CRIMES PRATICADOS NA *DARK WEB* E A DIFICULDADE DE RESPOSTA ESTATAL

CRIMES PRACTICED ON THE DARK WEB AND THE DIFFICULTY OF STATE RESPONSE

Kennedy Josué Greca de Mattos[1]

RESUMO

A facilidade da troca de informações via Internet tanto traz facilidade para uma rápida comunicação e agilidade no ramo de negócios, quanto pode colocar a privacidade, intimidade e a segurança das pessoas em risco. O avanço tecnológico traz benefícios, entretanto diversas práticas ilegais e criminosas encontram um lugar propício para sua proliferação. O presente artigo trata dos crimes praticados na dark web, a parte mais profunda da internet, ambiente marcado pelo uso da criptografia e do anonimato de seus usuários. Nesse sentido, busca-se compreender que o aumento dos crimes cibernéticos se torna cada vez mais evidente e a legislação atual nacional não demonstra ser suficientemente efetiva para coibir a atuação desses criminosos. Dessa forma, como afirmam Rezer e Fortes, sabendo que a sociedade de risco continuará convivendo com o crescimento tecnológico, e que não há como pará-lo, necessita-se de legislações que protejam os usuários e que delimitem até onde esses avanços podem evoluir. Atualmente não há uma legislação brasileira específica para a proteção dos usuários das "coisas", conectadas a internet. Assim, surge a oportunidade de pautar esse tema para a criação de novas leis, sem aguardar que impactos extremos aconteçam.

Palavras-chaves: Dark web. Crimes cibernéticos. Tipificação específica criminal.

ABSTRACT

The ease of exchanging information via the Internet both facilitates quick communication and agility in the business sector, as well as putting the privacy, intimacy and security of people at risk. Technological advances bring benefits, however, several illegal and criminal practices find a favorable place for their proliferation. This article deals with crimes committed on the dark web, the deepest part of the internet, an environment marked by the use of cryptography and the anonymity of its users. In this sense, we seek to understand that the increase in cyber crimes is becoming increasingly evident and the current national legislation does not prove to be effective enough to curb the actions of these criminals. Thus, as stated by Rezer and Fortes, knowing that the risk society will continue to live with technological growth, and that there is no way to stop it, there is a need for legislation that protects users and limits how far these advances can evolve. Currently, there is no specific Brazilian legislation for the protection of users of "things", connected to the internet. Thus, the opportunity arises to guide this theme for the creation of new laws, without waiting for extreme impacts to happen.

Keywords: Dark web. Cyber crimes. Specific crimes typification.

INTRODUÇÃO

A história da internet conta que, nos primórdios, a ferramenta era exclusivamente de uso militar e científico, sendo seu acesso de uso limitado à grande parte da população. Não é por outro motivo que os primeiros crimes praticados nesse ambiente surgiram somente nos anos 60, quando os criminosos passaram a usar o conhecimento tecnológico adquirido para acessar informações

[1] Doutorando no Programa de Direitos Fundamentais e Democracia do Centro Universitário Autônomo do Brasil.

sigilosas de usuários e de grandes empresas de diferentes ramos de negócio, assim "(...) ocorreram as primeiras referências sobre essa modalidade de crimes com as mais diversas denominações, inclusive maior incidência em casos de manipulação e sabotagem de sistemas de computadores".[2]

Nos anos 80, surge o termo *internet* como "(...) um conjunto de redes de computadores interligadas pelo mundo inteiro, que têm em comum um conjunto de protocolos e serviços, possuindo a peculiaridade de funcionar pelo sistema de trocas de pacotes e cada pacote pode seguir uma rota distinta para chegar ao mesmo ponto"[3]. E, somente nos anos 90, é que a exploração comercial da internet teve início, devido à invenção da *world wide web* (www), como um pacote de informações em formato de texto ou mídia, organizado de forma a que o usuário pudesse acessar as páginas na rede, ou seja, navegar nos sites, a partir de sequências associativas denominadas *hiperlinks* entre blocos vinculados por remissões[4].

Contudo, na medida em que a internet ganhava popularidade como uma ferramenta tecnológica aplicada na indústria, no comércio, nas profissões liberais, nas relações interpessoais, transformando a vida em sociedade, os crimes cibernéticos foram surgindo e aumentando exponencialmente.

Com a evolução da internet em território nacional, estatísticas demonstram que o número de domicílios com acesso à rede é de 74,9%, estando amplamente disseminada entre todas as regiões do Brasil[5]. Dessa forma, é sabido que o acesso à web em nosso país tem significado uma importante ferramenta tanto para comunicação entre pessoas como para impulsionar mundo dos negócios.

No entanto, em que pese o mundo virtual representar um avanço tecnológico para o Brasil, há um aumento vertiginoso de prática de ilícitos, o que sem dúvida constitui um novo desafio para a ciência do direito, diante da necessidade de adequação dos tipos penais tradicionais aos praticados no âmbito digital.

A pesquisa desenvolvida no presente artigo diz respeito à tipificação dos crimes virtuais ocorridos na dark web e a necessidade da existência de um código

---

[2] Carneiro, Adeneele Garcia. "Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação". Âmbito Jurídico. Disponível em: http://www.ambito-juridico.com.br/site/index.php/?n_link=revista_artigos_leitura&artigo_id=11529&revista_caderno=17. Acesso em: 17 de abril de 2020. p. 01.
[3] Rosa, Fabrízio. "Crimes de informática". Campinas: Bookseller, 2007.
[4] Ministério Público Federal. "Crimes cibernéticos: manual prático de investigação". São Paulo: Procuradoria da República de São Paulo: 2006, p. 04.
[5] Ibge – Instituto Brasileiro De Geografia E Estatística. "Uso de internet, televisão e celular no Brasil". Disponível em: https://educa.ibge.gov.br/jovens/materias-especiais/20787-uso-de-internet-televisao-e-celular-no-brasil.html. Acesso em: 20 de abril de 2020.

penal próprio aos cybers crimes, vez que a resposta estatal parece não atender satisfatoriamente aos anseios dos cidadãos de forma a coibir o aumento de incidentes criminosos na rede.

1 DA SURFACE WEB À DARK WEB

Podemos dizer, que existem basicamente duas partes na internet: a surface web, parte acessível a todos os usuários através de um programa de navegação padrão; e a deep web, esta um espaço muito maior, com dados não registrados, no qual seu acesso é muito mais restrito. Nesse sentido, conforme explicam os autores Pompéo e Seefeldt, a busca na web se dá justamente mediante as duas categorias "(...) a) a primeira delas é a conhecida como surface web (podendo ser chamada também de clearnet); e b) enquanto a segunda é o que especialistas de sistemas de informação chamam de deep web".[6]

Segunda a definição de Chris Sherman e Gary Price, a invisible web, termo usado pelos autores para se referirem à deep web, é o universo quase intangível onde existem milhares de páginas de textos, arquivos e outras variadas mídias, cujos motores de buscas gerais não podem, seja por limitações técnicas, seja por não quererem, por escolha deliberada, incluir aos seus índices de pesquisa. Os autores ainda afirmam que o que é invisível hoje, pode se tornar visível futuramente, principalmente com a evolução da tecnologia dos mecanismos de buscas[7].

Ainda como assevera Pompéo e Seefeldt, "a expressão deep web foi criada por Michael K. Bergman, fundador do programa Bright Planet, software especializado em coletar, classificar e procurar conteúdo nessa esfera da web". [8]Sendo assim, essa expressão de deep traz uma ligação à profundeza, enquanto que surface se limita àquilo que está na superfície.

Dessa forma, a deep web normalmente é associada como um espaço obscuro na internet, onde há a ocorrência de crimes dos mais variados tipos reunidos em um território aparentemente sem lei. Com efeito, a deep web não é

---

[6] Pompéo, Wagner Augusto; Seefeldt, João Pedro. Nem tudo está no Google: deep web e o perigo da invisibilidade. In: Congresso Internacional de Direito e Contemporaneidade. Santa Maria: UFSM, 2013, p. 439.

[7] Sherman, Chris; Price, Gary. The invisible web: uncovering information sources search engines can't see. Illinois: Cyberage Books, 2003, p. 283.

[8] Pompéo, Wagner Augusto; Seefeldt, João Pedro. Nem tudo está no Google: deep web e o perigo da invisibilidade. In: Congresso Internacional de Direito e Contemporaneidade. Santa Maria: UFSM, 2013, p. 440.

acessível facilmente a todos que navegam na internet, pois a maioria das pessoas não sabe de que forma entrar ou explorar esse mundo virtual.

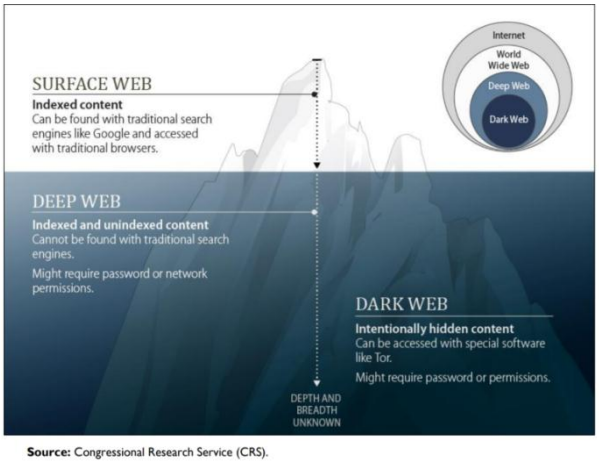
No que diz respeito ao tamanho desse universo virtual, Michael Bergman afirma que

> (...) informações públicas na Deep Web são comumente de 400 a 500 vezes maior que as definidas da World Wide Web . A Deep Web contém 7.500 terabytes de informações comparadas a 19 terabytes de informação da Surface Web . A Deep Web contém aproximadamente 550 bilhões de documentos individuais comparados com 1 bilhão da Surface Web. Existem mais de duzentos mil sites atualmente na Deep Web . Seis das maiores enciclopédias da Deep Web contém cerca de 750 terabytes de informação, suficiente para exceder o tamanho da Surface Web quatro vezes. Em média, os sites da Deep Web recebem 50% mais tráfego mensal, ainda que não sejam conhecidos pelo público em geral. A Deep Web é a categoria que mais cresce no número de novas informações sobre a Internet. Deep Web tende a ser mais estrita, com conteúdo mais profundo, do que sites convencionais. A profundidade de conteúdo de qualidade total da Deep Web é de 1.000 a 2.000 mil vezes maior que a da superfície. O conteúdo da Deep Web é altamente relevante para todas as necessidades de informação, mercado e domínio. Mais da metade do conteúdo da Deep Web reside em tópicos específicos em bancos de dados. Um total de 95% da Deep Web é informação acessível ao público não sujeita a taxas ou assinaturas (...).[9]

Indo bem mais a fundo na deep web, chega-se a um conteúdo que só pode ser acessado através do uso de um programa próprio. A esse espaço dá-se o nome de dark web, um segmento intencionalmente escondido da deep web[10].

Uma ilustração de toda essa estrutura da web pode ser interessante para melhor visualizá-lo:

Figura 1[11]:



Source: Congressional Research Service (CRS).

[9] Bergman apud Pompéo, Wagner Augusto; Seefeldt, João Pedro. Nem tudo está no Google: deep web e o perigo da invisibilidade. In: Congresso Internacional de Direito e Contemporaneidade. Santa Maria: UFSM, 2013, p. 441.

[10] Flinkea, Kristin. Dark Web. Congressional Research Service. 2017, p. 02

[11] Idem, p. 6. Tradução: Surface web: conteúdo indexado. Pode ser encontrado através de mecanismos de pesquisas tradicionais, como Google, e acessado através de navegadores padrões. Deep web: conteúdo indexado e não indexado. Não pode ser encontrado através de mecanismos de busca convencionais. Pode ser preciso senha ou permissão de rede. Dark web: conteúdo intencionalmente escondido. Pode ser acessado somente com programas especiais como Tor. Pode ser preciso senha ou permissão.

A ferramenta para que se possa acessar o conteúdo da dark web é através da instalação de um programa específico para navegação, a exemplo do Tor, software mais usado para esse fim, o qual, segundo Andy Beckett, seu desenvolvimento inicial era direcionado ao Laboratório de Pesquisa Naval Americano, no intuito de proteger a comunicação governamental[12].

Sabe-se, ademais, que devido ao anonimato que o Tor proporciona ao usuário, muito do que acontece na dark web é feito através desse programa, desde a prática criminal até trocas de mensagens e informações entre pessoas residentes em países totalitários.

No que tange ao funcionamento do programa, Silveira explica que "(...) o Tor distribui a comunicação através de uma rede de voluntários transmissores ao redor do mundo, impedindo o monitoramento da conexão, dos sites acessados e evitando que se descubra a localização física dos interagentes."[13]

Assim, o uso positivo da ferramenta acontece quando, por exemplo, alguns jornalistas o utilizam para se comunicarem de forma mais segura com suas fontes; ou quando as organizações não governamentais utilizam-no para que colaboradores de outros países possam se conectar e trabalhar de forma segura e não rastreável; ou quando grupos de ativistas, como a Electronic Frontier Foundation (EFF) usam-no como um mecanismo para manter as liberdades civis online asseguradas[14].

Outrossim, muito embora a dark web possibilite também outros benefícios, como a liberdade de expressão àquelas pessoas que não possam exercê-la por causa do regime totalitário em que vivem, é fato que, para países democráticos, segundo Duarte e Mealha, a utilização da ferramenta como meio para a prática de crimes tem sido alarmante e urgem medidas rápidas no intuito de coibi-los satisfatoriamente:

> É aqui que chegamos ao centro do debate: por um lado o Tor permite, entre outras coisas, assegurar a privacidade das comunicações entre utilizadores e visualizar artigos e blogs que não se encontram na Surface Web; por

[12] Beckett apud Monteiro, Silvana Drumond; FIDENCIO, Marcos Vinicius. As dobras semióticas do ciberespaço: da web visível à invisível. TransInformação , v. 25, n.1, p. 35-46, jan./abr. 2013. Disponível em: http://www.scielo.br/pdf/tinf/v25n1/a04v25n1.pdf. Acesso em: 16 de abril de 2020, p. 43.

[13] Silveira, Sergio Amadeu. A Internet e o novo Cavalo de Tróia. Rio de Janeiro: PoliTICs, n. 10, ago. 2011.p. 6.

[14] Tor Project: anonymity online. Disponível em: https://www.torproject.org/. Acesso em: 22 de abril de 2020

> outro lado o anonimato serve de ferramenta para que ocorra a prática de atividades ilícitas. Existe uma linha muito tênue que separa a esfera pública da esfera privada. O Tor permite reforçar a segurança ao utilizar a Internet. Cabe ao bom senso de cada um a forma como utiliza as ferramentas ao seu dispor. [15]

Segundo pesquisas, os conteúdos que mais são acessados na dark web são os de pornografia infantil, os de tráficos de órgãos e os de mercado negro. Nota-se um aumento do número de visualizações também em páginas que divulgam documentos sigilosos do governo como o WikiLeaks, os de troca de moedas como bitcoins e de tutoriais para fraude virtual[16].

Os bitcoins, aliás, vêm se tornando cada vez mais uma moeda de negociação, tendo sido "inventada e partilhada em 2009 pelo japonês Satoshi Nakamoto, sendo uma moeda encriptada que todas as pessoas podem adquirir em troca de dinheiro, produtos ou serviços. O número de pessoas a utilizar este método vem crescendo largamente e uma das razões para tal é o facto das taxas de pagamento serem de 2 a 3% mais baratas do que o pagamento por cartão de crédito. Ao contrário do método tradicional, as taxas são suportadas pelo comprador, e não pelo vendedor."[17]

Sendo assim, o bitcoin, segundo Ulrich, é "resultado de mais de duas décadas de pesquisa e desenvolvimento por pesquisadores praticamente anônimos". Ainda, segundo o autor, o sistema representa um avanço importante no sistema cambial digital, "(...) cujo desenvolvimento foi possibilitado por vinte anos de pesquisa em moedas criptográficas e quarenta anos de pesquisa em criptografia por milhares de pesquisadores ao redor do mundo."[18]

Uma das principais vantagens do bitcoin está na redução dos custos das transações. Assim, Ulrich afirma que não há fronteiras políticas à moeda digital:

> Você pode enviar e receber Bitcoins de qualquer lugar a qualquer pessoa, esteja ela onde estiver, sem ter que ligar ao gerente do banco, assinar qualquer papel, comparecer a alguma agência bancária ou ATM. Nem mesmo precisa usar VISA ou PayPal. Você pode ter domicílio no Brasil, estar de férias em Xangai e enviar dinheiro a uma empresa na Islândia com a mesma facilidade com que envia um e-mail pelo seu iPhone. [19]

---

[15] Duarte, David; Mealha, Tiago. Introdução à deep web. Lisboa: IET Working Papers Series, 2016, p. 2.
[16] Idem, p. 11.
[17] Idem, p. 12.
[18] Ulrich, Fernando. Bitcoin: a moeda na era digital. São Paulo: Instituto Ludwig von Mises Brasil, 2014, p. 44.
[19] Idem, p. 63.

Apesar de toda tecnologia objetivar boas, modernas e desburocratizadas práticas de negociação, acordos e trocas de informações, o que se vê é uma redefinição dos crimes tradicionais em relação à plataforma virtual possibilitada pelo anonimato que a dark web traz.

2 A DIFÍCIL TIPIFICAÇÃO DOS CRIMES CIBERNÉTICOS ASSOCIADOS À DARK WEB NO BRASIL

Segundo o site Safernet Brasil, os crimes cibernéticos mais praticados são os de intolerância religiosa, violação de direitos autorais, contra a honra e o patrimônio, pornografia infanto-juvenil, racismo e xenofobia[20]; todos esses já tipificados pelo nosso ordenamento jurídico.

Com relação aos crimes praticados na dark web, segundo relatórios de Michael Chertoff e Toby Simon, tem-se uma proliferação maior dos delitos mais graves, como pornografia infanto-juvenil, racismo, assassinatos encomendados, venda de armas, drogas e órgãos, tráfico de pessoas e animais, entre outros[21].

A dificuldade de identificar os autores dos crimes virtuais, principalmente quando ocorridos na dark web, e a consequente punição resultou em uma preocupação mundial. Assim sendo, a Convenção de Budapeste, fruto de um trabalho desenvolvido pelo Conselho da Europa, surge como forma de discussão de soluções a esses crimes ao priorizar a proteção da sociedade contra os avanços da criminalidade. Durante a Convenção, houve a proposta de escolha de uma legislação comum com objetivo de promover a cooperação entre os Estados da União Europeia.

Com a efetivação da Convenção de Budapeste, que entrou em vigor em 1º de julho de 2004, e a abertura à assinatura por todos os países que desejassem, ficou demonstrada a necessidade de combate aos crimes cibernéticos por toda a sociedade mundial.

Os seguintes crimes foram tipificados na Convenção de Budapeste[22]:

> 1) Infrações contra a confidencialidade, integridade e disponibilidade dos dados e sistemas informáticos:
> a) acesso doloso e ilegal a um sistema de informática;

[20] Safer Net Brasil . Relatório de dados da internet. Disponível em: http://www.safernet.org.br/site/indicadores. Acesso em: 19 de abril de 2020

[21] Chertoff, Michael. SIMON, Toby. The Impact of the Dark Web on Internet Governance and Cyber Security, Global Commission on Internet Governance. Paper Series: No. 6, February 2015. p. 6

[22] Ministério Público Federal. Crimes cibernéticos: manual prático de investigação. São Paulo: Procuradoria da República de São Paulo: 2006, p. 79 a 100.

> b) interceptação ilegal de dados ou comunicações telemáticas;
> c) atentado à integridade dos dados (conduta própria de um subgrupo hacker, conhecido como cracker);
> d) atentado à integridade de um sistema;
> e) produção, comercialização, obtenção ou posse de aplicativos ou códigos de acesso que permitam a prática dos crimes acima indicados.
> 2) Infrações informáticas:
> a) falsificação de dados;
> b) estelionatos eletrônicos (v.g., os phishing scams).
> 3) Infrações relativas ao conteúdo:
> a) pornografia infantil (produção, oferta, procura, transmissão e posse de fotografias ou imagens realistas de menores ou de pessoas que aparecem como menores, em comportamento sexual explícito);
> b) racismo e xenofobia (difusão de imagens, ideias ou teorias que preconizem ou incentivem o ódio, a discriminação ou a violência contra uma pessoa ou contra um grupo de pessoas, em razão da raça, religião, cor, ascendência, origem nacional ou étnica; injúria e ameaças qualificadas pela motivação racista ou xenófoba; negação, minimização grosseira, aprovação ou justificação do genocídio ou outros crimes contra a humanidade);
> 4) Atentado à propriedade intelectual e aos direitos que lhe são conexos.

A necessidade de cooperação entre diversos países é também vista por Medeiros, quando este afirma que "não há fronteiras demarcadas no ambiente cibernético"[23].

No mesmo viés, Castells assevera que:

> O Estado não desaparece (...). É apenas redimensionado na Era da Informação. Prolifera sob a forma de governos locais e regionais que se espalham pelo mundo com seus projetos, formam eleitorados e negociam com governos nacionais, empresas multinacionais e órgãos internacionais. A era da globalização da economia também é a era de localização da constituição política. O que os governos locais e regionais não têm em termos de poder e recursos é compensado pela flexibilidade e atuação em redes.[24]

O Brasil ainda não é signatário da Convenção de Budapeste, o que seria um avanço para um efetivo combate aos crimes cibernéticos, já que estes entram em confronto constante com o princípio da extraterritorialidade, de forma que, se tivéssemos um código comum de tipificação destes crimes, o problema poderia ser resolvido nesse quesito.

Algumas condutas delituosas, normas penais incriminadoras em vigor no país, são praticadas no universo da web e merecem uma abordagem já que a combinação de seus diversos núcleos pode caracterizar a prática do ato ilícito conhecido como ransomware.

---

[23]Medeiros, Assis. Hackers: entre a ética e a criminalização. Florianópolis: Visual Books, 2002, p. 147.

[24]Castells, Manuel. Fim do Milênio. São Paulo: Paz e Terra, 2007, p. 203.

Em relação ao crime de Divulgação de Segredo, seu tipo é descrito no artigo 153 do Código Penal e expressa em seu § 1º-A que “divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública. Pena: detenção, de 1 (um) a 4 (quatro) anos, e multa”[25].

O tipo apresenta elementos de caráter criminoso, sendo estes a divulgação de conteúdo de documento particular ou de correspondência confidencial; a ausência de justa causa para essa divulgação; a divulgação levada a efeito pelo destinatário ou detentor do documento particular ou de correspondência confidencial; e a potencialidade de dano a outrem.

Cezar Bitencourt afirma que “sigiloso é algo que não deve ser revelado, confidencial, limitado ao conhecimento restrito, não podendo sair da esfera de privacidade de quem o detém”. E, ainda, “é indispensável que a operação ou o serviço refira-se a conteúdo cuja revelação tenha idoneidade para produzir dano”[26].

Ademais, o tipo descrito é norma penal em branco, eis que somente se configurará a modalidade qualificada se as informações consideradas como sigilosas ou reservadas forem aquelas apontadas como tal pela lei.

O Dano por difusão de código malicioso, presente na Lei Contra a Ordem Tributária (Lei n° 8.137, de 27 de dezembro de 1990), no artigo 2º, V, verificamos a preocupação do legislador no sentido de punir a conduta de “utilizar ou divulgar programa de processamento de dados que permita ao sujeito passivo da obrigação tributária possuir informação contábil diversa daquela que é, por lei, fornecida à Fazenda Pública”, dando uma sanção considerada de menor potencial ofensivo.

No intuito de tipificar o crime no âmbito virtual, o Projeto de Lei do Senado nº 76/2000 propôs a inserção do artigo 163-A, ao Código Penal, com a seguinte redação:

> Dano por difusão de código malicioso eletrônico ou digital ou similar Art. 163-A. Criar, inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado. Pena: reclusão, de 1 (um) a 3 (três) anos, e multa.
> Art. 4º O caput do art. 163 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) passa a vigorar com a seguinte redação:
> “Dano

[25] Brasil. Decreto-Lei 2.848, de 07 de dezembro de 1940. Código Penal. Diário Oficial da União, Rio de Janeiro, 31 dez. 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 15 de abril de 2020

[26] Bitencourt, Cezar Roberto. Tratado de Direito Penal. São Paulo: Saraiva, 2019, p. 497.

> Art. 163. Destruir, inutilizar ou deteriorar coisa alheia ou dado eletrônico alheio:"[27]

A Fraude eletrônica e estelionato, conhecida como Phishing, é uma espécie de fraude virtual, por meio do qual o agente obtém informações da vítima, senhas e dados pessoais, quando se passa por terceiro (um banco, uma loja, um órgão) levando a vítima a erro, sendo que o objetivo é a obtenção de vantagem patrimonial ilícita. É o que ocorre no estelionado, tipo descrito no artigo 171 do Código Penal: "Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento"[28].

Neste caso o artifício e o ardil encontram-se circunscritos ao gênero da fraude, ou seja, o engodo, o engano, a artimanha do agente, no sentido de fazer com que o lesado incorra em erro e ali, por vezes, permanecendo. De outra monta, a conduta em que o agente se utilizando de meios ardilosos, insidiosos, fazendo com que o lesado incorra, ou seja, mantido em erro, a fim de que o próprio agente pratique a subtração, está situada no disposto no artigo 155, § 4º, inciso II, segunda figura (fraude), do Código Penal, que é utilizada pelo agente, a fim de facilitar a subtração por ele levada a efeito[29].

Nelson Hungria já escrevera que o "meio fraudulento é também, qualquer ardil no sentido de provocar a ausência momentânea do dominus ou distraindo-lhe a atenção, para mais fácil proceder a perpetração do furto"[30].

No substitutivo proposto pelo PLS n° 76/2000 o art. 171-A visa atender ao crime no formato digital, com a seguinte redação:

> Difusão de código malicioso
>
> Art. 171-A. Difundir, por qualquer meio, programa, conjunto de instruções ou sistema informatizado com o propósito de levar a erro ou, por qualquer forma indevida, induzir alguém a fornecer, espontaneamente e por qualquer meio, dados ou informações que facilitem ou permitam o acesso indevido ou sem autorização, à rede de computadores, dispositivo de comunicação ou a sistema informatizado, com obtenção de vantagem ilícita, em prejuízo alheio:
> Pena – reclusão, de um a três anos. [31]

---

[27] Brasil. PLS nº 76 de 26 de outubro de 2000. Atividade Legislativa do Senado Federal. Disponível em: https://www.lexml.gov.br/urn/urn:lex:br:senado.federal:projeto.lei;plc:2003;89. Acesso em: 13 de abril de 2020

[28] Brasil. Decreto-Lei 2.848, de 07 de dezembro de 1940. Código Penal. Diário Oficial da União, Rio de Janeiro, 31 dez. 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 15 de abril de 2020

[29] Greco, Rogério. Curso de direito penal: Parte geral. Rio de Janeiro: Impetus, 2019, p. 419.

[30] Hungria, Nelson. Comentários ao Código Penal, vol. 7. Rio de Janeiro: Forense, 1956, p. 44.

> § 1º A pena é aumentada de sexta parte, se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática de difusão de código malicioso.

A Extorsão, ato de obrigar alguém a adotar um determinado comportamento, por meio de ameaça ou violência, com a intenção de obter vantagem, recompensa ou lucro é crime 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.[32]

3 RANSOMWARE COMO CRIME AINDA NÃO TIPIFICADO

Quando combinamos todos esses tipos penais, percebemos a preocupação de setores jurídicos e de investigação policial com a prática do ransomware que, segundo definição trazida por Gavin O'Gorman e Geoff McDonald, é uma "categoria de programa malicioso que, quando rodado, desabilita funcionalmente o computador ou a rede". Na sequência, "quando o usuário acessa o computador ou a rede, o programa malicioso mostra uma mensagem que demanda um pagamento para que se possa retornar à normalidade, ou seja, o ransomware é uma forma de extorsão"[33]. Geralmente, juntamente com a mensagem é anexado um contador que mostra o prazo para o pagamento da quantia exigida para a liberação do sistema, importe que é fixado em bitcoins, moeda, como visto anteriormente, não rastreável.

O ransomware, crime ainda não tipificado em nosso ordenamento jurídico, portanto, reúne a extorsão (obrigando alguém a tomar determinado comportamento por meio de ameaça) e o dano por inserção de código malicioso, além de poder resultar em fraude eletrônica (ao capturar dados que podem ser usados se passando por terceiros e induzindo usuários a erro) e divulgação de segredo (conforme dados coletados), caso não se pague a quantia exigida pelo agente.

---

[31] Brasil. PLS nº 76 de 26 de outubro de 2000. Atividade Legislativa do Senado Federal. Disponível em: https://www.lexml.gov.br/urn/urn:lex:br:senado.federal:projeto.lei;plc:2003;89. Acesso em: 13 de abril de 2020

[32] Brasil. Decreto-Lei 2.848, de 07 de dezembro de 1940. Código Penal. Diário Oficial da União, Rio de Janeiro, 31 dez. 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 15 de abril de 2020.

[33] Trad. livre, no original: *Ransomware is a category of malicious software which, when run, disables the functionality of a computer in some way. The ransomware program displays a message that demands payment to restore functionality. (…) In other words, ransomware is an extortion racket*. In O'GORMAN, Gavin. MCDONALD, GEOFF. Ransomware: A Growing Menace. Montain View: Symantic, 2012, p. 02

Nos últimos anos, nota-se um crescente número de ataques envolvendo ransomware: os governos, na impossibilidade de identificação dos criminosos e suas localizações em tempo hábil, têm pago a quantia exigida. Essa modalidade, infelizmente, tornou-se um dos crimes mais graves enfrentados atualmente.

Por exemplo[34], nos Estados Unidos, o Condado de Jackson desembolsou US$ 400 mil, assim como West Raven, em Connecticut (US$ 2 mil), além de Riviera Beach (US$ 600 mil) e Lake City (US$ 460 mil) – ambos no estado da Flórida. Um dos casos mais conhecidos ocorreu em 2018, quando o prefeito de Atlanta, na Geórgia, não aceitou realizar o pagamento, tendo a administração pública que gastar inicialmente US$ 3 milhões para começar a reestabelecer os sistemas afetados.

Em território nacional, estatísticas[35] mostram que o Brasil é o 2º país com mais ameaças de ransomware no mundo, o que mostra a necessidade urgente de medidas para coibir essa prática criminosa. O ataque mais recente, ocorrido em 15 de abril de 2020, envolvendo o Brasil foi à Companhia Energétia EDP[36], presente em onze estados brasileiros, no qual os criminosos invadiram os sistemas e exigiram o pagamento em bitcoins no valor estimado em 56 milhões de reais sob ameaça de divulgação e venda de dados pessoais de clientes na dark web. Ainda não houve divulgação oficial de como ocorreu o desfecho, mas, segundo o site da revista Exame, até o dia 24 de abril, “a página criada pelos hackers mantinha-se no ativo com a mesma mensagem de sempre – apesar de não haver uma razão lógica para isso”[37].

CONCLUSÃO

[34] Consumidor Moderno. Ransomware: sequestro de dados. Disponível em: https://www.consumidormoderno.com.br/2019/07/30/ransomware-sequestro-dados/.Acesso em: 19 de abril de 2020.
[35] Canaltech. Brasil é o 2º país com mais ameaça de ransomware. Disponível em: https://canaltech.com.br/seguranca/brasil-e-o-2o-pais-com-mais-ameacas-de-ransomware-no-mundo-aponta-estudo-134683/. Acesso em: 17 de abril de 2020.
[36] Livecoins. EDP hackeada em 56 milhões de bitcoins. Disponível em: https://livecoins.com.br/companhia-energetica-portugal-hackeada-rs-56-milhoes-em-bitcoins/. Acesso em: 20 de abril de 2020.
[37] Exame Informática. EDP. Disponível em: https://visao.sapo.pt/exameinformatica/noticias-ei/internet/2020-04-22-edp-so-a-arquitetura-de-rede-impediu-um-apagao-geral-durante-ataque-de-hackers/ Acesso em: 04 de maio de 2020.

Conforme demonstrado neste artigo, bem assim em pesquisa realizada por David Augusto Fernandes[38], desde as negociações até a Convenção de Budapeste, passaram-se cerca de cinco anos, e o projeto de lei PLS n° 76/2000 que propunha novas tipologias para os delitos cibernéticos, está sem definição há vinte anos, causando instabilidade social.

Isso contribui para, ainda segundo Fernandes[39], que se vislumbre continuamente a invasão de sistemas de informática, não havendo uma lei precisa para inibir e punir aqueles que utilizam seus conhecimentos de informática para ações criminosas, causando prejuízo a milhares de pessoas físicas e jurídicas. Dessa forma, coadunando com os estudos do autor, "o Brasil poderia aderir ou adotar a Convenção de Budapeste, haja vista que nos projetos de leis anteriormente referidos há uma similitude entre as intenções apresentados e o conteúdo da Convenção". Isso deve ser implementado como forma de alinhar o país aos esforços na persecução desse tipo de crime e fortalecer a cooperação internacional nesse particular.

Ademais, com o avanço da internet das coisas, em que vários aparelhos estão conectados e trocando informações entre si, cada vez mais a prática de crimes virtuais pode tomar dimensões indesejáveis e, como afirmam os autores Rezer e Fortes,

> a sociedade de risco continuará convivendo com esse crescimento tecnológico, não há como pará-lo, necessita-se de legislações que protejam os usuários e que delimitem até onde esses avanços podem evoluir. Atualmente não há uma legislação brasileira específica para a proteção dos usuários das "coisas", conectadas a internet. (...) Surge a oportunidade de pautar esse tema para a criação de novas leis, sem aguardar que impactos extremos aconteçam[40].

No mesmo sentido, Eduardo Magrani escreve que todos esses dispositivos conectados diariamente irão armazenar, transmitir e compartilhar uma volumosa quantidade de dados íntimos da vida do indivíduo. A segurança e a privacidade dos usuários correm riscos com o aumento da utilização desses dispositivos, alguns já existentes, outros que entrarão em breve no mercado[41].

---

[38] Fernandes, David Augusto. Crimes Cibernéticos: o descompasso do Estado e a realidade. Disponível em: https://www.direito.ufmg.br/revista/index.php/revista/article/download/P.0304-2340.2013v62p139/248. Acesso em: 24 de maio de 2020.

[39] *Idem.*

[40] Rezer, Morgana; Fortes, Vinícius. A internet das coisas na sociedade de risco: uma análise a partir do direito à privacidade. Florianópolis: Compedi, 2018. p. 23 e 24.

[41] Magrani, Eduardo. A internet das coisas. Rio de Janeiro: FGV Editora, 2018, p.24.

No caso dos crimes cibernéticos, o objetivo primordial da ciência do direito é a sua repressão, e como escreve também Fernandes[42], “utilizando-se de normas eficientes e práticas, mediante as quais a sociedade se sinta segura” para acessar a internet, sem que haja alguma interferência daqueles que por meio escusos busquem conseguir lucros, acabando por causar prejuízos monetários e danos morais irreversíveis.

REFERÊNCIAS

Bitencourt, Cezar Roberto. Tratado de Direito Penal. São Paulo: Saraiva, 2019.

Brasil. Decreto-Lei 2.848, de 07 de dezembro de 1940. Código Penal. Diário Oficial da União, Rio de Janeiro, 31 dez. 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 15 de abril de 2020.

_____. Lei 8.137, de 27 de dezembro de 1996. Define crimes contra a ordem tributária, econômica e contra as relações de consumo. Diário Oficial da República Federativa do Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8137 .htm Acesso em: 15 de abril de 2020.

_____. PLS nº 76 de 26 de outubro de 2000. Dispõe sobre os crimes cometidos na área de informática, e suas penalidades, dispondo que o acesso de terceiros, não autorizados pelos respectivos interessados, a informações privadas mantidas em redes de computadores, dependerá de prévia autorização judiciária. Atividade Legislativa do Senado Federal. Disponível em: https://www.lexml.gov.br/urn/ urn:lex:br:senado.federal:projeto.lei;plc:2003;89. Acesso em: 13 de abril de 2020.

Canaltech. “Brasil é o 2º país com mais ameaça de ransomware”. Disponível em: https://canaltech.com.br/seguranca/brasil-e-o-2o-pais-com-mais-ameacas-de-ransomware-no-mundo-aponta-estudo-134683/. Acesso em: 17 de abril de 2020.

Carneiro, Adeneele Garcia. “Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação”. Âmbito Jurídico. Disponível em: http://www.ambito-juridico.com.br/site/index.php/?n_link=revista_artigos_leitura&artigo_id=11529&revista_caderno=17. Acesso em: 17 de abril de 2020.

Castells, Manuel. Fim do Milênio. São Paulo: Paz e Terra, 2007.

Chertoff, Michael. SIMON, Toby. The Impact of the Dark Web on Internet Governance and Cyber Security, Global Commission on Internet Governance. Paper Series: No. 6, February 2015.

Consumidor Moderno. “Ransomware: sequestro de dados”. Disponível em: https://www.consumidormoderno.com.br/2019/07/30/ransomware-sequestro-dados/. Acesso em: 19 de abril de 2020.

Duarte, David; MEALHA, Tiago. Introdução à deep web. Lisboa: IET Working Papers Series, 2016.

Exame Informática. “EDP”. Disponível em: https://visao.sapo.pt/exameinformatica/noticias-ei/internet/2020-04-22-edp-so-a-arquitetura-de-rede-impediu-um-apagao-geral-durante-ataque-de-hackers/ Acesso em: 04 de maio de 2020.

Fernandes, David Augusto. “Crimes Cibernéticos: o descompasso do Estado e a realidade”. Disponível em: https://www.direito.ufmg.br/revista/index.php/revista/article/download/P.0304-2340.2013v62p139/248. Acesso em: 24 de maio de 2020.

[42] Fernandes, David Augusto. Crimes Cibernéticos: o descompasso do Estado e a realidade. Disponível em: https://www.direito.ufmg.br/revista/index.php/revista/article/download/P.0304-2340.2013v62p139/248. Acesso em: 24 de maio de 2020.

Flinkea, Kristin. Dark Web. Washington: Congressional Research Service. 2017.

Greco, Rogério. Curso de direito penal: Parte geral. Rio de Janeiro: Impetus, 2019.

Hungria, Nelson. Comentários ao Código Penal, vol. 7. Rio de Janeiro: Forense, 1956.

IBGE – Instituto Brasileiro De Geografia E Estatística. “Uso de internet, televisão e celular no Brasil”. Disponível em: https://educa.ibge.gov.br/ jovens/materias-especiais/20787-uso-de-internet-televisao-e-celular-no-brasil.html. Acesso em: 20 de abril de 2020.

Livecoins. “EDP hackeada em 56 milhões de bitcoins”. Disponível em: https://livecoins.com.br/companhia-energetica-portugal-hackeada-rs-56-milhoes-em-bitcoins/. Acesso em: 20 de abril de 2020.

Magrani, Eduardo. A internet das coisas. Rio de Janeiro: FGV Editora, 2018.

Medeiros, Assis. Hackers: entre a ética e a criminalização. Florianópolis: Visual Books, 2002.

Ministério Público Federal. Crimes cibernéticos: manual prático de investigação. São Paulo: Procuradoria da República de São Paulo: 2006

Monteiro, Silvana Drumond; FIDENCIO, Marcos Vinicius. A web invisível: um olhar sobre a parcela de informação no ciberespaço que os mecanismos de busca não conseguem indexar. Disponível em: http://www.uel.br/grupo-pesquisa/ciberespaco/doc/web_invisivel_enaic.pdf>. Acesso em: 17 de abril de 2020.

Monteiro, Silvana Drumond; FIDENCIO, Marcos Vinicius. As dobras semióticas do ciberespaço: da web visível à invisível. TransInformação , v. 25, n.1, p. 35-46, jan./abr. 2013. Disponível em: http://www.scielo.br/pdf/tinf/v25n1/a04v25n1.pdf. Acesso em: 16 de abril de 2020.

O’gorman, Gavin. MCDONALD, GEOFF. Ransomware: A Growing Menace. Montain View: Symantic, 2012

Pompéo, Wagner Augusto; SEEFELDT, João Pedro. Nem tudo está no Google: deep web e o perigo da invisibilidade. In: Congresso Internacional de Direito e Contemporaneidade. Santa Maria: UFSM, 2013.

Rezer, Morgana; FORTES, Vinícius. A internet das coisas na sociedade de risco: uma análise a partir do direito à privacidade. Florianópolis: Compedi, 2018.

Rosa, Fabrízio. Crimes de informática. Campinas: Bookseller, 2007.

Safer Net Brasil . Relatório de dados da internet. Disponível em: http://www. safernet.org.br/site/indicadores. Acesso em: 19 de abril de 2020

Sherman, Chris; PRICE, Gary. The invisible web: uncovering information sources search engines can’t see. Illinois: Cyberage Books, 2003.

Silveira, Sergio Amadeu. A Internet e o novo Cavalo de Tróia. Rio de Janeiro: PoliTICs, n. 10, ago. 2011.

Tor Project: anonymity online. Disponível em: https://www.torproject.org. Acesso em: 22 de abril de 2020

Ulrich, Fernando. Bitcoin: a moeda na era digital. São Paulo: Instituto Ludwig von Mises Brasil, 2014.