Em busca dessa eficácia, a nova legislação alemã de combate aos crimes informáticos, que permite à autoridade policial atuar em dispositivos individuais apenas mediante ordem judicial, representa um avanço sobre os programas de vigilância americanos, feitos em massa e sem autorização judicial.

A observância dos procedimentos de garantismo integral, com o endurecimento das medidas penais e processuais, mantendo-se o respeito aos direitos fundamentais dos acusados, é o caminho que vai permitir conciliar o interesse público, no sentido da produção de efetiva persecução penal, com o respeito aos direitos fundamentais inseridos na Constituição.

REFERÊNCIAS

ABELSON, H. *et al*. Keys Under Doormats: mandating insecurity by requiring government access to all data and communications. Cambridge, **MIT-CSAIL.** TR-2015-026 July 6, 2015. Disponível em: https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf. Acesso em: 07 ago. 2017.

ARAÚJO, C. G. **Aspectos nacionais e internacionais dos crimes de informática**. Portal de e-governo, inclusão digital e sociedade do conhecimento. Florianópolis: UFSC, 2015. Disponível em: http://www.egov.ufsc.br/portal/conteudo/aspectos-nacionais-e-internacionais-dos-crimes-de-inform%C3%A1tica. Acesso em: 07 ago. 2017.

BLEIKER, C. New surveillance law: German police allowed to hack smartphones. **Deutsche Welle**. 22 jun. 2017. Disponível em: http://www.dw.com/en/new-surveillance-law-german-police-allowed-to-hack-smartphones/a-39372085. Acesso em: 07 ago. 2017.

CALABRICH, Bruno; FISCHER, Douglas; PELELLA, Eduardo. **Garantismo penal integral: questões penais e processuais, criminalidade moderna e a aplicação do modelo garantista no Brasil**. Salvador: *Jus*PODIVM, 2010.

CAVALCANTE, M. A. L. Primeiros comentários à Lei n. º 12.737/2012, que tipifica a invasão de dispositivo informático. **Dizer Direito**, 14 dez. 2012. Disponível em: http://www.dizerodireito.com.br. Acesso em: 08 ago. 2017.

DEUTSCHLAND. Bundestag. **Entwurf eines Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens**. Berlin, 2017. Disponível em: http://dip21.bundestag.de/dip21/btd/18/112/1811277.pdf . Acesso em: 07 ago. 2017.

FERRAJOLI, L. **Direito e razão**: teoria do garantismo penal. 3.ed. rev. São Paulo: Editora Revista dos Tribunais, 2010.

GERMAN, C. As novas leis de segurança na Alemanha e nos Estados Unidos: os efeitos para a comunicação global**. Revista CEJ**, Brasília, nº 19, p. 78-84, out/dez/2002.

GRAÇA, P. J. B. O **Ciberataque como Guerra de Guerrilha**: O Caso dos Ataques DoS/DDoS à Estônia, Geórgia e ao Google China. 2013. 74 f. Dissertação (Mestrado em Estratégia). Instituto Superior de Ciências Sociais e Políticas. Universidade de Lisboa, Lisboa, 2013.

HOLANDA, A. B. **Dicionário Aurélio da Língua Portuguesa**. Curitiba: Positivo Editora, 2010.

MALAQUIAS, R. A. D., 2015. **Crime cibernético e prova**: a investigação criminal em busca da verdade. Curitiba: Juruá, 2015.

MATSUYAMA, K. G.; LIMA, J. A. A. **Crimes cibernéticos**: atipicidade dos delitos. Disponível em: http://www.cedipe.com.br/3cbpj/docs/artigos_pdf/11_crimes_ciberneticos_atipicidade_dos_delitos.pdf. Acesso em: 07 ago. 2017.

MOCCIA, S. Emergência e defesa dos direitos fundamentais. **Revista Brasileira de Ciências Criminais**, ano 7, n. 25, jan-mar, 1999, p. 58/91.

PALAZUELOS, F. Vírus Petya é mais perigoso e mais sofisticado que WannaCry**. El País,** 28 jun. 2017**.** Disponível em:

https://brasil.elpais.com/brasil/2017/06/28/tecnologia/1498639459_556568.html. Acesso em: 07 ago. 2017.

SILVA, A. M. F.; SILVA, C. K. O problema da tipificação dos crimes informáticos: aspectos controversos a respeito da aplicação do artigo 154-A da Lei nº 12.737/2012, Lei Carolina Dieckmann. **Anais.** XXIII Conpedi, Direito Penal, Processo Penal, João Pessoa, 2013, p. 394 - 419.

STALLINGS, W.; BROWN, L. **Segurança de computadores**: princípios e práticas. Rio de Janeiro: Elsevier, 2014

TRAFIMCHUK, A. **Decrypting the Petya Ransomware.** Check Point Software, Tel Aviv, 2016. Disponível em: https://blog.checkpoint.com/2016/04/11/decrypting-the-petya-ransomware/. Acesso em: 07 ago. 2017.

UNITED STATES. Uniting and strengthening America by Providing appropriate tools required to intercept and obstruct terrorism (USA Patriot Act). **Public Law** 107-56, oct. 26, 2001. Disponível em: https://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf. Acesso em: 07 ago. 2017.

UNTERSINGER, M. ; LELOUP, D. ; REYNAUD, F. Le virus Petya paralyse entreprises et administrations à travers le monde. **Le Monde**, 27 jun. 2017. Disponível em: http://www.lemonde.fr/pixels/article/2017/06/27/un-virus-informatique-paralyse-entreprises-et-administrations-dans-plusieurs-parties-du-monde_5151918_4408996.html . Acesso em: 07 ago. 2017.