Revista de Criminologias e Políticas Criminais

Organização Comitê Científico
Double Blind Review pelo SEER/OJS
Recebido em: 06.12.2021
Aprovado em: 17.12.2021

A REVOLUÇÃO TECNOLÓGICA E OS DELITOS DIGITAIS: UMA ANÁLISE DA (IN) SUFICIÊNCIA LEGISLATIVA BRASILEIRA

Camila Giovana Xavier de Oliveira Frazão[1]
Ricardo Alexandre Lopes Assunção[2]
Thainá Penha Pádua[3]

Resumo: Objetiva-se investigar os impactos da Revolução Tecnológica e como eles tem moldado um novo ramo do Direito Penal, no que toca à repressão dos delitos informáticos, com uma análise história do recente avanço legislativo brasileiro sobre o tema. A escolha do objeto de estudo se justifica em razão de sua relevância jurídica e prática, especialmente em uma sociedade cada vez mais hiperconectada e, por sua vez, vulnerável. Por meio da pesquisa bibliográfica e da utilização do método hermenêutico, demonstrou-se que a problemática aventada ainda é insuficiente para lidar com os novos desafios da contemporaneidade.

Palavras-chave: Delitos informáticos; *Internet*; Revolução Tecnológica; Estado de Direito, Direito Penal.

THE TECHNOLOGICAL REVOLUTION AND DIGITAL CRIMES: AN ANALYSIS OF BRAZILIAN LEGISLATIVE (IN) SUFFICIENCY

Abstract: The objective is to investigate the impacts of the Technological Revolution and how they have shaped a new branch of Criminal Law, with regard to the repression of digital crimes, with a historical analysis of the recent Brazilian legislative advance on the subject. The choice of the object of study is justified due to its legal and practical relevance, especially in an increasingly hyperconnected and, in turn, vulnerable society. Through bibliographical research and the use of the hermeneutic method, it was demonstrated that the raised issue is still insufficient to deal with the new challenges of contemporaneity.

Keywords: Digital crimes; *Internet*; Technological Revolution; Rule of Law, Criminal Law.

[1] Mestranda no Programa de Pós Graduação *Stricto Sensu* em Proteção aos Direitos Fundamentais da Universidade de Itaúna. Pós-Graduada em Direito Material e Processual do Trabalho pela Faculdade Pitágoras, Unidade Divinópolis. Bacharel em Direito pela Faculdade Pitágoras, Unidade Divinópolis. Advogada. Professora do Curso de Direito da Faculdade UNA, Unidades Bom Despacho e Divinópolis. E-mail: camilax.adv@gmail.com

[2] Mestrando em Proteção dos Direitos Fundamentais pela Universidade de Itaúna. Graduado pela FADOM-Faculdade de Direito do Oeste de Minas (2002), especialista em Direito Empresarial pela UNIPAC-Universidade Presidente Antônio Carlos (2007), advogado, professor do Centro Universitário UNA de Bom Despacho/MG. E-mail: ricardolopesadv@gmail.com

[3] Mestranda no Programa de Pós Graduação *Stricto Sensu* em Proteção aos Direitos Fundamentais da Universidade de Itaúna. Pós graduada em Direito Processual pela Fundação Educacional de Oliveira - FEOL. Pós graduanda em Direito Penal pela Damásio S/A. Bacharel em Direito pelo Centro Universitário de Lavras. Advogada. Professora do Curso de Direito da Fundação Educacional de Oliveira - FEOL. E-mail: advocaciapadua@gmail.com. Pesquisadora em Direito e Tecnologia.

1. Introdução

Nas últimas décadas, os índices de criminalidade se elevaram exponencialmente, a sociedade de forma geral tem sua liberdade cada vez mais arriscada com o aumento das condutas delituosas, e, por esses e outros motivos, a confiança nas instituições responsáveis por fazer manter a paz social tem tido um déficit considerável.

A *Internet* criou um eirado paralelo para a forma como as comunicações, troca de informações e bens são desenvolvidos. Embora a dimensão digital agregue as experiências do ser humano em superfícies diferentes, ela exacerba o risco de novas ameaças delituosas. Da mesma forma como os mercados, o consumo e as relações interpessoais evoluem dentro de campos digitais e virtuais, o mesmo pode acontecer com o crime.

A tecnologia tem mudado aceleradamente a forma como as pessoas se interagem com o mundo a sua volta. No intuito de atender as várias demandas consumeristas, por exemplo, as empresas e o mercado de forma geral, tem desenvolvido produtos com interfaces tecnológicas que seriam impensadas há uma década.

No limiar de toda essa evolução tecnológica é crível detectar que, atualmente, o Código Penal deve lidar com conjunturas criminosas que vão além do plano físico e tradicional. Hoje, o agente criminoso não precisa ir até a rua para cometer ações delituosas, estas podem ser realizadas no conforto de sua casa.

Como incidem em crimes considerados silenciosos, por não ameaçarem abertamente a vítima, a legislação, para bloqueá-los, tende a ser individualizada, necessitando a adaptação das leis para acoimar e majorar a segurança da população.

Neste mesmo contexto, por se tratar de novos tipos penais, o Direito tem como tarefa identificar essas novas circunstâncias que atacam os princípios da liberdade, segurança, privacidade e a cidadania dos indivíduos. Ademais, pode-se ponderar como entrave a velocidade dos adiantamentos tecnológicos a contraponto da criação de legislações, por isso, escolheu-se como problemática: como o Direito Penal brasileiro tem evoluído para tipificar condutas violadoras de direitos que ocorrem em ambiente virtual?

A partir desta pergunta, o presente artigo busca investigar os impactos que estas novas esferas tecnológicas tem trazido para o Direito Penal, debruçando sobre a

evolução história da legislação penal brasileira e o avanço dos chamados crimes virtuais.

O estudo se justifica em razão de sua relevância jurídica e prática, especialmente em uma sociedade cada vez mais hiperconectada e, por sua vez, vulnerável. A acessibilidade e eficácia da Internet e das tecnologias da informação, também promovem o desenvolvimento de cibercrimes e comportamentos delituosos, demandando repressão estatal.

O método utilizado é o hermenêutico, buscando-se compreender, por meio de ponderações crítico-científicas, acerca das nuances que interseccionam o avanço tecnológico e a aplicação eficaz das normas penais, além do seu (tardio) surgimento.

Por meio da pesquisa bibliográfica, análises temáticas, teóricas, interpretativas e comparativas foi possível demonstrar criticamente que tais proposições evidenciam uma necessidade de reflexão árdua sobre o tema.

2. Impactos da Revolução Tecnológica no Direito Penal vigente

A história em sua perspectiva mundial, revela que não é possível desvincular o instrumento do artifício, nem a técnica da tecnologia e que ambas sempre foram e são empregadas como meios de domínio social.

Este processo onde a tecnologia mecaniza as coisas e o ser humano, tem gerado situações adversas, que podem ser ao mesmo tempo otimistas ou pessimistas, ou até mesmo apocalípticas e integradas como prefere Umberto Eco (2015).

Para se entender o contexto em que este processo se desenvolveu é de suma importância trazer à tona as nuances relacionadas a globalização. Esta, deve ser entendida em dois fenômenos distintos. A um, globalização significa que muitos aspectos da atividade política, econômica e social estão adquirindo perspectivas globais. A dois, caracteriza um novo contexto de intensificação dos níveis de interação entre Estados e sociedades. A novidade reside no alcance das relações sociais, expandido em virtude da tecnologia da informação, intensificando ainda mais estas interconexões (HELD, 1995).

Sob esta égide Zigmunt Bauman (2001) têm uma visão mais sombria sobre a globalização, entendendo que esta nada mais é que uma forma de se polarizar e anular as pessoas, uma vez que de um lado têm-se aqueles que estão inseridos nas novas

tecnologias e de outro, os indivíduos que estão excluídos desta seara por serem incapazes de superar a "velocidade de escape" da órbita do território, acabando por ser nele confinados.

As mutações sociais estão duramente ligadas às transformações tecnológicas da qual a sociedade se calha para seu desenvolvimento. É sabido que hoje existe uma nova realidade, uma nova dimensão: a dimensão cibernética, na qual são inexistentes as barreiras físicas, e que atua em uma velocidade deveras surpreendente. Este contexto, fez com que coisas e pessoas se intermeassem em um grau jamais concebido.

A habilidade ou inabilidade de uma sociedade em dominar a tecnologia ou incorporar-se às suas transformações, fazer uso e decidir seu potencial tecnológico, remodela em ritmo acelerado e traça a história e o destino social das mesmas; remetendo que essas modificações não ocorrem de forma igual e total em todos os lugares (CASTELLS, 199).

O avanço destas tecnologias, em especial as digitais, afetará profundamente todas as estruturas econômicas e sociais. Inteligência artificial, robótica avançada, *data science*, *fintechs* e outras abas desse acontecimento vão deixando o status de utopia para se incorporar discretamente no dia a dia das pessoas.

A partir disto têm-se que o uso desenfreado da *internet* sempre foi algo muito discutido entre a população de forma geral, fazendo com que os crimes cibernéticos apresentassem um maior protagonismo no estudo do Direito Penal

A *Informática* e suas várias conjecturas, trouxeram para a seara penalista novas perspectivas de se pensar o caráter punitivo das normas. Ao definir o fenômeno tecnológico, Marcuse (1993) leciona que a tecnologia serve para instituir formas de controle e de coesão social mais eficientes, porém sutilmente agradáveis ao ser humano. Ressalta ainda, o importante e peculiar aspecto da neutralidade tecnológica, pontuando que a tecnologia não pode ser separada do emprego que dela se faz, ou seja, a máquina é indiferente ao uso político que dela se pretende e se executa, a tecnologia obedece a uma predeterminação humana.

Porém, em que pese a relação predeterminada entre homem e máquina, é de se perceber que os estímulos digitais direcionados aos internautas, em especial aos usuários de redes sociais, são verdadeiros 'gatilhos' que disparam projéteis de endorfinas e irradiam sensações viciantes de empoderamento advindas do ato de

consumir, mesmo sem a mais mínima necessidade da aquisição; provocam prazer decorrente de curtidas em exposições excessivas e fúteis; promovem descargas adrenérgicas na circulação sanguínea carregadas de ideologias maniqueístas impulsionando raiva, preconceito racial, social, sexual, bem como o medo difundido pela desinformação de índole política disparada massivamente por robôs. (PATINO, 2019).

Todos os dias pessoas se conectam à internet para compartilhar, armazenar, analisar e processar um alto volume de dados. Esta prática é chamada de *big data*. Sobre tal fenômeno Hannes Grassegger e Mikael Krogerus lecionam que:

> Qualquer pessoa que não tenha passado os últimos cinco anos vivendo em outro planeta estará familiarizada com o termo big data. Big data significa, em essência, que tudo o que fazemos, tanto online como offline, deixa vestígios digitais. Cada compra que fazemos com nossos cartões, cada busca que digitamos no Google, cada movimento que fazemos quando nosso telefone celular está em nosso bolso, cada like é armazenado. Especialmente cada like. Durante muito tempo, não era inteiramente claro o uso que esses dados poderiam ter — exceto, talvez, que poderíamos encontrar anúncios de remédios para hipertensão logo após termos pesquisado no Google "reduzir a pressão arterial. (Grassegge; Krogerus, 2017).

Toda esta revolução tecnológica acabou por impactar diretamente no Direito penal vigente, uma vez que a criminalidade informática, teve como sua maior bandeira a globalização, que pelos favoráveis atributos do meio, obteve um solo novo e convidativo para a prática de crimes e fraudes.

Para conseguir seus arremates, o Direito prescreve comportamentos, através de conjecturas normativas inseridas em procedimentos jurídicos. A definição usual de direito reza: direito é o conjunto de normas coativas válidas em um Estado (JERING, 2015).

Assim sendo, dependendo da valoração atribuída a determinadas coisas, sua proteção será maior ou menor pelo ordenamento jurídico. Neste aspecto sobressai-se o Direito Penal quando disciplina proteção e recompensa. Para esta seara é ilícito jurídico o fato social que contrariar o ordenamento jurídico, sendo o ilícito penal sua modalidade mais grave, por lesar os bens mais importantes dos membros da sociedade (BITTENCOURT, 2016).

É inegável a relevância que a tecnologia tem na sociedade contemporânea. Não há tampouco como denegar a necessidade de proteção desse instrumento pelo

Direito Penal. Tal necessidade demonstra o que alguns chamam de princípio da fragmentaridade do Direito Penal. Neste contexto, explica Bittencourt:

> Nem todas as lesões que lesionam bens jurídicos são proibidas pelo Direito Penal, como nem todos os bens jurídicos são por ele protegidos. O Direito Penal limita-se a castigar as ações mais graves praticadas contra os bens jurídicos mais importantes, decorrendo daí o seu caráter fragmentário, uma vez que se ocupa somente de uma parte dos bens jurídicos protegidos pela ordem jurídica. Isso, segundo Régis Prado, "é o que se denomina caráter fragmentário do Direito Penal. Faz-se uma tutela seletiva do bem jurídico, limitada àquela tipologia agressiva que se revela dotada de indiscutível relevância quanto à gravidade e intensidade da ofensa. (BITTENCOURT, 2016, p. 55)

O maior desafio da evolução humana é cultural. Pode-se dizer o mesmo do Direito. Como instrumento de regulação de condutas, o Direito deve refletir a realidade da sociedade. Agora, quem adapta os legisladores e os aplicadores da lei à nova realidade social? Adaptar-se a essa nova realidade significa dar continuidade à vocação histórica do Direito, que sempre seguiu as transformações ocorridas na estrutura da sociedade (PINHEIRO, 2013).

Para se chegar a um exercício de poder coercitivo que impõe privação de direitos, por exemplo, o Direito Penal não deve ser vulgarizado, o mesmo só deve ser passível de extensão quando houver situações que assim exijam, como o que ocorre com a evolução dos crimes virtuais, acentuados pela chamada terceira revolução industrial.

3. Legislação brasileira *versus* Cibercrimes- Considerações iniciais e evolução histórica

A Revolução Digital, fruto da terceira revolução industrial em meados de 1969, transformou as relações sociais a tal ponto que não é mais possível enxergar um mundo desligado da informática e da virtualidade.

Tendo como pano de fundo a hiperconexão entre os seres humanos, em um planeta com aproximadamente 7,7 bilhões de habitantes, cerca de 4,1 bilhões são usuários da *internet*[4], necessário introduzir aos ordenamentos jurídicos conceitos de

[4] Dados de 2018, segundo o site https://www.internetworldstats.com/stats.htm. Acesso em 15 set 2021.

Direito Constitucional Informático, Direito Penal Informático, Cibercriminologia, entre outros, pois o Direito (até então) tradicional não dá conta das novas questões que se apresentam.

A Kroll, empresa sediada em Nova Iorque, atua na prevenção e gerenciamento de riscos, segurança de dados, segurança cibernética de empresas e periodicamente emite relatórios globais sobre fraudes e riscos. Segundo a pesquisa, no Brasil, em 2019, 55% dos entrevistados afirmam que suas empresas sofreram pelo menos um caso de vazamento de informações (16% acima da média global),[5] o que favorece a prática de diversos delitos informáticos.

SILVA SANCHEZ (2001, p. 32) explica que o Direito Penal é requisitado para as situações inéditas, que, por serem tão novas e muitas vezes indefinidas, exigem uma resposta do Poder Público com a criação de leis que possuem técnicas demasiadamente abertas (as chamadas leis penais em branco), além de, principalmente, a criação de normas de perigo, concreto e abstrato.

Dessa forma, tem-se uma expansão necessária do Direito Penal, o que não deve ser confundido com um expansionismo desenfreado e inconsequente. Esse campo do Direito, como qualquer outro, precisa acompanhar as evoluções sociais. No entanto, não deve deixar de ser a *ultima ratio* para se tornar um instrumento primário de educação e controle social.

Conforme ponderam Eugenio Raúl Zaffaroni e José H. Pierangeli (2002, p.100), o Direito Penal provê à segurança jurídica: a coerção penal. Todo ramo do direito provê a segurança jurídica. No entanto, só o Direito Penal a realiza com coercitividade penal, que se difere de outras sanções jurídicas. Sendo assim, somente são submetidas à pena algumas condutas antijurídicas previamente tipificadas, cujo processo seletivo está em permanente revisão.

Feitas essas considerações iniciais, é necessário salientar que a compreensão dos riscos advindos da sociedade da informação ainda não são perfeitamente conhecidos- se é que um dia serão.

No que toca ao ‘’ local’’, os delitos informáticos podem ser cometidos em áreas ‘’ escuras’’ da *internet*, em que, para se ter acesso, são necessários alguns instrumentos

[5] https://www.kroll.com/pt-br/publicacoes/global-fraud-risk-report-2019. Acesso em 18 set 2021

diferenciados (*softwares)*, o que dificulta a investigação e a repressão por parte da polícia.

A *deep web*, também chamada de *hidden web*, é uma parcela não indexada da rede, não havendo a possibilidade de se obter resultados em mecanismos de busca, em razão da existência de barreiras de acesso, como por exemplo, a necessidade de pagamento. O acesso só pode ser realizado por ferramentas específicas, como navegadores e dispositivos, muitas vezes com a exigência de autorização através de *login* e senha.

Já as *darknets*, são um segmento especializado da *deep web*, onde é possível realizar a troca de conteúdo criptografado de qualquer tipo, de forma totalmente anônima, se traduzindo em um ambiente propício à prática de delitos.

> O maior estímulo aos crimes virtuais é dado pela crença de que o meio digital é um ambiente marginal, um submundo em que a ilegalidade impera. Essa postura existe porque a sociedade não sente que o meio é suficientemente vigiado e que seus crimes são adequadamente punidos. O conjunto norma sanção é tão necessário no mundo digital quanto no real. Se houver essa falta de crédito na capacidade punitiva da sociedade digital, os crimes aumentarão e os negócios virtuais serão desestimulados (PINHEIRO, 2012, p. 165).

Diante da possibilidade de cometimento dos delitos virtuais em zonas cinzentas e quase sempre não alcançadas pelo aparato estatal repressivo, o desafio no combate se faz maior ainda. Passa-se então à análise histórico- gradativa da legislação brasileira e seus avanços (tardios?) na tipificação de condutas cibernéticas violadoras de direitos humanos.

O Direito Penal Informático, o qual, por ser uma aresta do Direito Penal, obviamente é do ramo do Direito Público, teve o seu ‘’ início’’ no ordenamento brasileiro, pode-se dizer, com a promulgação da Lei nº 9.459/1997, que tipificou o delito de preconceito, com uma forma qualificada no parágrafo 2º, prevendo um aumento da pena se a conduta for praticada *por intermédio dos meios de comunicação social ou publicação de qualquer natureza* (BRASIL, 1997).

De maneira acertada, o legislador buscou enquadrar e trazer um agravamento na repressão dos atos cometidos no ambiente digital (local do crime), até pelo alcance inimaginável e imediato que possuem.

Três anos depois, com a promulgação da Lei nº 9.983/2000, pela primeira vez foi concebida a tipificação de crimes de informações, incluindo o artigo 313- A e 313- B

no Código Penal Brasileiro, prevendo como ilegais as condutas de funcionários que inserem, facilitam a inserção de dados falsos ou modificam dados verdadeiros nos sistemas informatizados da Administração Pública, com o fim de obter vantagem ilícita para si ou para outrem (BRASIL, 2000).

No entanto, o avanço legislativo se deu doze anos após, com o advento da Lei nº 12.735/2012, que trouxe determinações aos órgãos de polícia no sentido de se estruturar e se aparelhar no combate à cibercriminalidade. Outro ponto relevante da lei foi de possibilitar ao magistrado, após ouvido o Ministério Público, a determinação da cessação das transmissões eletrônicas, mesmo antes do inquérito policial (BRASIL, 2012). Para Patrícia Peck Pinheiro,

> O maior problema jurídico dos crimes virtuais é a raridade de denúncias e, pior, o despreparo da polícia investigativa e de perícia para apurá-las. Embora já seja possível fazer boletins de ocorrência pela Internet, são poucas as equipes e profissionais preparados para a investigação de um crime virtual (PINHEIRO, 2013, p. 165).

Já a Lei nº 12.737/2012, se adiantou um pouco mais e inaugurou expressamente a matéria penal informática, adicionando ao Código Penal o artigo 154- A, que tornou crime a invasão de dispositivo informático alheio, mediante a violação indevida de mecanismo de segurança, com o objetivo de obter, alterar ou destruir dados para alguma vantagem ilícita. Também se torna crime a conduta de produzir, oferecer, vender ou difundir dispositivo ou programa de computador que possibilita a invasão de dispositivo informático alheio (BRASIL, 2012).

O artigo 266 do Código Penal também foi alterado- ampliado, considerando, a partir de 2012, como criminosa a conduta do agente que interrompe ou perturba serviço informático, o que antes não estava expressamente previsto em qualquer dispositivo. Outra modificação no *códex*, pela referida lei, se deu no artigo 298 do Código Penal, que trata da falsificação de documento particular, ampliando o espectro e considerando também a falsificação de cartão de crédito ou débito (BRASIL, 2012).

A Lei nº 12.965 de abril de 2014, conhecida como ‘’ Marco Civil da Internet’’, ou ‘’ Constituição da Internet’’, apesar de não ter trazido nenhuma tipificação de crime, é considerada um marco histórico brasileiro, no que tange ao estabelecimento de princípios, garantias, direitos e deveres para o uso da *internet* no país (BRASIL, 2014).

Em 24 de setembro de 2020, houve a promulgação da Lei nº 13.718/18, que inseriu o artigo 218- C no Código Penal, tipificando como crime a divulgação de cena

de estupro de vulnerável, de cena de sexo ou de pornografia, sem o consentimento da vítima, em qualquer meio ou sistema informático (BRASIL, 2018).

Em seguida, adentrou ao ordenamento brasileiro a Lei nº 13.772/2018, criminalizando o registro não autorizado da intimidade sexual no artigo 216-B do Código Penal, além de alterar a Lei nº 11.340/06 (Lei Maria da Penha), enquadrando a conduta como sendo violência doméstica e familiar, passível de sanção pela referida legislação (BRASIL, 2018).

A Lei Geral de Proteção de Dados foi promulgada no ano de 2018, sob o número 13.709, inspirada no modelo europeu, trazendo disposições acerca do tratamento dos dados pessoais, de forma que se garanta o direito à privacidade, à liberdade e a autodeterminação do indivíduo (BRASIL, 2018). No entanto, não inseriu no ordenamento nenhuma conduta a ser tida como criminosa.

Em dezembro de 2019, entra em vigência a Lei nº 13.968, inserindo no Código Penal o parágrafo 4º, precisamente no artigo 122, permitindo o aumento de pena para aqueles que induzem, instigam ou auxiliam no suicídio ou automutilação de outrem por meio de computadores, redes sociais ou transmitida em tempo real (BRASIL, 2019).

No ano seguinte, em fevereiro, é editado o Decreto nº 10.222 que aprovou a Estratégia Nacional de Segurança Cibernética, com o objetivo de fortalecer as ações de governança cibernética, elevando o nível de proteção da sociedade (BRASIL, 2020).

No presente ano, 2021, foi promulgada a Lei nº 14.132, resultado do Projeto de Lei nº 1.369/2019, que criminalizou a conduta de perseguição reiterada, inclusive pela *internet* (cyber*stalking)*, prevendo pena de seis meses a dois anos, além de multa, prevista no artigo 147-A do Código Penal Brasileiro (BRASIL, 2021).

A evolução legislativa exposta não esgota as espécies de delitos informáticos. Isso porque, no que toca à classificação, existem os delitos digitais próprios (ou puros), que são aqueles voltados ao atingimento dos sistemas e/ou dados e os delitos digitais impróprios (impuros), que são aqueles cuja relação com a tecnologia é que esta é o meio empregado para o seu cometimento, como explica Vicente Greco Filho:

> Focalizando-se a Internet, há dois pontos de vista a considerar: crimes ou ações que merecem incriminação praticados por meio da internet e crimes ou ações que merecem incriminação praticados contra a Internet, enquanto bem jurídico autônomo. Quanto ao primeiro, cabe observar que os tipos penais, no que concerne à sua estrutura, podem ser crimes de resultado de conduta livre, crimes de resultado de conduta vinculada, crimes de mera conduta ou formais

> (sem querer discutir se existe distinção entre estes) e crimes de conduta com fim específico, sem prejuízo da inclusão eventual de elementos normativos. Nos crimes de resultado de conduta livre, à lei importa apenas o evento modificador da natureza, com, por exemplo, o homicídio. O crime, no caso, é provocador o resultado morte, qualquer que tenha sido o meio ou a ação que o causou. (GRECO FILHO, 2000, p. 95).

Sendo assim, é possível que se tenha delitos digitais impróprios nos mais diversos diplomas legais brasileiros, como no Código Penal, no Código de Defesa do Consumidor, no Estatuto da Criança e do adolescente e nas leis especiais. Uma ameaça de morte, por exemplo, pode ser proferida através de uma rede de relacionamentos *online*. Ou seja, se o meio utilizado for o informático, aquela conduta delituosa será um ciberdelito impróprio.

Um crime que tem sido costumeiramente praticado, sobretudo durante a pandemia pelo vírus Covid-19 em que as pessoas passaram a trabalhar mais pela *internet*, é chamado de *phishing*, que ocorre quando informações confidenciais de pessoas ou empresas são "pescadas" por algum meio digital contendo um link malicioso (MULLER, 2012).

Assim, o agente envia *e-mails* fraudulentos – passando-se por instituições financeiras, por órgãos públicos, ou por serviços de crédito - para uma enorme quantidade de pessoas, tudo com o fim de obter suas informações pessoais, tais como número do cartão de crédito e senha (GOMES e SILVA, 2014). Apesar de não ser um crime virtual próprio, se enquadra no artigo 158 do Título II (Dos Crimes Contra o Patrimônio) do Código Penal, qual seja, o delito de extorsão.

É possível observar que o Direito voltado às questões tecnológicas é recente, fruto das necessidades de uma sociedade informatizada e interconectada, que diante dos novos desafios e problemas que se apresentam, precisa de respostas, sobretudo a partir do momento em que o cometimento de delitos se tornou extremamente fácil, aparentemente protegido pelo anonimato das redes. Spencer Toth Sydow (2021, p. 59) afirma que, seja de modo escondido, criptografado ou virtualmente '' às claras'', o delito informático ocorre em toda a virtualidade constantemente e deve ser compreendido como um todo para evitar resultados danosos.

Fato é que não há mais que se falar em procedimentos tradicionais, como por exemplo, aquele previsto no artigo 6º do Código Penal. Quando a autoridade policial tomava conhecimento da prática de uma infração penal, deveria, primeiramente, se

dirigir ao local, providenciando o isolamento até que os peritos chegassem. Em seguida, apreender objetos que tiveram relação com o fato e por fim, proceder ao reconhecimento de pessoas e coisas e a acareações. Como isso se aplicaria no meio digital?

A virtualidade propõe novas estratégias de enfrentamento aos crimes e às contravenções penais, de modo que o legislador precisa atuar seriamente na tipificação das condutas que violam, principalmente, os direitos fundamentais relativos à privacidade, liberdade, igualdade e dignidade da pessoa, colocados em risco pelas novas tecnologias, como bem afirmam Elias J. Neto e José Luis Bolzan de Morais, já em uma interpelação internacionalista da questão:

> As clássicas abordagens dos Direitos Humanos (por todos, veja-se Luigi Ferrajoli (2007)), embora reconheçam que sua violação por atores privados, entendem que os Estados – com a sua constituição política – são capazes de conter as tendências totalizantes de todos os demais sistemas sociais. Contudo, os Direitos Humanos violados com uso das TICs não podem ser adequadamente protegidos pelo Direito centrado no Estado Nacional (NETO e MORAIS, 2018).

A partir da virtualização de tudo (e de todos), as fronteiras geográficas comumente conhecidas não subsistem mais na Era da Informação, principalmente em relação ao cometimento de crimes virtuais. O conceito tradicional de territorialidade é colocado em xeque. Qualquer sujeito brasileiro, tecnologicamente medíocre, pode instantaneamente cometer um grave delito no interior da Austrália, sem sair de sua residência no Brasil. A *internet* possibilita isso e escancara a limitação do modelo estatal atual, pois os mecanismos de controle jurídico existentes restam desafiados em razão de sua ineficiência. Qual seria, então, a posição mais acertada do Direito?

> São necessárias propostas teóricas que reconheçam o poder normativo dos códigos de computadores gestados dentro do segredo da iniciativa privada. Essas teorias devem ser capazes de propor soluções para garantir que aquele primeiro vácuo (relativo à ausência de poder legitimado democraticamente no meio virtual) seja preenchido por normas constitucionais, protetoras dos Direitos Humanos (NETO e MORAIS, 2018).

Para Carlo Bordoni (2017, p. 30), esse período, o *interregnum* não se apresenta, como resultado, como um tempo de espera, de ausência de capacidade de agir, mas como uma tumultuada alternativa à ordem constituída, em cuja ausência de regras provoca insuficiências, tragédias e desordens, porque contra os mais fracos e os

desamparados se abate aquele poder incontrolado que a política (o *Kathékon)* tinha a responsabilidade de frear. E talvez, pelo entendimento de S. Rodotá, a partir do advento da *Internet,* deve-se cogitar um constitucionalismo global, com normas supra estatais, em um Direito expansivo em linha horizontal.

> Todo esto, claro está, debe ser considerado en la perspectiva de la desestructuración/reconstrucción entre esfera pública y privada. Y tal vez reflexionando sobre Internet puedan delinearse las vías de un posible constitucionalismo global, no entregado a una «vertical domestication», con normas supraestatales incorporadas a los derechos estatales, sino uma construcción del derecho por expansión, horizontal, un conjunto de órdenes jurídicas correlativas, no punto de llegada, sino estructuradas para aguantar los retos de un tiempo tan mudable, una especie de constitución infinita (RODOTÁ, 2012, p. 379).

De qualquer modo, pensar a cibercriminalidade atualmente, é cogitar a criação de um diploma legislativo próprio, que trate dos delitos informáticos e traga outras espécies de sanções, a fim de se regular o tema de maneira mais completa. Em suma, aos problemas novos devem ser buscadas respostas novas (RODOTÁ, 2012).

5. Considerações finais

Uma nova sociedade baseada em ideias desenvolvimentistas por meio do uso da tecnologia somada a uma crescente dependência da automatização e o incremento da velocidade dão origem a um novo segmento de risco, novos bens jurídicos, novos valores individuais.

O Direito, enquanto condição de possibilidade de ação entre os indivíduos e também elemento limitador da liberdade, para aqueles que querem dela abusar, se coloca como elemento fundamental para o controle e a proibição de condutas praticadas que violem direitos fundamentais.

A compreensão dessa (nova) realidade requer cautela, principalmente quando o Direito Penal é convocado a trazer respostas diante do crescimento dos crimes praticados na virtualidade.

Os cidadãos- usuários precisam se educar, se informar e compreender que, dentro do segmento social virtual, são eles responsáveis pela maioria de suas condutas na virtualidade. Um clique para uma permissão indevida na rede pode alterar o destino de um indivíduo e seus valores perante a coletividade que o cerca.

A ideia de descentralização do dever de cuidado é necessária. O usuário não deve figurar como um mero espectador das ações cometidas no meio virtual, mas deve assumir suas responsabilidades e consequências por suas ações, de modo que o Estado possa (tentar) dar conta do restante.

6. Referências

BAUMAN, Zygmunt. **Modernidade líquida**. Tradução Plinio Dentzien. Rio de Janeiro: Zahar, 2001. 258 p.

BITTENCOURT, Cézar Roberto. **Tratado de direito penal: parte geral**. São Paulo, Saraiva, 2016, 22ª ed., 35 - 55 p.

BORDONI, Carlo. **Fine del mondo liquido**. Superare la modernità e vivere nell'interregno. Milano: Il Saggiatore. 2017. p. 30

CASTELLS, Manuel. **A sociedade em rede**. São Paulo: Paz e Terra, 1999.

ECO, Umberto. **Apocalípticos e integrados.** 7. ed. Tradução: Geraldo Gerson de Souza. São Paulo: Perspectiva, 2015.

BRASIL, **Lei nº 9.459 de 13 de maio de 1997.** Altera os arts. 1º e 20 da Lei nº 7.716, de 5 de janeiro de 1989, que define os crimes resultantes de preconceito de raça ou de cor, e acrescenta parágrafo ao art. 140 do Decreto-lei nº 2.848, de 7 de dezembro de 1940. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/l9459.htm> Acesso em 19 set 2021

BRASIL, **Lei nº º 9.983, de 14 de julho de 2000.** Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9983.htm> Acesso em 19 set 2021

BRASIL, **Lei nº 12.735, de 30 de novembro de 2012.** Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm> Acesso em 19 set 2021

BRASIL, **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm> Acesso em 19 set 2021

BRASIL, **Lei nº 12.965 de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <

http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso em 19 set 2021

BRASIL, **Lei nº 13.718 de 24 de setembro de 2018**. Altera o Decreto- Lei nº 2.848 de 1940 para tipificar os crimes de importunação sexual, divulgação de cena de estupro e dá outras providências. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13718.htm> Acesso em 19 set 2021

BRASIL, **Lei nº 13.772 de 19 de dezembro de 2018**. Altera o Decreto- Lei nº 2.848 de 1940 e a Lei 11.340 de 07 de agosto de 2006. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13772.htm> Acesso em 19 set 2021

BRASIL, **Lei nº 13.709 de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm> Acesso em 19 set 2021

BRASIL, **Lei nº 13.968 de 26 de dezembro de 2019**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para modificar o crime de incitação ao suicídio e incluir as condutas de induzir ou instigar a automutilação, bem como a de prestar auxílio a quem a pratique. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13968.htm> Acesso em 19 set 2021

BRASIL, **Lei nº 14.132 de 14 de março de 2021.** Acrescenta o art. 147-A ao Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para prever o crime de perseguição; e revoga o art. 65 do Decreto-Lei nº 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais). Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14132.htm> Acesso em 19 set 2021

BRASIL. **Decreto-lei nº 10.222 de 05 de fevereiro de 2020**. Aprova a Estratégia Nacional de Segurança Cibernética. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm> Acesso em 19 set 2021

GOMES, Rebeca B. de O.; SILVA, Marcelo Sarsur L. da. **O enquadramento jurídico penal do *phishing* e suas repercussões no furto informático.** In: LETRAS JURÍDICAS | N.3 | 2/2014

GRASSEGGER, Hannes; KROGERUS, Mikael. **The data that turned the world upside down**. Motherboard, 28 jan. 2017.

GRECO, Vicente Filho. **Algumas observações sobre o direito penal e a internet**. Boletim IBCCRIM, v. 8, p. 3, 2000.

HELD, D. **Democracy and the Global order: From the modern State to Cosmopolitan Governance**. Stanford: Stanford University Press, 1995, 324 p.

JERING, Rudolf Von apud FERRAZ JÚNIOR, Tércio Sampaio. **Introdução ao estudo do direito: técnica, decisão, dominação**. São Paulo, Atlas, 2015, 8ª ed., 71 p.

MARCUSE, Herbert. **El hombre unidimensional. Ensayo sobre la ideología de la sociedad industrial avanzada**. Barcelona: Editorial Planeta-De Agostini, 1993, 20 p.

MULLER, Leonardo. **O que é phishing?** In: TecMundo. Publicado em: 05.07.2012. Disponível em: <https://www.tecmundo.com.br/phishing/205-o-que-e-phishing-.htm>. Acesso em 15 set 2021

NETO, Elias Jacob de Menezes. MORAIS, Jose Luis Bolzan. **A fragilização do Estado-Nação na proteção dos Direitos Humanos violados pelas tecnologias da informação e comunicação**. Rev. direitos fundam. democ., v. 23, n. 3, p. 231-257, set./dez. 2018.

PATINO, Bruno. **La Civilisation du Poisson Rouge**. Petit tratie sur le marché de l'attention. Paris: Grasset. 2019.

PINHEIRO, Patrícia Peck. **Direito Digital.** São Paulo: Saraiva, 2013.

RODOTÀ, Stefano. **El derecho a tener derechos**. Trad. José Manuel Revuelta. Bologna: Editoral Trotta. 2014.

SILVA SANCHEZ, Jesus Maria. **La expansión del derecho penal**. *Aspectos de la política criminal em las sociedades postindustriales.* Madrid: Civitas. 2001, p. 32

SYDOW, Spencer Toth. **Curso de Direito Penal Informático**: Partes Geral e Especial. Salvador: Editora Jvspodium, 2021.

ZAFFARONI, Eugenio Raúl. PIERANGELI, José Henrique. **Manual de Direito Penal brasileiro**. São Paulo: Editora Revista dos Tribunais, 2002.