INSTITUTO ENSINAR BRASIL
FACULDADES UNIFICADAS DE LEOPOLDINA

LINDES DANIEL NETO

A PROTEÇÃO PENAL À PRIVACIDADE NA REDE: CRIMES CIBERNÉTICOS PRÓPRIOS E AS DEFICIÊNCIAS ESTRUTURAIS DO ORDENAMENTO JURÍDICO BRASILEIRO

LEOPOLDINA
2018

LINDES DANIEL NETO
FACULDADES UNIFICADAS DE LEOPOLDINA

A PROTEÇÃO PENAL À PRIVACIDADE NA REDE: CRIMES CIBERNÉTICOS PRÓPRIOS E AS DEFICIÊNCIAS ESTRUTURAIS DO ORDENAMENTO JURÍDICO BRASILEIRO

Trabalho de Conclusão de Curso apresentado ao Curso de Direito das Faculdades Unificadas de Leopoldina, como requisito parcial para obtenção do título de Bacharel em Direito.

Área de Concentração: Direito Digital. Direito Penal.

Orientador: prof. Me. Victor Freitas Lopes Nunes.

LEOPOLDINA
2018

FACULDADES UNIFICADAS DE LEOPOLDINA

FOLHA DE APROVAÇÃO

O Trabalho de Conclusão de Curso intitulado: A PROTEÇÃO PENAL À PRIVACIDADE NA REDE: CRIMES CIBERNÉTICOS PRÓPRIOS E AS DEFICIÊNCIAS ESTRUTURAIS DO ORDENAMENTO JURÍDICO BRASILEIRO, elaborado pelo aluno LINDES DANIEL NETO foi aprovado por todos os membros da Banca Examinadora e aceita pelo curso de Direito das Faculdades Unificadas de Leopoldina, como requisito parcial da obtenção do título de

BACHAREL EM DIREITO

Leopoldina, ___ de dezembro de 2018.

_____

Prof(ª). Orientador(a): _____

_____

Pro(ª). Examinador(a) 1: _____

_____

Prof(ª). Examinador(a) 2: _____

AGRADECIMENTOS

A Deus por minha vida, família e amigos.

Ao meu orientador, pelo empenho dedicado à elaboração deste trabalho.

A todos os professores por me proporcionar o conhecimento não apenas racional, mas a manifestação do caráter e afetividade da educação no processo de formação profissional.

RESUMO

Esta pesquisa retrata sobre os problemas que a privacidade enfrenta no ciberespaço em meio à evolução tecnológica, gerando grande reflexo no Direito, especialmente, no Direito Penal, uma vez que o desenvolvimento tecnológico também proporcionou um novo ambiente para a prática de atos delituosos. O objetivo do trabalho é mostrar de que maneira os crimes cibernéticos também afetam a vida privada da pessoa na rede mundial de computadores, compreendendo as condutas praticadas pelos cibercriminosos junto à ineficácia atual das tipificações existentes no sistema brasileiro. Portanto, é feita uma análise das condutas que podem ser consideradas crimes cibernéticos próprios e quais são as legislações aplicáveis a estes tipos de delitos. A observação da legislação de cooperação internacional para uma proteção mais eficiente desses crimes que são praticados tanto na surface ou na deepweb permitiu, no esforço comparativo, compreender a timidez dos passos dados pelo Legislador brasileiro. Por fim, à guiza de conclusão percebe-se a necessidade de o Brasil também se engaje na cooperação internacional para combater os crimes cibernéticos, dado o caráter mundial deste problema, para se ter melhor efetividade da aplicação lei penal.

Palavras-chave: Privacidade. Dados Pessoais. Crimes Cibernéticos Próprios.

ABSTRACT

This research portrays the problems that privacy faces in cyberspace in the midst of technological evolution, generating a great reflex in the Law, especially in the Criminal Law, since the technological development also provided a new environment for the practice of criminal acts. The purpose of this paper is to show how cybercrime also affects the private life of the person in the world computer network, understanding the behaviors practiced by cybercriminals along with the current inefficiency of the typifications existing in the Brazilian system. Therefore, an analysis is made of the conduct that can be considered as cyber crimes and what are the laws applicable to these types of crimes. The observation of the international cooperation legislation for a more efficient protection of these crimes that are practiced on the surface or deepweb allowed, in the comparative effort, to understand the timidity of the steps taken by the Brazilian Legislator. Finally, the conclusion is that Brazil must also engage in international cooperation to combat cybercrime, given the global nature of this problem, in order to have a better enforcement of criminal law.

KEY-WORDS: Privacy. Personal data. Cyber Crimes.

SUMÁRIO

1 INTRODUÇÃO

O presente trabalho busca analisar como a evolução tecnológica impactou no Direito, principalmente no Direito Penal. Analisam-se as condutas típicas já previstas no ordenamento em matéria de crimes cibernéticos próprios de forma não exaustiva, pretendendo compreender em que medida os tipos penais postos pela legislação vigente são necessários e suficientes para a prevenção e, eventualmente, punição de violações à privacidade na Era Digital.

A privacidade vem sendo constantemente ameaçada pelo ciberespaço, de modo que, dados pessoais estão cada vez mais acessíveis aos cibercriminosos, que desenvolvem constantemente suas práticas delitivas frente a ineficácia do sistema jurídico brasileiro em penalizar tais práticas. Trata-se, portanto, de tema não apenas atual, mas de destacada relevância para o Direito do século XXI.

Não é mais possível que os ordenamentos jurídicos mundo afora e o brasileiro especificamente negligenciem a necessidade de uma ordenação global voltada ao combate dos crimes cibernéticos. Entretanto, as mais diversas assimetrias, bem como a tênue fronteira entre os crimes cibernéticos comuns e o ciberterrorismo em nada contribuem para o desenvolvimento de dispositivos jurídicos voltados ao combate efetivo da criminalidade na rede mundial de computadores.

A análise da problemática proposta, parte de uma aspiração compreensiva do estado da arte do Direito Penal, especificamente no que toca aos crimes cibernéticos próprios, os quais são determinados como aqueles que tem como objeto de proteção jurídica o direito de privacidade. Neste caso, a própria ideia de privacidade precisa ser considerada segundo suas implicações no contexto atual, em que todos os sujeitos de direito estão conectados. Neste cenário, as pessoas têm expostos ou expõem elas próprias informações albergadas pelas hipóteses de incidência deste Direito Fundamental.

A seguir, apresenta-se uma mirada sobre Direito Digital, como ele afeta a sociedade. Inicialmente abordam-se os princípios que regem o Direito Digital, os quais estão previstos pelo Marco Civil da Internet, tais como a neutralidade da rede, privacidade e preservação da segurança. Avançando, na seção seguinte do próximo capítulo, trata-se da proteção dos dados pessoais que foi objeto da lei nº

13.709/2018 regulamentando as informações dos usuários na rede. Posteriormente analisa-se, como a privacidade se desenvolveu na sociedade da informação, a partir de um novo protótipo conceitual dada pela doutrina.

O terceiro capítulo tratará, especificamente, dos crimes cibernéticos próprios, nos quais o objeto da violação é o próprio sistema informático. Estes crimes tipificam condutas que violam a privacidade do usuário na rede, tais como o acesso não autorizado, a transferência ilegal de dados e o *phishing*. Aproveita-se também para explicitar algumas definições essenciais à compreensão da complexidade do problema de pesquisa proposto. As definições de *surface* e *deep web*, relativas às diferentes estruturas da internet, pela sua própria arquitetura, voltada a proteção do anonimato, compõem o ambiente no qual a persecução criminal se inicia quanto aos crimes cibernéticos próprios.

Por fim, no último capítulo, apresenta-se a legislação aplicável aos crimes cibernéticos próprios e discutem-se as dificuldades em lidar com esta versão contemporânea da criminalidade, em que a mera tipificação penal não é suficiente para solucionar os conflitos do ciberespaço, os quais decorrem da falta de harmonização do Direito Penal material e Processual Penal, bem como da falta de uma normativa internacional aplicável à espécie.

2 DIREITO DIGITAL

Metodologicamente, este trabalho tem cunho interdisciplinar, porquanto proponha o estudo do direito e da informática. Trata-se, de fato, de uma pesquisa de caráter eminentemente bibliográfica, valendo-se, portanto, de fontes secundárias. O exame proposto é qualitativo, para o qual importa conteúdo latente dos conceitos sob análise, uma vez que se busca extrair do arcabouço conceitual o significado não aparente dos conceitos analisados. Para tanto, recorre-se a análise de conteúdo, visto que se propõe o contraste entre o sistema analítico de conceitos formulado a partir do direito à privacidade junto ao direito digital à legislação penal brasileira.

O presente trabalho será voltado a compreensão dos crimes cometidos pela rede mundial de computadores, tais crimes, compreendidos como crimes cibernéticos que colocam em risco a vida privada do usuário na rede. No entanto, antes de determinar as espécies dos crimes cibernéticos que serão o objeto de estudo deste trabalho, será necessário apresentar primeiramente os princípios norteadores do Direito Digital, princípios estes que são voltados para a proteção dos dados do usuário na rede.

Deste modo, o advento da internet na sociedade trouxe grandes modificações na forma de comunicação e interação do ser humano. Com o grande desenvolvimento e expansão da rede mundial de computadores, o direito passou a ser desempenhado e violado por este sistema. Portanto, conflitos, causas e processos que antes eram resolvidos apenas no mundo real, foram transferidos também para o mundo virtual.

Por se tratar de uma sociedade, o Direito não foge a ela, sendo necessária sua observância, de modo que o Direito não despreze essa realidade, fazendo-o elaborar novos mecanismos jurídicos para que a sociedade não fique desamparada, dando origem assim ao Direito Digital.

O Direito Digital traz uma missão importante para o Legislativo, tendo diversos projetos de lei em tramitação que dizem a respeito dos institutos e práticas do Direito Digital, com a finalidade de compreender melhor essa mudança social, pois, o Direito Digital evolui de forma espontânea e rápida, devendo o Direito acompanhar esta mudança.

Entende-se que o Direito Digital não é explicitamente um novo ramo do Direito, sendo apenas uma adaptação dos institutos jurídicos já existentes para a área da tecnologia da informação. Trata de um instrumento para disciplinar as relações entre o próprio homem e a tecnologia, vindo para regular e sistematizar as evoluções advindas da sociedade da informação. Tornando assim, um direito multidisciplinar, com uma reunião de matérias já conhecidas como o Direito Civil, Direito Penal, Direito Constitucional, Processual Civil e do Consumidor, pois, ele saiu daquele meio que era só tecnológico dos softwares e contratos, abrangendo e complementando os demais ramos do Direito (PINHEIRO, 2016).

Na esfera penal podemos ver o estelionato virtual, ameaças e crimes contra a honra que são frequentemente praticados na rede. Portanto, tem-se importância do Direito Digital para estabelecer uma regra na rede, pois, a tecnologia e a informática afetam a vida social do homem de modo geral.

2.1 Os princípios do direito digital

Com a necessidade de se regular uma sociedade digital surgiu uma lei regulamentadora, a Lei 12.965/2014, conhecida por Marco Civil da Internet, estabelecendo princípios, garantias, direitos e deveres dos usuários da rede no Brasil.

O art. 3° do Marco Civil prevê que a internet brasileira se encontra consolidada pelos princípios da neutralidade da rede, da privacidade e da preservação da segurança.

A neutralidade da rede diz a respeito em que a rede deve tratar tudo aquilo que ela incorpora de forma isonômica, ou seja, lidando e tratando todos da mesma forma, sem discriminações quanto a natureza do conteúdo e a identidade do usuário na rede. Referente ao princípio da neutralidade da rede, Maria Celina (2017, p. 112) elucida:

> O princípio impõe que a filtragem ou os privilégios de tráfego devam respeitar apenas e tão somente critérios técnicos e éticos, não sendo admissíveis motivos políticos, comerciais, religiosos ou culturais que criem qualquer forma de discriminação ou favorecimento.

A neutralidade da rede é muito importante para garantir o acesso à tecnologia, pois, se não há neutralidade, teremos alguns interesses que podem parecer conflitantes. É muito comum que determinada companhia telefônica dê acesso ao telefone fixo e junto a internet. Portanto, para esta companhia é muito importante que você faça o uso do telefone. Sem a neutralidade da rede, esta mesma companhia poderia degradar a conexão na rede pelo uso de outro meio de comunicação como o Skype ou qualquer outro software de comunicação pela internet por exemplo, obrigando o consumidor a usar o telefone fixo para ligar para outra pessoa e pagando mais caro pelo serviço.

O princípio da neutralidade da rede vem previsto no art. 9° da lei 12.965/2014 (BRASIL, 2014): “Art. 9° O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação”. Assim como todas as pessoas são iguais perante a lei, todos os dados devem ser iguais perante a rede, tratando-se todos os dados que nela correm da mesma forma.

Neste meio tecnológico, o princípio da privacidade é o da preservação da confidencialidade de dados pessoais e da própria vida íntima. Observa-se que o princípio da privacidade ultrapassou daquele meio de pessoa, informação e segredo, passando para a esfera da circulação e controle das informações, devendo o indivíduo exercer o controle sobre o uso dos próprios dados pessoais armazenados na rede.

A privacidade tem a finalidade de proteger a vida íntima da pessoa humana, mas ela vem se modificando constantemente para se adaptar à realidade na sociedade da informação. Na exposta perspectiva, Aline de Castro (2018, p. 46) exemplifica:

> A privacidade, então, diz respeito ao poder de acesso e controle que uma pessoa tem dos próprios dados, bem como o direito de selecionar o que quer expor de si mesmo aos outros por meio de prévio consentimento. Logo, o consentimento do interessado é o ponto de referência de todo sistema de tutela da privacidade, existindo a questão de quais serão as medidas a serem tomadas e as consequências se uma pessoa considerar que sua privacidade está sendo violada por uma informação divulgada de maneira não autorizada na rede.

Sendo assim, ter privacidade na rede envolve o poder controlar a utilização das suas próprias informações. Na conceituação constitucional, quando se fala em

intimidade, é versado sobre o direito de ser deixado só, porém, hoje, não se tem a mesma dimensão de segredo constatado anteriormente, pois, os segredos e eventos pessoais do indivíduo, não estão mais seguros entre quatro paredes, uma vez expostos na rede mundial de computadores.

O princípio da preservação da segurança busca proteger e equilibrar direitos e garantias do provedor e do usuário na rede, inclusive à proteção dos dados pessoais que será melhor explicada no próximo tópico. Neste sentido, o art. 3º, V, do Marco Civil (BRASIL, 2014) dispõe: “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”.

Entende-se que a preservação da segurança deve ainda ser realizada com base em medidas técnicas internacionalmente reconhecidas como eficazes, uma vez considerada, também, a “escala global da rede”, (BRASIL, 2014), nos termos do art. 2º, I, bem como o consentimento relativo ao compartilhamento de dados de qualquer não pode se dar em violação ao disposto no art. 7º, VI (BRASIL, 2014), quanto à clareza e completude dos contratos que envolvem a prestação de serviços e que tenham como contraprestação do usuário, dentre outras eventuais contraprestações, a permissão para a cessão onerosa ou gratuita, de dados para a composição de um *big data*[1].

Trata-se, neste caso, de matéria que veio a ser regulada recentemente com a promulgação da Lei nº 13.709/2018, a qual se volta à segurança e à proteção dos dados dos usuários da internet.

2.2 Privacidade e proteção de dados pessoais

A Lei nº 13.709/2018 inovou o ordenamento jurídico brasileiro, uma vez que dispôs sobre a proteção geral de dados pessoais, com isso, o ordenamento jurídico brasileiro incorporou-se em uma lei única para proteger e tratar os dados pessoais. Está lei positiva regras que regulamentam o armazenamento de informações dos usuários por parte de empresas e órgãos públicos. A partir dela, espera-se garantir

1 O ciberespaço gera, diariamente, 2,5 quintilhões de bytes, sendo que, atualmente, quase 90% dos dados foram gerados durante os últimos dois anos, portanto, este volume imensurável de dados é denominado de big data.

mais segurança jurídica para o cidadão que quer ter a seus direitos assegurados enquanto navega na rede mundial de computadores.

Anteriormente, a regulamentação legal da matéria resumia-se ao Marco Civil que versava sobre os princípios gerais da proteção de dados pessoais para aplicação da internet e para os provedores de acesso. Todo aquele universo que envolvia os dados pessoais estava sem parâmetro jurídico próprio. A nova lei geral de proteção de dados terá uma aplicação mais ampla afetando qualquer atividade que envolva a utilização de dados pessoais, incluindo o tratamento de dados que circulam pela internet de consumidores, empregados, dentre outros. Sua aplicabilidade integrará toda e qualquer pessoa natural ou jurídica de direito público ou privado que realize o tratamento de dados pessoais, o que somente poderá se dar mediante o consentimento explícito do usuário, regulado pelo Capítulo II, Seção I da Lei nº. 13.709/2018 (BRASIL, 2018).

Os dados pessoais correspondem a qualquer dado relacionado a uma pessoa identificada ou identificável, ou seja, é toda e qualquer informação que identifique ou torne identificável uma pessoa, nos termos do art. 5º da Lei nº. 13.709/18 (BRASIL, 2018). A interpretação combinada deste dispositivo e do art. 3º, III do Marco Civil (BRASIL, 2014), permite compreender que dados envolvem tanto as informações armazenadas ou transportadas[2], art. 7º, I e III (BRASIL, 2014), quanto outras informações relativas aos dados, as quais não se confundem com o dado em si, assim chamados metadados, expressos no art. 7º, III e VII (BRASIL, 2014).

Atualmente, uma série de agentes privados que tem acesso a uma sequência de dados dos usuários, que muitas vezes são obtidos e coletados sem o necessário respeito à “autodeterminação informativa” (BRASIL, 2014), o que, no entanto, não é considerado, necessariamente ato criminoso. Ainda assim, a proteção dos dados pessoais é fundamental, pois, serão estes dados que assegurarão a privacidade de qualquer uma pessoa na sociedade da informação, portanto, o uso inadequado desses dados pessoais pode gerar vastos danos ao usuário.

---

2 Neste sentido, a Lei nº 13.709/ 2018 (BRASIL, 2018), dispõe: “Art. 5º Para os fins desta Lei, considera-se: I – dado pessoal: informação relacionada a pessoa natural identificada ou identificável; II – dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; III – dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento”.

Uma das inovações importantes que a lei de proteção de dados traz diz respeito à transferência internacional de dados. Considerando o caráter global da rede, as relações de transferências de dados se dão em escala internacional, de modo que, esta nova lei possibilita que empresas possam transferir dados para outros países, desde que elas comprovem a segurança desses dados por meio de selos e certificados.

2.3 Privacidade na sociedade da informação

A privacidade é o direito fundamental de manter o controle sobre o que, quando, onde e como informações pessoais são compartilhadas. O cenário atual não permite que se pense da privacidade como o antigo direito a ser deixado só. A privacidade na sociedade da informação, além de ser um direito fundamental, é de suma importância sua proteção que está diretamente ligada à liberdade, o que coloca o direito à privacidade como uma necessidade para garantia da dignidade da pessoa humana (RODOTÀ, 2007).

A antiga acepção do direito à privacidade envolvia em si a idealização de que a proteção à vida privada decorresse somente em meio de uma propriedade. Desta forma, entende-se que no século XIX a propriedade era contemplada como o essencial desenvolvimento da personalidade do indivíduo, sendo o direito à propriedade imprescindível para assim chegar à privacidade. Neste sentido, podemos afirmar que o nascimento da privacidade não se deu por uma exigência “natural” do ser humano, mas como uma aquisição que apenas a classe burguesa continha naquele século. Portanto, ocorreu a descentralização da propriedade a privacidade, reformulando assim a concepção do direito a ser deixado só.

Os conceitos clássicos de privacidade passam por uma reconstrução, a partir de uma reflexão teórica. Na visão de Stefano Rodotà (2007, p. 7), as novas tecnologias estão tornando a sociedade cada vez mais transparente.

> Assediados por computadores, espiados por olhos furtivos, filmados por telecâmeras invisíveis. Os cidadãos da sociedade da informação correm o risco de parecer homens de vidro: uma sociedade que a informática e a telemática estão tornando totalmente transparente.

Percebe-se uma mudança radical na contextualização do direito à privacidade na sociedade da informação. Rodotà (2007, p. 7) diz que a ideia de “menos privacidade, mais segurança” é uma receita falsa. Partindo dessa premissa, a ideia do autor é baseada na pretensão do Estado, e mesmo entidades privadas, de conhecer tudo, inclusive aspectos mais íntimos de nossas vidas.

Com o avanço tecnológico, nascem novas ideias que modificam os valores e costumes da sociedade. A privacidade é um direito fundamental que está cada vez mais sendo ameaçado na sociedade da informação, tornando um grande desafio proteger este direito no ciberespaço. Uma quantidade cada vez maior de dados pessoais está sendo transferida em todo o mundo e os usuários estão perdendo o controle sobre os dados pessoais. Abrem-se assim possibilidades de uma série de consequências negativas.

A vida em meio à tecnologia tornou a vigilância e a concentração de dados, bem mais simples do que era antes, em consequência disso, as pessoas se tornaram cada vez mais acessíveis a qualquer tipo de invasão a sua privacidade.

No ciberespaço, a privacidade está ficando cada vez mais fragilizada, de modo que, além do usuário ser cada vez mais acessível a qualquer tipo de invasão na rede, sua privacidade também poderá ser violada através dos crimes que ocorrem na rede mundial de computadores, crimes estes que são tipificados como crimes cibernéticos por meio da invasão de dispositivos pessoais, uma vez que a utilização, por parte dos provedores de acesso ou quem quer que tenha a guarda de dados dos usuários configura crimes de natureza diversa.

Segundo a NCA (2016), cuja tradução livre identifica (Agência Nacional de Crime do Reino Unido), os crimes cibernéticos em 2015 foram responsáveis por 53% de todos os crimes ocorridos nos países que compõem o Reino Unido. Em outro relatório, a CNN *Business* em 2014 (PAGLIERY, 2014), constatou que quase a metade da população adulta dos EUA foram vítimas de algum ataque pela internet.

Observa-se que com a expansão do “mundo virtual” ou “ciberespaço”, a utilização da internet facilitou na prática de crimes já existentes, bem como a criação de novas práticas criminosas. Nesse sentido, de acordo com os dados relatados acima, os crimes cibernéticos estão atingindo grande parte da sociedade, de modo que, crimes estes que serão explicados no próximo capítulo.

3 CRIMES CIBERNÉTICOS

A tecnologia vem impactando em diversos aspectos vida, de modo que, ela também não deixaria de refletir no Direito Penal, apresentando um novo paradigma para esta área. O sistema informático transformou-se também em instrumento para prática dos atos delituosos. Portanto, não há dúvidas que a extensão da tecnologia implicaria na prática de condutas ilícitas específicas.

Tudo que se faz na internet ou em sistemas informáticos deixa rastros. Muitos desses rastros evidentemente não serão visíveis em primeiro contato. O fato de se utilizar um telefone celular, torna possível localizá-lo não só pelo GPS, mas também pelo próprio sistema das ondas e antenas. Isto é importante, pois, quando falamos em crimes cibernéticos existem basicamente duas perspectivas, aqueles crimes praticados por pessoas comuns, e aqueles praticados pelos hackers[3] (FREITAS, 2011).

Assim, deu-se a origem aos crimes cibernéticos, que são classificados pela doutrina como crimes próprios e impróprios. Neste sentido, Fabiano Kummer (2017 p. 25) classifica os crimes próprios:

> Onde os bens jurídicos violados são os próprios dados computacionais, e que só podem ser perpetrados por meio de sistemas de informática, sendo, sem esses, impossível a execução do ato e consumação do delito. São, em geral, delitos recentes, ou, até mesmo, crimes ainda não tipificados. Entre os crimes informáticos próprios mais comuns no Brasil, citamos: invasão a dispositivos informáticos para furtos de senhas, obtenção e transferência ilegal de dados; dano a banco de dados ou sistemas de informação; disseminação de vírus; ataques de phishing (expediente em que a vítima é levada a acessar anúncios falsos, em determinados links, e que, uma vez acessados, baixam na máquina um programa autoexecutável (Cavalo de Troia), ou Keylogger, ambos destinados à captura de senhas); socialengineering (um tipo de fraude virtual, ou estelionato virtual, na qual o usuário é induzido a preencher determinado formulário tido como confiável, mas, na verdade, está fornecendo dados para que os criminosos tirem vantagens, invariavelmente senhas de bancos); pharming, que é a técnica pela qual se modificam os servidores de nome de domínio (Domain Name System Servers, DNS), para que o mesmo conduza a um endereço que contenha um site falso, que, invariavelmente, coletará dados sigilosos do usuário; e outros.

Entende-se que os crimes próprios são aqueles cometidos contra um sistema informático, seja qual for a motivação do agente, por exemplo, invasão a dispositivos

3 Aquele que invade sistemas informáticos em benefício próprio, obtendo dados e informações alheias (informações, documentos, programas etc.), ou aquele sujeito com alto grau de conhecimento informático que em tese praticaria condutas voltadas ao interesse econômico ou pessoal.

informáticos para furtos de senhas, obtenção e transferência ilegal de dados, dano a banco de dados ou sistemas de informação, disseminação de vírus, etc.

Deste modo, Fabiano Kummer (2017 p. 24) também classifica os crimes impróprios:

> Apesar de serem cometidos por meio de sistemas informatizados, poderiam sê-lo, independentemente do sistema informatizado, violando bens jurídicos já protegidos no Código Penal. Entre os crimes informáticos impróprios mais comuns no Brasil, destacamos: extorsão, falsidade ideológica, ameaça, pornografia infantil, furto qualificado por fraude (art. 155, §4º, II, CP), estelionato (art. 171, CP), induzimento, instigação ou auxílio ao suicídio (art. 122, CP), dentre outros.

O autor deixa claro que os crimes impróprios são tradicionalmente tipificados em nosso ordenamento jurídico, no entanto, sua prática se dá em meio ao sistema informático, sendo considerados os crimes impróprios a extorsão, falsidade ideológica, ameaça, pornografia infantil, furto qualificado por fraude, estelionato, entre outros.

Neste sentido, os crimes próprios são aqueles praticados na maioria das circunstâncias por hackers, independentemente da consecução de outro resultado que não a violação de bem jurídico ligado à privacidade do agente, desde que esteja configurada a vontade deliberada de praticar a conduta delituosa. Enquanto os crimes impróprios são aqueles praticados por qualquer pessoa, o que inclui os hackers, voltados à violação de bens jurídicos diversos protegidos por tipos penais outros, os quais têm como meio da execução da conduta o meio digital.

Considerando que este trabalho pretende abordar apenas os crimes próprios, uma vez que são estes os que protegem a privacidade das informações dos usuários na rede, passa-se à análise das condutas que são tipificadas pela legislação penal para o combate a estes crimes.

3.1 Condutas que violam a privacidade

Antes de tratar das tipificações penais específicas, é preciso compreender que a tipificação penal não é um fim em si mesmo, uma vez que se volta à proteção de um bem jurídico da pessoa, o qual pode ser violado de tal forma que a coação às

práticas que potencialmente lhe removem efetividade deve se dar através da *última ratio* do Direito, qual seja o Direito Penal.

Neste caso, é preciso, preliminarmente, conhecer as ações que tem, ainda que potencialmente, o condão de violar direitos do usuário, notadamente, a sua privacidade. Destaque-se que não se trata de um rol exaustivo, resumindo-se à enumeração de condutas já conhecidos pelo campo jurídico.

3.1.1 Acesso não autorizado

O acesso não autorizado se dá a partir de uma invasão ou do simples acesso a qualquer dispositivo informatizado, em que a conduta do infrator ao acessar este dispositivo ocorre de forma não autorizada, motivada desde o mero interesse de superar os desafios técnicos de segurança, até pela intenção de fraudar e manipular dados. Caracteriza-se, portanto, no acesso não autorizado ao espaço de privacidade alheio, com a finalidade de obter, com objetivos diversos, as informações sigilosas do usuário.

O administrador do sistema é um elemento que tem plenos poderes em relação aos armazenamentos de dados. Isso não significa que o mesmo esteja livre para fazer qualquer conduta. Seu amplo acesso é para a operacionalização e administração do sistema, nunca para arbitrariedades (FREITAS, 2011). Ou seja, caso o administrador do sistema tem acesso a todas as contas do e-mail, ele não poderá acessar apenas pela sua curiosidade, mas sim meramente para operacionalização do sistema.

A falta de segurança é o principal indício para que ocorra a invasão e roubo de dados do usuário. A prática mais comum de invasão de dispositivo informático é o Ransomware[4], também conhecido como sequestro de dados. O sujeito ativo que destas condutas são denominados “Crackers”. Sobre o conceito de crackers Marcelo Xavier (2011, p. 93) versa:

> Esses podem ser considerados os verdadeiros criminosos da rede. Eles se divertem com destruições de sites e sua repercussão na imprensa. São

4 Espécie de software malicioso que, utilizando criptografia ou compactação de dados com senha, torna refém as informações digitais de suas vítimas, exigindo pagamento para sua recuperação.

> também ladrões, valendo-se da internet para roubar dinheiro e informações. O cracker é aquele que, basicamente, “quebra” um sistema de segurança, invadindo-o. Fanáticos pelo vandalismo, também adoram “pichar” páginas da web deixando, na maioria das vezes, mensagens de conteúdo ofensivo e racista.

Os crackers atuam de modo a obter informações de diversas formas, informações estas que são pessoais e sigilosas. Neste caso, a violação ao sigilo destas informações é uma violação à privacidade.

São condutas que se consumam pelo simples contato com o dado do usuário, que a partir delas encontra-se exposto àquele que os acessam. Neste caso, o objeto da proteção é o sigilo do dado ou, dito de outro modo, a segurança das informações pessoais contidas nos dados objeto do acesso não autorizado.

3.1.2 Transferência ilegal de dados

O acesso aos dados de um computador ligado à rede pode se desenvolver de muitas formas. Atualmente, uma forma muito comum de se obter dados de usuários se dá através dos spywares[5], vulgarmente chamados de vírus. Os spywares são códigos maliciosos capazes espionar o que o usuário faz na rede, especialmente as práticas de origem confidencial do usuário ou aquelas que dizem a respeito à intimidade do indivíduo.

Quanto a este tipo de softwares espiões, é possível encontrá-los nas mais variadas formas, a exemplo dos *keyloggers*[6]. Este tipo de programa consegue capturar todos os dígitos que o usuário tecla em seu computador. É, portanto, de extrema valia para aquele que deseja obter esses dados de forma ilícita, podendo capturar senhas de contas bancárias, números e códigos de cartões de créditos, login de acesso a sistemas diversos, dentre outros.

Estas condutas se consumam pela instalação do vírus no sistema do usuário, que a partir destes aplicativos maliciosos o usuário encontra-se exposto àquele que

---

5 Spyware consiste em um programa que rastreia informações do usuário contidas em seu computador, recolhendo informações sobre o usuário, seus costumes na Internet e transmite essa informação a uma entidade externa na Internet, sem o conhecimento e consentimento do usuário.

6 Keylogger é um programa criado para gravar tudo o que uma pessoa digita em um determinado teclado de um computador. Ele é um programa do tipo spyware e é utilizado quase sempre para capturar senhas, dados bancários, informações sobre cartões de crédito e outros tipos de dados pessoais.

detêm o controle do spyware. Neste caso, o objeto da proteção é, novamente, o sigilo do dado ou, dito de outro modo, a segurança das informações pessoais contidas nos dados objeto da espionagem.

3.1.2.1 Phishing

Phishing é uma forma de fraude na internet, na qual um *scanner* ou hacker, finge ser uma pessoa ou organização legítima com o intuito de roubar informações pessoais do usuário. Uma forma muito comum que vem sendo empregada opera através dos e-mails, que enviam informações para tentar enganar o usuário, almejando que este revele informações pessoais, a exemplo de informações financeiras como os números de cartões de créditos ou senhas. Este é um dos golpes mais comuns na Web, por isso os criminosos cibernéticos estão modificando constantemente a forma dos seus ataques para incluir cada vez mais detalhes, pretendendo fazer o usuário acreditar que aquilo não é um golpe e aquela página é legitima.

Diversos assuntos são usados para atrair a curiosidade do usuário, como um suposto site de vendas que pede para que se confirmem ou se modifiquem informações da suposta conta do usuário clicando em um determinado link. O grande problema é que muitos desses links podem não direcionar o consumidor até os sites de vendas, mas sim para um site onde um arquivo que poderá instalar um *keylogger* no sistema, conforme já explicado no tópico anterior. Com isso, viola-se o sigilo das informações que o usuário digita, incluindo suas senhas pessoais. O mesmo link também pode levar a um site de vendas falso, pedindo para o usuário inserir suas informações pessoais. Neste segundo caso, o crime é impróprio, porque dado por vício na manifestação da vontade do agente, isto é, trata-se de crime de estelionato praticado através da internet, o que não é um crime próprio.

3.1.3 Ataque de negação de serviço / DoS

O “denial of service” (DoS) ou a negação de serviço, são ataques que tem como objetivo tirar do ar um ou vários servidores (também chamado de DDoS – Ataque de negação de serviço distribuído) que prestam informações, ou seja, em um ataque “DoS”, computadores são utilizados para tirar do ar um servidor de informações. Durante o ataque, o servidor recebe muitas informações que são enviadas de outro computador, gerando uma sobrecarga durante o processamento de dados, de modo que o servidor acaba não conseguindo processar o trafego constante desses dados, cedendo ao ataque e ficando indisponível na rede, ou seja, impossibilitando o usuário comum acessar este servidor na web.

Evitar um ataque DoS exige muito conhecimento técnico, pois, se o fluxo de dados chegar ao provedor desprotegido, o mesmo não conseguirá bloqueá-lo, uma vez que sua função não é bloquear esse fluxo dados, mas sim transmiti-lo para o servidor. Quando o fluxo dados chegarem no servidor, o mesmo precisará de algum dispositivo técnico para o tratamento desses dados, sem a devida proteção, o servidor não conseguirá se prevenir do ataque. Existem equipamentos que detectam os IP[7] (Endereço de Protocolo da Internet) de origem repetida e que começam a bloquear este trafego. É, ainda assim, possível que o condutor do ataque perceba este movimento e comece a mudar a origem do IP, gerando uma o que se costuma chamar de guerra cibernética.

No ordenamento brasileiro, ainda não há nenhum caso de condenação que tenha envolvimento em ataque DoS. É importante destacar que o ataque DoS pode ter alguns efeitos colaterais e são estes efeitos que importam para os fins que se pretende este trabalho. Entre os efeitos colaterais de um ataque DoS é possível a potencialização das condutas anteriormente descritas, ante o dano resultante que o ataque causou. Este tipo de ataque é muito usado como o pontapé inicial para a prática de outros crimes cibernéticos (próprios) como a quebra do sigilo de dados e das informações, aproveitando-se da fragilidade do servidor no momento dos ataques.

3.2 A tutela da privacidade na rede: a *surface* e a *deep* web

7 Endereço IP (Internet Protocol) é um número que identifica o computador ou qualquer dispositivo eletrônico na rede.

Os maiores mecanismos de busca de hoje podem prever sua pesquisa, interpretar consultas com várias palavras e veicular inúmeras páginas da web. Esses mecanismos de buscas funcionam como “rastreadores” de URL. Deste modo, como os mecanismos de busca examinam a superfície do que está on-line, os sites exibidos nos resultados são parte do que é chamado de surface web, ou seja, o objetivo é de organizar todas as informações na rede e torná-la mais acessível para o usuário.

Todos esses sites que atuam na surface web, contam – ou ao menos devem contar, segundo a legislação brasileira – com um sistema de segurança para que seja possível armazenar os dados daqueles que acessaram seu provedor, o que permite rastear individualmente o usuário que praticou as condutas anteriormente descritas.

Entre os dispositivos legais do marco civil, está a obrigação das empresas provedoras de conexão à internet de armazenarem informações fundamentais para identificação de autoria e comprovação de materialidade. Deste modo, os provedores com o marco civil da internet, passaram a ter obrigação de armazenar os registros cadastrais de conexão (logs), determinando pelo prazo de 1 (um) ano destacando no seu art. 13 na subseção da guarda de registros de conexão (BRASIL, 2014):

> Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.

Desta forma, entende-se que os registros de conexão são transformados em instrumentos probatórios mediante ordem judicial. Além do dever de guarda, o artigo também trata que o registro seja mantido em ambiente controlado e de segurança, pois, registros esses são informações relativas a privacidade do usuário.

Porém, engana-se aquele que pensa que tudo o que é acessível pela internet pode ser encontrado na surface web. Há um outro lado da rede, conhecido como deep web.

A deep web, genericamente falando, seria toda parte da internet que não é indexada nos motores padrões de buscas ditos anteriormente (BERGMAN, 2001). A

grande dificuldade na deep web encontra-se na identificação dos usuários que usam deste meio para praticar as condutas criminosas anteriormente descritas.

Este lado da rede tem sua conexão p2p (Peer-to-Peer) por ser descentralizada, fugindo dos protocolos padrões, ou seja, a deep web independe de um servidor central, mobilizando uma arquitetura de rede em que o usuário funciona tanto como cliente quanto como servidor, permitindo assim o compartilhamento de dados sem a necessidade de um servidor central.

A razão dessa dificuldade de identificar os usuários é o anonimato, ou seja, os dados que circulam na deep web são criptografados ou escondem-se no sistema de túneis de acesso. Como os sites não estão indexados aos padrões de busca da suface web, o usuário acessa um site, que o leva a outro, este a outro e assim sucessivamente. Torna-se, portanto, praticamente impossível rastrear o percurso trilhado, em função das sucessivas trocas de servidor, os quais nem sempre submetem-se às regras de proteção de dados mundialmente difundidas. Em relação ao acesso anônimo da deep web, Fabiano Kummer (2017, p. 60) explica:

> Essa característica do acesso anônimo aos sites lá encontrados leva à prática de atos ilegais, que, se fossem expostos à luz do Google, muito provavelmente, não seriam praticados. Seria mais ou menos como se você fosse invisível (e aí cabe um exercício de consciência pessoal, ao nos perguntarmos: “O que faríamos se fôssemos invisíveis?”). Fica na consciência de cada um; e no dever das autoridades, de não dar as costas a este mundo virtual.

Entende-se que a deep web é um pedaço da rede onde as pessoas querem se manter isoladas pelo zelo da sua própria privacidade ou tornando-se um espaço grave para execução de crimes cibernéticos. Segundo a delegada da polícia federal Diana Calazans Mann (POLÍCIA FEDERAL, 2018), o Brasil é o terceiro país do mundo a fazer a identificação de usuários da deep web, focando na exploração sexual infantil em razão da gravidade deste assunto. Os infratores são pessoas que sabem o que estão fazendo, usando daquele lado da rede para se esconder, aproveitando das ferramentas ali presentes, para dificultar sua identidade na rede.

A polícia federal vem desenvolvendo uma operação chamada “Underground”, a fim de combater os criminosos que aproveitam deste anonimato na rede para o cometimento de atos ilícitos, focada na distribuição de imagens e vídeos de exploração sexual infantil. Em abril de 2018 a segunda fase da operação

Underground resultou na identificação de um grupo de produtores deste tipo de material por conta das modernas técnicas desenvolvidas pela polícia federal, chegando a um grupo integrado por 13 pessoas que faziam parte deste comércio de imagens ilícitas.

A identificação dos usuários que cometem crimes cibernéticos na deep web é uma tarefa bastante complicada, pois uma coisa é você identificar uma pessoa através da surface, onde há o registro de dados e outra é identificar na deep web, por conta dos dados criptografados e do anonimato.

É importante destacar como ocorrem as transações financeiras na deep web, as quais são feitas, normalmente, por meio de moeda virtual. Usualmente, a moeda corrente é o Bitcoin[8], uma moeda virtual criada em 2008, que permite a transferência virtual de um dispositivo informático para outro, sem a intermediação de qualquer instituição financeira. É um tipo de criptomoeda, ou seja, não pode ser rastreada, em função da sua criptografia. Além de ser uma moeda já difundida para fins legais, é muito usada no mercado ilegal da deep web, justamente por ser uma moeda que não permite rastrear transações financeiras na rede. Neste caso, não apenas a prática de ilícitos é acobertada pela criptografia ou pelo anonimato, mas também a forma de pagamento para financiar determinadas condutas ilícitas também o é.

O acesso a deep web, ainda assim, não é ilegal. Muitos utilizam desta parte da rede como uma forma de anonimato e privacidade total, assim como os jornalistas usam para conversarem com fontes anônimas, até mesmo manifestantes que vivem em países onde há um governo totalitário, usam a deep web como um meio de denúncia e ação política. Não se trata, portando, diga-se, desde logo, de um apoio à criminalização ou à determinação da ilegalidade desta parte da rede, mas apenas do destaque de que a falta de determinações legais específicas globalmente aplicáveis, tornam-na praticamente imune aos esforços de combate às ilegalidades que nela são praticadas.

---

8 Bitcoin é um sistema de dinheiro eletrônico peer-to-peer (um tipo de moeda onde nós somos os próprios usuários, e que não permite identificar o emissário e o receptor da moeda). É uma rede de consenso que permite um novo tipo de método de pagamento e uma forma de dinheiro totalmente digital. É a primeira rede de pagamento peer-to-peer descentralizada que é alimentada por seus usuários sem autoridade central ou intermediários. Do ponto de vista do usuário, o Bitcoin talvez seja melhor descrito como “dinheiro para a Internet”.

4 COMBATE AOS CRIMES CIBERNÉTICOS PRÓPRIOS: TIPOS PENAIS, SEUS PROBLEMAS E POSSÍVEIS SOLUÇÕES

O Código Penal consagra em seu art. 1° o princípio da legalidade: “Não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal” (BRASIL, 1940). Deste modo, o Estado só poderá punir crimes tipificados em lei. Além do princípio da legalidade, deve-se considerar também o princípio da anterioridade, a partir do qual lei penal não retroagirá, salvo para beneficiar o réu (BRASIL, 1988).

Neste aspecto, para os crimes cibernéticos impróprios, não há que se inovar, pois tipos penais dos mais diversos já estão definidos em lei e estes crimes, especificamente, materializam-se na utilização de meios informáticos para sua prática. Os meios digitais são, portanto, mero instrumento para a prática dos crimes impróprios, assim como o é, por exemplo, uma arma para a prática de um homicídio ou de um roubo.

Há, no entanto, os crimes cibernéticos próprios, aqueles que objetivam a proteção de bens jurídicos ligados à difusão e violação de conteúdos através dos meios informáticos. Pela característica dinâmica da sociedade da informação, novos potenciais ilícitos informáticos manifestam-se a cada momento e novas formas de violação de direitos dos usuários são perceptíveis, de maneira que a legislação penal precisa ser aparelhada para lidar com os acontecimentos do ciberespaço, sem o que apenas se difundiria a insegurança.

Portanto, a legislação brasileira precisa de soluções normativas para a proteção dos usuários, bem como para o combate dos crimes que ocorrem no ciberespaço. Este último aspecto, de caráter eminentemente penal, é o que passa a ser objeto deste capítulo.

4.1 A legislação aplicável aos crimes próprios

No ordenamento brasileiro, há normas específicas para a incriminação do acesso não autorizado para as pessoas em modo geral e para funcionário público,

em específico. Neste último caso, o Código Penal (BRASIL, 1940) tem a seguinte redação:

> Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano: Pena – reclusão, de 2 (dois) a 12 (doze) anos, e multa
> Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente: Pena – detenção, de 3 (três) meses a 2 (dois) anos, e multa.

Observa-se que ambos os artigos tratam, como já apontado, de crimes praticados por funcionário público. No art. 313-A a ação delitiva poderá se perfazer tanto pela prática dos atos apontados no tipo, quanto pela facilitação para que tais atos sejam praticados. Neste caso, as ações típicas envolvem a inserção de dados falsos, bem como a alteração ou exclusão de dados corretos. Trata-se, portanto, de norma voltada ao combate da transferência ilegal de dados disponíveis em sistemas informáticos ou a bancos de dados da Administração Pública. Destaque-se, por fim quanto a este dispositivo, que não só almejando o recebimento de vantagem indevida para si ou para terceiro poderá o funcionário público incidir em tal tipo, mas também o fará se praticar qualquer destas ações para produzir algum tipo de dano.

Quanto ao art. 313-B, o objeto da proteção é a integridade dos sistemas de informações ou dos programas de informáticas utilizados pela Administração Pública, portanto, o objeto aqui é, em linha de princípio, a proteção contra o acesso não autorizado, podendo também ser classificado como um ataque de navegação, a depender da alteração realizada. Para tanto, são puníveis os atos que modifiquem ou alterem sem autorização os códigos fontes destes programas ou sistemas informáticos. Não há, no art. 313-B previsão da facilitação, ainda assim, parece imputável o tipo àquele que em conluio com funcionário público responsável pela facilitação do acesso, pratica os atos típicos previstos neste dispositivo. Se isto for verdade[9], em ambos os dispositivos, mesmo que interrompido o *iter criminis* antes da manipulação dos dados ou do código fonte, o fato típico poderá ser imputado ao, uma vez que já configurado o acesso não autorizado, desde que se demonstre a intenção de produzir qualquer dos resultados previstos.

---

9 Ainda que não o seja quanto ao art. 313-B, o será para o art. 313-A.

É importante notar também, especialmente quanto a este último dispositivo em comento, que se o ato for praticado por um ou mais indivíduos, “por razões de xenofobia, discriminação ou preconceito de raça, cor, etnia e religião, quando cometidos com a finalidade de provocar terror social ou generalizado, expondo a perigo pessoa, patrimônio, a paz pública ou a incolumidade pública” (BRASIL, 2016), com objetivo de “sabotar o funcionamento ou apoderar-se” (BRASIL, 2016) de serviços públicos essenciais, notadamente aqueles elencados no art. 2º, IV da Lei n.13.260/2016, que está-se diante de hipótese de crime de terrorismo, consubstanciado no ataque de navegação para os casos de sabotagem e/ou, para os casos de apoderamento, também de transferência ilegal de dados, bastando, nestes casos que os sistemas de gestão destes serviços públicos sejam informáticos.

Mais recentemente, a Lei nº 12.737/2012, conhecida como “Lei Carolina Dieckmann”, trouxe uma importante inovação no combate ao crime de invasão de dispositivo informático alheio. O Projeto de Lei n° 2.793/2011, apresentado pelo deputado Paulo Teixeira já estava percorrendo normalmente seu procedimento no congresso, juntamente a vários outros versando sobre o mesmo tema. Contudo, em maio de 2011, ocorreu o furto de 36 fotos íntimas da atriz Carolina Dieckmann, caso que teve grande destaque na mídia. O fato ocorreu quando a atriz levou seu computador para a manutenção técnica, posteriormente ela sofreu chantagens para se evitasse divulgação dessas fotos, as quais acabaram por ser expostas na internet.

Na data dos fatos, mesmo frente a lacuna normativa específica quanto ao crime cibernético próprio, os cinco responsáveis pelo caso foram julgados e condenados pelo crime de extorsão, furto e difamação. Até então, não havia nenhum tipo criminal de invasão de dados de sistemas informatizados. Por conta deste caso e face à grande repercussão na mídia, acelerou-se o processo legislativo do mencionado projeto de lei, promulgando-se ao final a Lei n. 12.737/2012, sancionada em 03 de dezembro de 2012. Esta lei, alterou o Código Penal (BRASIL, 2012) e tratou de inserir e definir como crime o seguinte tipo:

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

> vulnerabilidades para obter vantagem ilícita: Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa.

Na verdade, o inteiro teor do artigo acima mencionado tipificou diversas condutas, notadamente o acesso sem autorização a dispositivos informáticos alheios e a transferência ilegal de dados. O *caput* acima transcrito, por si só, aborda os atos ligados ao acesso não autorizado. Desta forma, independentemente do dispositivo estar conectado à internet, preenchidas concomitantemente três condições: (a) violação de mecanismo de segurança; (b) com intenção de modificar, extrair ou apagar os dados de qualquer dispositivo e; (c) ante a falta a autorização, expressa ou tácita, do proprietário do aparelho, estará configurado o acesso não autorizado. Na parte final, o dispositivo ainda imputa a mesma consequência àquele que instalar *spyware* em aparelho alheio.

Em qualquer dos casos, não será necessária a violação do sigilo dos dados do usuário ou do proprietário de aparelho, bastando a intenção de violar o sigilo, o que se manifesta pela invasão ou pela instalação do vírus. Quanto a esta última hipótese, observe-se, adicionalmente, que ela também envolve os casos de tentativa de *phishing*, nos quais instala-se um aplicativo malicioso nos equipamentos informáticos. Complementarmente, o parágrafo 1° (BRASIL, 2012), determina: “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”; e o parágrafo 2º deste mesmo artigo revela informação relevante, quando ao aumento da pena da invasão caso sua consumação resulte em prejuízo econômico (BRASIL, 2012).

O crime será qualificado, caso a invasão viole (i) o sigilo das comunicações, (ii) segredos comerciais ou industriais, (iii) informações sigilosas, ou ainda, (iv) resulto no controle, por parte do invasor, do próprio aparelho invadido (BRASIL, 2012), para o que poderá a pena ser aumentada no caso da transferência ilegal destes dados (BRASIL, 2012). Destaque-se, por fim, outra cláusula de aumento de pena, casos quaisquer dos atos típicos seja praticado em face de autoridades da república, nos termos do § 5º (BRASIL, 2012).

Note-se, por fim, quanto a este artigo, que suas previsões complementam aquelas já comentadas quanto aos artigos 313 A e B, uma vez que nestes últimos trata-se de crime praticado por funcionário público, enquanto na previsão da

alteração promovida no CP pela Lei Carolina Dieckmann o crime cibernético próprio pode ser praticado por qualquer pessoa, tendo como vítima tanto o cidadão, quanto entidades jurídicas diversas, o que envolve as pessoas jurídicas que compõem o Estado.

A mesma lei também acrescentou os parágrafos 1° e 2° ao artigo 266 do Código Penal (BRASIL, 1940) que traz o crime de interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública.

> Art. 266 – Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento:
> Pena – detenção, de um a três anos, e multa.
> § 1° Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.
> § 2° Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública.

Esta espécie de interrupção ou perturbação de serviços, cuja prestação contemporânea se dá mediante a ampla utilização de redes cibernéticas, especialmente quanto aos serviços telemáticos, poderá ser feito por meio de ataque de negação de serviço (DOS/DDOS), como já explicado no capítulo anterior. Trata-se de previsão específica que alberga serviços não expressamente previstos pela proteção conferida pela Lei Antiterrorismo.

4.2 Da dificuldade em se definir a autoria dos crimes cibernéticos próprios

No ciberespaço, nem sempre é uma tarefa fácil a obtenção dos indícios de autoria e comprovação de materialidade. Na seção anterior, teve-se uma ideia das legislações aplicáveis aos crimes cibernéticos próprios, porém grande parte não faz jus a técnica, dando margem a interpretações imprecisas, dificultando assim na sua aplicabilidade. A Convenção de Budapeste (UNIÃO EUROPEIA, 2001), que será objeto de análise a seguir, especialmente em função das regras processuais que propõe, aponta de forma mais específica as ações que devem ser consideradas criminosas pelos países signatários deste tratado.

Cite-se, como exemplos, o uso abusivo de dispositivos, que compreende não apenas, mas também: “uma palavra-passe, um código de acesso ou dados informáticos semelhantes que permitam aceder a todo, ou a parte de um sistema informático com a intenção de serem utilizados para cometer qualquer uma das infracções definidas nos Artigos 2º a 5º” (UNIÃO EUROPEIA, 2001) e; a falsidade informática, voltado ao combate da

> Introdução, a alteração, a eliminação ou a supressão intencional e ilegítima de dados informáticos, produzindo dados não autênticos, com a intenção de que estes sejam considerados ou utilizados para fins legais como se fossem autênticos, quer sejam ou não directamente legíveis e inteligíveis (UNIÃO EUROPEIA, 2001).

A Lei n° 12.737/2012 pode ser considerada um avanço ao ordenamento jurídico do país, no entanto, não é suficiente para solucionar o problema legislativo relativo aos crimes cibernéticos, uma vez que não basta a mera previsão dos tipos penais elencados anteriormente. Em contrapartida, o Direito Penal material também precisa vir acompanhado de uma atualização dos dispositivos processuais, sem o que a própria legislação material terá sua eficácia diminuída. O problema processual é sobretudo a ineficácia dos dispositivos voltados à produção de provas ligadas à autoria delitiva.

O ciberespaço tem caráter global, não conhece limites territoriais, portanto, transcende fronteiras. Em função desta transnacionalidade, é necessário um maior grau cooperação internacional dentre os órgãos judiciários e investigativos de diferentes países. Em busca de intensificar a cooperação nesta matéria, em 23 de novembro de 2001, na capital da Hungria, Budapeste, foi firmada a Convenção do Conselho Europeu sobre o Cibercrime, conhecida como Convenção de Budapeste (UNIÃO EUROPEIA, 2001). Tal convenção é, na verdade, um tratado internacional multilateral de Direito Penal e de Direito Processual Penal, voltado a garantir, sobretudo, a efetividade das investigações e ações penais que combatem os crimes cibernéticos, regulamentando e facilitando a obtenção do conjunto probatório.

Atualmente a convenção está ratificada por 61 nações, número que inclui os membros da União Europeia e também países que não pertencem a este bloco, como os Estados Unidos, o Canadá, o Japão, a Argentina, o Chile, entre outros. Até a data consultada para fins de desenvolvimento deste trabalho, o Brasil ainda não

havia se tornado signatário da Convenção de Budapeste. Do Preâmbulo da Convenção de Budapeste (UNIÃO EUROPEIA, 2001), destaca-se:

> Convictos da necessidade de prosseguir, com carácter prioritário, uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adoção de legislação adequada e da melhoria da cooperação internacional.
> Reconhecendo a necessidade de uma cooperação entre os Estados e a indústria privada no combate à cibercriminalidade, bem como a necessidade de proteger os interesses legítimos ligados ao uso e desenvolvimento das tecnologias da informação.

Evidencia-se que a luta contra a criminalidade no ciberespaço somente será eficientemente combatida se houver cooperação entre os diversos países que hospedam os serviços ligados à internet. Ante a ausência de regulamentação internacional, especialmente de tratados internacionais de uniformização de procedimentos e de cooperação como esta convenção, basta ao infrator valer-se de sites hospedados em servidores no exterior ou de programas mantidos por companhias sem sede no Brasil, não submetidos, pois, à legislação brasileira que determina a guarda dos dados de acesso, para ter grandes chances de se evadir da própria persecução criminal.

Neste caso, à exceção dos crimes enquadrados conforme a Lei Antiterrorismo (BRASIL, 2016), que tem pena mais elevada, de ao menos 12 anos de reclusão, os demais atos típicos podem prescrever em um curto espaço de tempo, em alguns casos, a exemplo, do *caput* do art. 154-A do Código Penal (BRASIL, 1940), a prescrição ocorrerá em, no máximo 03 anos da data do fato. Isto ocorre em função da dificuldade da identificação das provas de autoria, frente a eventual demora ou mesmo a negativa de fornecimento de informações de usuários que se valeram de serviços sediados fora do território brasileiro.

Preocupação semelhante está expressa, por exemplo, na previsão inscrita no art. 18 da Convenção (UNIÃO EUROPEIA, 2001), o qual determina que os signatários deverão adotar

> As medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes para ordenar:
> a) A uma pessoa que se encontre no seu território que comunique os dados informáticos específicos, na sua posse ou sob o seu controlo e armazenados num sistema informático ou num outro suporte de armazenamento de dados informáticos; e

> b) A um fornecedor de serviços que preste serviços no território da Parte, que comunique os dados na sua posse ou sob o seu controlo, relativos aos assinantes e respeitantes a esses serviços.

Neste mesmo sentido, observam-se previsões relativas à busca e apreensão de dados já armazenados (art. 19), bem como à interceptação em tempo real de informações relativas ao próprio conteúdo do tráfego de dados, nos termos do art. 21 (UNIÃO EUROPEIA, 2001). Ao lado das disposições processuais específicas à reunião de provas estão aquelas destinadas ao auxílio mútuo, seja este solicitado por um signatário, seja mesmo através a informação espontânea, conforme arts. 25 e 26, respectivamente, da Convenção (UNIÃO EUROPEIA, 2001).

Um segundo problema, também ligado à ineficácia da legislação processual, diz respeito à falta de regulamentação especificamente voltada à deep web, isto é, às estruturas e subestruturas mais profundas da rede mundial de computadores. Neste aspecto, ainda que seja possível considerar suficientes as tipificações de crimes cibernéticos próprios, mesmo que se possa divergir quanto à justeza dos quantuns de pena, de qualquer modo, a própria natureza desta zona agrava o problema anterior, relativo à ineficácia dos dispositivos processuais tradicionais, uma vez que a própria estrutura é voltada à proteção do anonimato.

Previsões como aquelas que se depreendem da interpretação combinada dos artigos 16[10] e 17[11] da Convenção de Budapeste (UNIÃO EUROPEIA, 2001), os quais desenvolvem mecanismos de controle do tráfego dos dados e sua expedita divulgação ao signatário solicitante. No caso específico do art. 17, assegura-se à parte solicitante a divulgação de informações relativas ao tráfego de dados e a via de sua transmissão, a partir das quais deve ser possível rastrear, dentro do sistema de túneis da deep web, o caminho percorrido pelo cibercriminoso, contribuindo para a reunião de provas da autoria do delito.

Sem uma previsão desta natureza, paradoxalmente, a investigação de crimes praticados na deep web dependeria da prática de condutas como as elencadas no

10 O artigo 16 dispõe: “cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para permitir às suas autoridades competentes exigir ou obter de uma outra forma a conservação expedita de dados informáticos específicos, incluindo dados relativos ao tráfego, armazenados por meio de um sistema informático, nomeadamente nos casos em que existem motivos para pensar que os mesmos são susceptíveis de perda ou alteração” (UNIÃO EUROPEIA, 2001 – grifos próprios).

11 O art. 17 dispõe que cada parte deverá “assegurar a divulgação rápida à autoridade competente da Parte ou a uma pessoa designada por essa autoridade, de uma quantidade de dados de tráfego, suficiente para permitir a identificação dos fornecedores de serviços e da via através do qual a comunicação foi efectuada” (UNIÃO EUROPEIA, 2001 – grifos prórios).

capítulo 3.1, as quais não consubstanciariam crimes, uma vez realizadas com autorização judicial. Neste caso, imperioso é considerar que a invasão de dispositivos de suspeitos da prática de ilícitos nas profundezas da web seria medida análoga à quebra de sigilos telefônico, mais especificamente à realização de um "grampo telefônico", ainda que ausente previsão normativa específica para esta espécie de "grampo de dados". Nesta hipótese, as autoridades policiais precisariam, a não ser que deixadas à própria sorte, hackear computadores ou outros dispostivos de suspeitos pela prática de crimes e segui-los pelos sistemas de túneis da deep web, encontrando as provas necessárias à imputação e eventual condenação pela prática de ilícitos.

Em 2015 o FBI no leste da Virgínia – Estados Unidos – usou uma ferramenta para hackear e identificar o Endereço de IP dos usuários que acessavam um site de abuso infantil por meio do Tor[12], chamado Playpen (RAYMOND, 2017). Apenas 01 (um) mês após o site ser lançado em 2014, já se contavam mais de 60.000 (sessenta mil) membros registrados. Em 2015 esses registros já haviam ultrapassado para 215.000 (duzentos e quinze mil) contas. Após o esforço do FBI, foi possível derrubar o site, transferindo os arquivos do mesmo para o servidor local da corporação, permitindo se identificar os usuários que acessavam o material ilícito, resultando em provas suficientes para instrução probatória. A corporação conseguiu identificar apenas 1.000 (mil) dos usuários em função da não prestação de informações pelos servidores do sistema de túneis e pelo próprio Tor, cujo mercado assenta-se na oferta de anonimato.

Em qualquer destes dois casos, seja na surface ou na deep web o sistema processual precisa se globalizar. A ausência de normas regulamentadoras dos registros de *logs* na web permite-se, no caso da deep web, estimula-se a prática de ilícitos que se valem do anonimato para serem perpetrados. Sem um sistema mundial de cooperação e de combate aos cibercrimes os sistemas processuais estarão deixados à própria sorte. De um lado, o criminoso pode contar com a negativa dos sistemas jurídicos de outros países em fornecer dados de acesso e, de outro lado, pode se valer do anonimato da deep web para percorrer e se hospedar

12 The Onion Router (Tor) é um programa de software de código aberto que permite aos usuários a proteção de sua privacidade e segurança contra uma forma comum de vigilância da Internet conhecida como análise de tráfego. O Tor foi originalmente desenvolvido para a Marinha dos EUA em um esforço para proteger as comunicações do governo.

em servidores mundo afora, dificultando a própria identificação de em qual país deve estar registrada determina operação realizada na rede.

5 CONCLUSÃO

A própria arquitetura da internet acaba sendo um fator que molda, possibilita e limita comportamentos, circunscreve também a eficácia da regulação jurídica. Consequentemente, a tecnologia está transformando globalmente o sistema jurídico, à medida que as relações da sociedade têm se tornado cada vez mais vinculadas ao ciberespaço.

Neste cenário, a atualização das disposições normativas protetivas da privacidade é algo fundamental. O Direito Penal material e, especialmente, o formal precisam se adequar, não apenas para digitalizar-se, mas também para prever e punir aqueles que praticam ilícitos contra a segurança dos dados e de seu tráfego na rede mundial de computadores. Observa-se que o sistema jurídico não deve caminhar em direção da mera tipificação dos crimes informáticos. É preciso considerar igualmente as especificidades das relações que se desenvolvem em um curto espaço de tempo e de forma fluida, características mundiais do ciberespaço.

Os tratados internacionais e a exemplo da Convenção de Budapeste, apresentam-se como um caminho, pois a cooperação internacional é imprescindível, já que muitos dos delitos praticados contra usuários da internet assumem contornos transnacionais e podem implicar em problemas quanto a aplicação da lei penal. Do mesmo modo, há que se considerar que é possível se valer da deep web, onde não é uma tarefa fácil identificar um usuário que aproveita da sua estrutura, em função da natureza anônima das relações firmadas, para cometer delitos, os quais são mascarados ou mesmo ocultados pelo sistema de túneis.

Analisou-se no decorrer da pesquisa, a partir de uma mirada contemporânea sobre as novas formas do direito à privacidade, um conjunto de condutas que podem – e são – consideradas potencialmente ofensivas à integridade dos dados e de seu tráfego na internet. A partir de novas normas jurídico-penais, tipos específicos foram positivados para punir os crimes cibernéticos próprios. Há, neste aspecto, reflexões que precisam ser levadas a sério, tanto no que toca à suficiência das previsões do Direito Penal material, quanto aquelas afetas à efetividade destas ante a obsolescência do Direito Penal formal ou processual.

Se os crimes cibernéticos não são um problema exclusivamente nacional, é necessário reunir estrategicamente os países mundo afora, bem como é

imprescindível intensificar os mecanismos de cooperação internacional para harmonizar os procedimentos garantido a efetividade e a aplicação da lei penal, sem o que apenas de forma deficiente se promoverá a proteção dos Direitos Fundamentais do usuário da rede mundial de computadores.

REFERÊNCIAS BIBLIOGRÁFICAS

BERGMAN, Michael K. *The deep web: surfacing hidden value. Journal of Eletronic Publishing*. vol. 7, n. 1. Ann Arbor: Michigan Publishing, 2001. Disponível em: <https://quod.lib.umich.edu/cgi/t/text/idx/j/jep/3336451.0007.104/--white-paper-the-deep-websurfacing-hidden-value?rgn=main;view=fulltext>. Acesso em 04 de nov. de 2018.

BRASIL. *Tipificação Criminal de Delitos Informáticos*, Lei nº 12.737 de 30 de novembro de 2012 (texto compilado). Brasília: Diário Oficial da União, 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em 28 de setembro de 2018.

BRASIL. *Marco Civil da Internet*, Lei nº 12.965, de 23 de abril de 2014 (texto compilado). Brasília: Diário Oficial da União, 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em 28 de setembro de 2018.

BRASIL. *Código Penal*, Decreto-Lei nº 2.848, de 31 dezembro de 1940 (texto compilado). Rio de Janeiro: Diário Oficial da União, 1940. Disponível em: <http://www.planalto.gov.br/CCivil_03/Decreto-Lei/Del2848.htm>. Acesso em 28 de setembro de 2018.

BRASIL. *Constituição da República Federativa do Brasil* de 1988, 05 de outubro de 1988 (texto compilado). Brasília: Diário Oficial da União, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em 18 de nov. de 2018.

BRASIL. Lei de *Proteção de Dados Pessoais*, Lei n° 13.709, 14 de agosto de 2018 (texto compilado). Brasília: Diário Oficial da União, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em 29 de setembro de 2018.

BRASIL. *Lei Antiterrorismo*, Lei nº 13.260, 16 de março de 2016 (texto compilado). Brasília: Diário Oficial da União, 2016. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Lei/L13260.htm>. Acesso em 27 de nov. de 2018.

CAMARGO, Coriolano Almeida. *Direito digital: novas teses jurídicas*. 1. Ed. Rio de Janeiro: Lumen Juris. 2018.

CHERTOFF, Michael. *A public policy perspective of the Dark Web, Journal of Cyber Policy [online], 2017*. Disponível em: <https://www.tandfonline.com/doi/full/10.1080/23738871.2017.1298643>. Acesso em 29 de novembro de 2018.

FREITAS, Marcelo Xavier. *Crimes digitais*. 1. Ed. São Paulo: Saraiva. 2011.

HOVEN, Jeroen van den. Privacy and information technology*. In. Stanford Encyclopedia of Philosofy [online]*, 2014. Disponível em: <https://plato.stanford.edu/entries/it-privacy/>. Acesso em 29 de setembro de 2018.

KIM, Gang-Hoon.; Silvana Trimi.; Ji-Hyong Chung, Big-Data Applications in the Government Secto*. Communications of the CAM* [online]. vol. 57, n. 3. Nova Iorque, 2014. Disponível em: <https://cacm.acm.org/magazines/2014/3/172509-big-data-applications-in-the-government-sector/abstract>. Acesso em 25 de outubro de 2018.

KUMMER, Fabiano Ratton. *Direito Penal na sociedade da informação*. 1. Ed. Paraná. 2017

MACHADO, Joana de Moraes. *A expansão do conceito de privacidade e a evolução na tecnologia de informação com o surgimento dos bancos de dados.* Revista da AJURIS. vol. 41, n. 134. Piauí, 2014. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/206-263-1-sm.pdf>. Acesso em 25 de outubro de 2018.

MINISTÉRIO PÚBLICO DO ESTADO DE SÃO PAULO. CENTRO DE APOIO OPERACIONAL CRIMINAL. *Nova lei de crimes cibernéticos entra em vigor [online]*. São Paulo, 2013. Disponível em: <http://www.mpsp.mp.br/portal/page/portal/cao_criminal/notas_tecnicas/NOVA%20LEI%20DE%20CRIMES%20CIBERN%C3%89TICOS%20ENTRA%20EM%20VIGOR.pdf>. Acesso em 18 de nov. de 2018.

NATIONAL CRIME AGENCY, NCA *STRATEGIC CYBER INDUSTRY GROUP, Cyber Crime Assessment 2016 [online]*, 2016. Disponível em: <http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016>. Acesso em 25 de outubro de 2018.

PAGLIERY, Jose. Half of American adults hacked this year. *CNN Business [online]*, 2014. Disponível em: <https://money.cnn.com/2014/05/28/technology/security/hack-data-breach>. Acesso em 25 de outubro de 2018.

PINHEIRO, Patrícia Peck. *Direito Digital*. 6.ª Edição. Saraiva, São Paulo, 2016.

POLÍCIA FEDERAL, *PF combate distribuição de imagens pornográficas com crianças na deepweb.* São Paulo, 26 de abril de 2018. Disponível em: <http://www.pf.gov.br/agencia/noticias/2018/04/pf-combate-distribuicao-de-imagens-pornograficas-com-criancas-na-deepweb>. Acesso em 30 de setembro de 2018.

RAYMOND, Nate. U.S. court allows evidence from FBI child porn site probe. *Reuters [online]*, 2017. Disponível em: <https://www.reuters.com/article/us-usa-cyber-childporn/u-s-court-allows-evidence-from-fbi-child-porn-site-probe-idUSKBN1CW32V>. Acesso em 30 de novembro de 2018.

RODOTÁ, Stefano. *A Vida na sociedade da vigilância:* a privacidade hoje. Tradução: Maria Celina Bodin de Moraes. São Paulo. Renovar. 2007.

TEFFÉ, Chiara Spadaccini.; MORAES, Maria Celina B. Redes sociais virtuais: privacidade e responsabilidade civil. Análise a partir do Marco Civil da Internet. *Pensar*, Fortaleza. Disponível em: <http://periodicos.unifor.br/rpen/article/view/6272>. Acesso em 22 de setembro de 2018.

UNIÃO EUROPEIA. *Convenção sobre o Cibercrime.* Budapeste *[online], 2001*. Disponível em: <http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf>. Acesso em 21 de novembro de 2018.