BRASÍLIA 2023

ISBN 978-85-7267-121-7

CADERNO DE PÓS-GRADUAÇÃO EM DIREITO

CRIMES DIGITAIS

COORDENAÇÃO:

LILIAN ROSE LEMOS ROCHA

ORGANIZAÇÃO:

PEDRO ROCHA AMORIM
NAIARA FERREIRA MARTINS
ANA CAROLINA COELHO SANTOS
ANA CAROLINA RODRIGUES DE SOUZA SILVA
CECÍLIA OLIVEIRA VENDRAMIN NUNES
JOSÉ RAMALHO BRASILEIRO JÚNIOR
RAMON FRANCO ARAÚJO DOS SANTOS

CEUB
EDUCAÇÃO SUPERIOR

Coordenação

Lilian Rose Lemos Rocha

CADERNO DE PÓS-GRADUAÇÃO EM DIREITO

CRIMES DIGITAIS

Organização

Pedro Rocha Amorim
Naiara Ferreira Martins
Ana Carolina Coelho Santos
Ana Carolina Rodrigues de Souza Silva
Cecília Oliveira Vendramin Nunes
José Ramalho Brasileiro Júnior
Ramon Franco Araújo dos Santos

Brasília
2023

CEUB

ICPD Instituto CEUB de Pesquisa e Desenvolvimento

Disponível em:
repositorio.uniceub.br

Dados Internacionais de Catalogação na Publicação (CIP)

Caderno de pós-graduação em direito: crimes digitais. / coordenador, Lilian Rose Lemos Rocha – Brasília: CEUB: ICPD, 2023.

77 p.

ISBN 978-85-7267-121-7

1. Direito digital. I. Centro Universitário de Brasília. II. Título.

CDU 34:004.541

Ficha catalográfica elaborada pela Biblioteca Reitor João Herculino

Centro Universitário de Brasília – CEUB
SEPN 707/709 Campus do CEUB
Tel. (61) 3966-1335 / 3966-1336

PREFÁCIO

Pioneirismo sempre foi uma característica do UniCEUB; outra característica é a evolução permanente. A Instituição sempre acompanhou a evolução tecnológica e pedagógica do ensino. Isso se coaduna com a filosofia institucional que é a de preparar o homem integral por meio da busca do conhecimento e da verdade, assegurando-lhe a compreensão adequada de si mesmo e de sua responsabilidade social e profissional. Destarte, a missão institucional é a de gerar, sistematizar e disseminar o conhecimento visando à formação de cidadãos reflexivos e empreendedores, comprometidos com o desenvolvimento socioeconômico sustentável.

E não poderia ser diferente. Com a expansão do conteúdo acadêmico que se transpassa do físico para o virtual, do local para o universal, do restrito para o difundido, isso porque o papel não é mais apenas uma substância constituída por elementos fibrosos de origem vegetal, os quais formam uma pasta que se faz secar sob a forma de folhas delgadas donde se cria, modifica, transforma letras em palavras; palavras em textos; textos em conhecimento, não! O papel se virtualiza, se desenvolve, agora, no infinito, rebuscado de informações. Assim, o UniCEUB acompanha essa evolução. É dessa forma que se desafia o leitor a compreender a atualidade, com a fonte que ora se entrega à leitura virtual, chamada de *ebook*.

Isso é resultado do esforço permanente, da incorporação da ciência desenvolvida no ambiente acadêmico, cujo resultado desperta emoção, um sentimento de beleza de que o conteúdo científico representa o diferencial profissional.

Portanto, convido-os a leitura desta obra, que reúne uma sucessão de artigos que são apresentados com grande presteza e maestria; com conteúdo forte e impactante; com sentimento e método, frutos da excelência acadêmica.

João Herculino de Souza Lopes Filho
Diretor ICPD/UniCEUB

APRESENTAÇÃO

Os trabalhos científicos ora apresentados são fruto da disciplina “Crimes Digitais”, ministrada no quarto bimestre de 2022 pelo Professor Pedro Rocha Amorim.

No período letivo foram, para além da teoria jurídica dos crimes digitais e de seus aspectos relacionados à prática jurisprudencial, analisadas situações complexas sob o prisma constitucional, penal e processual penal.

Foram selecionados quatro trabalhos correlatos a temas estudados durante o bimestre, de autoria das discentes Caroline Rabelo Corrêa, Deivinson Alves Lopes, Gabriela Freire Martins e Rafael Vieira Lopes.

Professor Me. Pedro Rocha Amorim

SUMÁRIO

CRIPTOMOEDAS E CRIME DIGITAL: ANÁLISE PROPEDÊUTICA DA NECESSIDADE REGULATÓRIA FRENTE À POLÍTICA ANTI-LAVAGEM DE DINHEIRO

Caroline Rabelo Corrêa [1]

RESUMO

Nos últimos anos, as criptomoedas se tornaram pautas de debate social quanto à sua origem, suas singularidades quando comparadas com as moedas tradicionais e os motivos pelos quais se tornaram tão atrativas aos investidores em relação a estas. Não obstante se reconheça a importância que os criptoativos alcançaram, bem como seus inegáveis benefícios ao comércio e às negociações interpessoais e intercontinentais, eles têm sido igualmente utilizados para a prática de atividades criminosas, tais como o financiamento do terrorismo e a lavagem de capitais. A recorrência desta última hipótese acende uma chama de alerta nas autoridades nacionais e internacionais que, ante a falta de previsão legislativa que regule suficientemente o tema, veem-se compelidas a pensar em soluções jurídicas e mercadológicas que sejam capazes de mitigar o uso das criptomoedas para essa finalidade. Portanto, o objetivo deste trabalho, realizado sob pesquisa exploratória e bibliográfica, é promover uma breve reflexão quanto à origem dos criptoativos, as suas características principais e de que formas elas podem contribuir para a prática criminosa na web. As hipóteses de regulação concernentes às criptomoedas serão levantadas, de forma a demonstrar o respaldo que pode ser utilizado no enfrentamento à lavagem de dinheiro com criptomoedas no Brasil. Algumas abordagens doutrinárias serão igualmente analisadas, com o intuito de reconhecer a crescente utilização de criptomoedas na lavagem de capitais e que, como tal, demanda um debate frequente da sociedade sobre as formas adequadas para combater esse fenômeno sem, contudo, frustrar os bons atributos que legitimamente tornaram as criptomoedas uma ferramenta em ascensão. A pesquisa foi realizada através do método qualitativo e os resultados foram obtidos pelo método dedutivo.

Palavras-chave: Criptomoedas. Lavagem de capitais. Regulação.

[1] Aluna do curso de pós-graduação *lato sensu* do Centro Universitário de Brasília – CEUB/ICPD. Advogada. Bancária. E-mail: caroline.rabelo@sempreceub.com.

ABSTRACT

In the past few years, cryptocurrencies have become the subject of social debate regarding their origin, their singularities when compared to traditional currencies and the reasons why they have become so attractive to investors in relation to them. Despite recognizing the importance that crypto-assets have achieved, as well as their indeniable benefits to trade and interpersonal and intercontinental negotiations, they have also been used for the practice of criminal activities, such as the financing of terrorism and money laundering. The recurrence of this last hypothesis lights a warning flame in national and international authorities who, given the lack of legislative provision that sufficiently regulates the subject, are compelled to think of legal and economic solutions that are capable of mitigating the use of cryptocurrencies to that purpose. Therefore, the objective of this work, carried out under exploratory and bibliographical research, is to promote a brief reflection on the origin of crypto assets, their main characteristics and in what ways they can contribute to criminal practice on the web. The hypotheses of regulation concerning cryptocurrencies will be raised, in order to demonstrate the support that can be used in the fight against money laundering with cryptocurrencies in Brazil. Some doctrinal approaches will also be analysed, with the aim of recognizing the growing use of cryptocurrencies in money laundering and that, as such, demands a frequent debate in society about the appropriate ways to combat this phenomenon without, however, frustrating the good attributes that legitimately made cryptocurrencies a rising tool. The research was carried out through the qualitative method and the results were obtained by the deductive method.

Keywords: Cryptocurrencies. Money laundering. Regulation.

1 INTRODUÇÃO

A globalização, em que pese ser uma nomenclatura um tanto recente, é um fenômeno cuja origem remonta às Grandes Navegações, a partir do século XV. Desde então, a exploração territorial e a expansão comercial promovida entre países auxiliaram na formação de uma realidade marcada pela crescente (e, talvez, inevitável) eliminação de barreiras físicas entre pessoas, culturas e continentes[2].

A relativização dos obstáculos geográficos e sociais também se revelou com a realização de transações financeiras em meio virtual, possibilidade que representou uma tecnologia disruptiva por si só. Afinal, elas viabilizam o desenvolvimento da economia e do comércio além-fronteiras em termos mais simples, mais rápidos e, em tese, mais seguros, além de corresponderem às transações físicas em todas as suas

[2] GONÇALVES, João; LOPES, Karina. O que é globalização. **Politize**, 2017. Disponível em: <https://www.politize.com.br/globalizacao-o-que-e/>. Acesso em 12 de nov. 2022.

qualidades e características – não há qualquer diferença entre negociar em dólares em uma corretora *online* ou em uma corretora física, por exemplo.

O que não se imaginava após esse marco econômico era o surgimento de um recurso digital que, na prática, funcionaria como uma moeda, apesar de não se submeter às qualidades e às limitações tradicionalmente atribuídas a uma. Os criptoativos, cujas características serão abordadas no capítulo subsequente, surgiram em 2008 e se tornaram populares com a difusão do primeiro que se têm ciência: o Bitcoin. Outras criptomoedas foram criadas naturalmente com o passar dos anos, mas atualmente o Bitcoin desponta como o mais valorizado dentre elas: uma unidade sua corresponde, hoje, por exemplo, a R$ 88.968,15[3].

A ausência de uma entidade centralizadora/controladora, o aparente anonimato, a segurança e as facilidades na sua comercialização, quando comparadas às moedas tradicionais, tornam as criptomoedas um atrativo para investidores em nível mundial. No entanto, da mesma forma que as suas particularidades os revelem interessantes para esses usuários, essas mesmas qualidades também atraem pessoas mal-intencionadas, que abusam dos facilitadores inerentes às criptomoedas para práticas criminosas, tais como o financiamento de terrorismo e a lavagem de dinheiro.

Como deve, então, o Direito regular o uso das criptomoedas, a fim de prevenir e reprimir a sua utilização criminosa, sem esvaziar as qualidades que fizeram dos criptoativos se desenvolverem de forma positiva para a economia internacional? A exigência legal de identificação dos usuários que realizem transações com criptomoedas se justificaria, ainda que prejudicasse o interesse de potenciais investidores? A definição da natureza jurídica dessas criptomoedas é necessária para fins de abrangência pela disciplina jurídica anti-lavagem de capitais, ou como condição de sua eficiência normativa?

Considerando esses questionamentos iniciais, os criptoativos, como fenômeno socioeconômico a ser adequadamente tratado pelo Direito nas redes, consagrar-se-á como a questão central do presente trabalho. Seu objetivo não será de

[3] Cotação realizada no dia 30 de nov. 2022, às 11h33. BITCOIN. **Google**, 2022. Disponível em: <https://www.google.com/search?q=valor+bitcoin&oq=valor+bitcoin&aqs=chrome..69i57j69i59j0i3j0i512l7.1829j1j7&sourceid=chrome&ie=UTF-8>. Acesso em 30 de nov. 2022.

responder definitivamente a essas perguntas, o que por óbvio demandaria um estudo mais amplo e aprofundado. O que se pretende, por ora, é promover uma breve análise sobre o atual cenário de popularização das criptomoedas, o seu uso para a prática de lavagem de capitais, e em que medida o Direito será(ia) capaz, mediante a regulação dos criptoativos, de alcançar esse resultado ou de, ao menos, promover uma investigação eficaz sobre essa prática.

2 O QUE SÃO AS CRIPTOMOEDAS

Não é possível começar a discorrer sobre criptomoedas sem abordar o contexto histórico daquela que se tornou a mais conhecida mundialmente: o Bitcoin. As grandes revoluções ocorrem em momentos de rupturas significativas no *status quo* social, e com o Bitcoin, não poderia ser diferente.

O referido criptoativo surgiu em um momento em que o mundo adentrava em uma das piores crises socioeconômicas desde a Grande Depressão: a Crise de 2008. Até hoje, ninguém sabe de fato a autoria desta criptomoeda, ou até mesmo se foi elaborada por mais de uma pessoa. Fato é que, em 2008, seu criador (ou criadores), alcunhado de Satoshi Nakamoto, compartilhou o *white paper*[4] sobre o Bitcoin em um fórum aberto na *internet*. O lançamento do seu código aberto deu-se um ano depois, em 2009.

A partir da tecnologia *peer-to-peer* (ponto a ponto, em tradução livre), o *Bitcoin* foi criado com a proposta de facilitar transações financeiras entre duas pessoas ao eliminar um terceiro fator comum nas transações monetárias até então: um ente centralizador. Além disso, a criptomoeda é reconhecida por manter anonimato de sua operação – os usuários sabem que uma transação foi realizada e o seu valor, mas as pessoas envolvidas no *peer-to-peer* permanecem sem identificação.

Mais do que a criptografia e a anonimização, uma das características do Bitcoin reside na sua finitude. Isto é, ela pode ser criada por computadores através de um processo denominado de "mineração", mas somente até determinada

[4] *White paper* é um documento disponibilizado publicamente para apresentar dados aprofundados sobre um determinado serviço ou problema, bem como suas soluções.

quantidade previamente estabelecida pelos seus idealizadores primários[5]. Desde o seu lançamento, o processo de mineração de novos Bitcoins se torna um processo que exige cada vez mais uma enorme quantidade de energia e de tecnologia sofisticada, de modo que a dificuldade de se gerar novas unidades da criptomoeda tende a valorizar as já existentes.

Outra característica que torna o Bitcoin atrativo em relação às moedas tradicionais é o fato de ser um ativo financeiro descentralizado. Em outras palavras, ausência de controle regulatório por parte de alguma entidade estatal ou pública revela a adesão aos criptoativos como voluntária e afasta a incidência das desvalorizações monetárias em seu valor, conforme ressalta Andrade:

> O monopólio das emissões de notas e moedas tornou os governos capazes de usar a inflação como mecanismo para exercer suas políticas e impor suas agendas, mas também consolidou o controle das instituições sobre as transações financeiras. As moedas digitais representam um mecanismo para a realização de operações financeiras sem a incidência dos mesmos custos da inflação impostos pelo Banco Central, por meio da criptografia do dinheiro[6].

Uma das particularidades do Bitcoin e das demais criptomoedas reside na sua operacionalização, que ocorre em um ambiente de *blockchain*. O sistema *blockchain* funciona como um grande livro-caixa virtual, pois nele são registradas todas as transações realizadas com a criptomoeda, cujo teor (e valor) é publicamente acessível. A auditoria pública dessas transações evita o chamado "gasto duplo", ou seja, afasta a possibilidade de que a mesma moeda seja comercializada duas vezes pelas mesmas partes.

Em que pese o valor das operações com criptomoedas ser de conhecimento público, há um fator que permanece desconhecido nos dados registrados no *blockchain*: a identidade das pontas de negociação – ou seja, quem vendeu e quem adquiriu a moeda. Nos termos da explicação de Ulrich, o anonimato frequentemente

[5] A quantidade de Bitcoins passíveis de mineração é de 21 milhões de unidades. Até hoje, foram minerados 19 milhões unidades da criptomoeda, e estima-se que sua última seja criada em meados de 2140. MARQUES, Gabriel. Ativo ainda mais escasso: 90% de todos os bitcoins já foram minerados. **Exame**, 2022. Disponível em: <https://exame.com/future-of-money/ativo-ainda-mais-escasso-90-de-todos-os-bitcoins-ja-foram-minerados/>. Acesso em 30 de nov. 2022.

[6] ANDRADE, Mariana Dionísio de. Tratamento jurídico das criptomoedas: a dinâmica dos bitcoins e o crime de lavagem de dinheiro. **Revista Brasileira de Políticas Públicas**, Brasília, v. 7, n. 3, p. 43-59, dez. 2017. p. 46.

atribuído a esses criptoativos não atinge a sua integralidade, de forma que o melhor termo a qualificar tal característica é o "pseudoanonimato", uma vez que o *blockchain* compila outras informações capazes de especificar, em certa medida, seus comerciantes:

> Enquanto as chaves públicas de todas as transações – também conhecidas como "endereços Bitcoin" – são registradas no blockchain, tais chaves não são vinculadas à identidade de ninguém. Porém, se a identidade de uma pessoa estivesse associada a uma chave pública, poderíamos vasculhar as transações no blockchain e facilmente ver todas as transações associadas a essa chave. Dessa forma, ainda que Bitcoin seja bastante semelhante ao dinheiro vivo, em que as partes podem transacionar sem revelar suas identidades a um terceiro ou entre si, é também distinto do dinheiro vivo, pois todas as transações de e para um endereço Bitcoin qualquer podem ser rastreadas. Nesse sentido, Bitcoin não garante o anonimato, mas permite o uso de pseudônimo[7].

Considerando as intenções despretensiosas daqueles que realizaram operações com o Bitcoin em seus primórdios, a surpresa pelo estrondoso e crescente sucesso dessa criptomoeda é compreensível. A primeira transação com a criptomoeda ocorreu em maio de 2010, como parte de uma brincadeira. Laszlo Hanyecz propôs, em um fórum na *internet*, a compra de duas pizzas por 10 mil Bitcoins, proposta que foi atendida em 22 de maio de 2010, 4 dias depois da publicação de sua proposta[8].

A título de comparação, na data da proposta de Laszlo, 10 mil Bitcoins valiam cerca de 41 dólares. Hoje, essa mesma quantidade da criptomoeda equivale a 158 milhões de dólares – quase 843 milhões de reais. Não à toa, os entusiastas de criptoativos celebram, em 22 de maio, o Bitcoin Pizza Day, em homenagem às pizzas mais caras da história, considerando o preço pago por elas na época e o seu equivalente atualmente.

Perpassada brevemente a história e as principais características das criptomoedas, surge a dúvida: considerando o termo comumente utilizado para

[7] ULRICH, Fernando. **Bitcoin: a moeda na era digital**. São Paulo: Instituto Ludwig Von Mises Brasil, 2014. Disponível em: <https://produtos.infomoney.com.br/hubfs/ebook-bitcoin.pdf>. Acesso em: 04 mar. 2023. P. 22.

[8] JOSA, Lucas. Bitcoin Pizza Day: a história da refeição mais cara de todos os tempos. Exame, 2021. Disponível em: <https://exame.com/future-of-money/criptoativos/bitcoin-pizza-day-a-historia-da-refeicao-mais-cara-de-todos-os-tempos/>. Acesso em: 21 nov. 2022.

designá-las, elas podem ser consideradas moedas em sentido estrito, para fins legais? Qual seria a sua natureza jurídica, com o intuito de subsidiar a aplicação das leis a elas relacionadas?

As criptomoedas não são regulamentadas no Brasil, apesar da existência projetos de lei em trâmite no Congresso Nacional destinados a esse propósito (conforme será posteriormente abordado, no terceiro capítulo). Com a lacuna legislativa, e dadas as limitações do presente trabalho, que não pretende esgotar o tema, definir adequadamente a natureza jurídica dos criptoativos torna-se uma tarefa complexa.

A primeira tentativa normativa de atribuir alguma classificação às criptomoedas surgiu em 2014, ano em que o Banco Central do Brasil (BACEN) emitiu um comunicado (Comunicado BACEN Nº 25306/2014)[9] diferenciando moedas eletrônicas de moedas virtuais.

As moedas eletrônicas, segundo o BACEN, "são recursos armazenados em dispositivo ou sistema eletrônico que permitem ao usuário final efetuar transação de pagamento denominada em moeda nacional". Por sua vez, as moedas virtuais "possuem forma própria de denominação, ou seja, são denominadas em unidade de conta distinta das moedas emitidas por governos soberanos, e não se caracterizam dispositivo ou sistema eletrônico para armazenamento em reais". Além disso, elas "não são emitidas nem garantidas por uma autoridade monetária" e "não têm garantia de conversão para a moeda oficial, tampouco são garantidos por ativo real de qualquer espécie". Nesse sentido, as criptomoedas são consideradas pelo BACEN como moedas virtuais.

Em 2019, a Receita Federal, por meio da Instrução Normativa n. 1888, de 3 de maio de 2019, disciplinou a obrigatoriedade de prestação de informações relativas às operações realizadas com criptoativos à Secretaria Especial da Receita. Nela, a Receita Federal definiu as criptomoedas da seguinte forma:

> Art. 5º Para fins do disposto nesta Instrução Normativa, considera-se:

[9] BRASIL. **Comunicado BACEN 25.306, de 19 de fevereiro de 2014**. Disponível em: <https://www.legisweb.com.br/legislacao/?id=265825>. Acesso em: 21 nov. 2022.

> I - criptoativo: a representação digital de valor denominada em sua própria unidade de conta, cujo preço pode ser expresso em moeda soberana local ou estrangeira, transacionado eletronicamente com a utilização de criptografia e de tecnologias de registros distribuídos, que pode ser utilizado como forma de investimento, instrumento de transferência de valores ou acesso a serviços, e que não constitui moeda de curso legal[10];

Considerando as características principais das criptomoedas, responsáveis por fazê-las eclodir em relação às moedas tradicionais – tais como o pseudoanonimato e a ausência de controle por uma entidade centralizada –, não é difícil imaginar que essas mesmas características atrairiam investidores interessados em utilizá-las para propósitos ilegítimos, tais como a lavagem de capitais. No capítulo a seguir, realizar-se-á uma breve análise acerca do crime de lavagem de dinheiro no Brasil e a forma pela qual os criptoativos, quando utilizados para esse fim, torna a investigação acerca da materialidade e da autoria desse delito muito mais desafiadora do que o comum.

3 O CRIME DE LAVAGEM DE DINHEIRO NO ORDENAMENTO JURÍDICO BRASILEIRO

A lavagem de capitais como tipificação penal é regulamentada no Brasil pela Lei 9.613/1998. A prática consiste no conjunto de atos e procedimentos para conferir uma aparência de licitude à capitais de procedência ilícita. Por essa razão é que o delito é chamado de "lavagem" de dinheiro: toma-se um capital de origem criminosa (dinheiro "sujo") para, após a lavagem, torná-lo "limpo".

Em termos legais, a lavagem pode abranger a ocultação de quaisquer bens, direitos e valores (art. 1º da Lei 9.613/1998)[11]. Ou seja, apesar de ser popularmente conhecida como lavagem de dinheiro, o delito não se aplica, portanto, exclusiva e necessariamente ao dinheiro como unidade monetária que conhecemos.

[10] BRASIL. Secretaria da Receita Federal do Brasil. **Instrução Normativa RBF nº 1888, de 03 de maio de 2019**. Disponível em: <http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?idAto=100592>. Acesso em 26 de nov. 2022.

[11] BRASIL. **Lei 9.613/1998, de 3 de março de 1998.** Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras - COAF, e dá outras providências. Disponível em: <https://www.planalto.gov.br/ccivil_03/Leis/L9613.htm>. Acesso em 21 de nov. 2022.

Uma das principais características da lavagem de capitais é se tratar de um tipo penal acessório, pois depende da existência de uma infração penal antecedente (crime ou contravenção). Em outras palavras, a lavagem de dinheiro só se configura se a ocultação for realizada sobre bens, valores ou direitos oriundos de uma infração penal anterior.

Outro fator particular à lavagem de capitais é que, considerando sua qualidade de tipo penal acessório, o julgamento da infração penal antecedente é dispensável para que se configure o delito de lavagem. Além disso, basta que as infrações antecedentes sejam consideradas típicas e ilícitas. Ainda que lhes recaia alguma causa excludente de culpabilidade ou de punibilidade, a lavagem de capitais posteriores a elas restará plenamente configurada.

A lavagem de capitais pode ser dividida em três fases: colocação, ocultação e integração. A primeira, como o próprio nome sugere, diz respeito à introdução dos bens, valores ou direitos ilícitos no sistema financeiro. A segunda, por sua vez, refere-se ao conjunto de operações realizadas para movimentar tais capitais nesse sistema. Por fim, na integração, os capitais legítimos oriundos da movimentação daqueles ilegítimos na segunda fase são reintroduzidos em mercado, de forma que são considerados legais. Para configuração do crime, basta que o agente pratique os atos da primeira fase (colocação).

Um dos pilares da regulamentação do delito de lavagem de capitais ao redor do mundo reside na prática do *Know Your Costumer*. Segundo ela, prestadores de serviços em geral devem adotar políticas que assegurem o conhecimento da identidade e da habitualidade das transações de seus clientes, de forma que qualquer ato ou omissão destinados a afastar essa identificação ou os padrões relacionados a esse cliente devem ser devidamente monitoradas, com o intuito de combater não apenas a lavagem de capitais, como também a corrupção e o financiamento de práticas terroristas[12].

A opção do legislador em abranger "bens, direitos e valores" para caracterização do crime de lavagem de capitais permite que as criptomoedas sejam

[12] KWC BRASIL. Know Your Costumer – Conceito. Disponível em: <https://kycbrasil.com/conceito/>. Acesso em 26 de nov. 2022.

consideradas "valores", no Brasil, para fins de cometimento do delito, ainda que não haja convergência na doutrina nacional ou inércia legislativa em determinar sua natureza jurídica, conforme visto no capítulo antecedente.

No entanto, essa realidade não se observa em outros países. Na doutrina alemã, por exemplo, há uma dificuldade em considerar as criptomoedas como ativos abrangidos pela lei germânica de lavagem de capitais. Explica Estellita[13] que se reconhece como valores aptos a serem objeto da prática o dinheiro em espécie, o dinheiro escritural e o dinheiro eletrônico. O primeiro se trata de meio legítimo de pagamento e possui existência corpórea. O segundo, apesar de não possuir não materializado em espécie, reveste-se de uma pretensão de exigibilidade perante instituições de crédito legítimas. O dinheiro eletrônico possui um emitente contra o qual exista uma pretensão jurídica de recebimento. As criptomoedas não se enquadram em nenhuma dessas qualificações, de forma que não é possível classificá-las como dinheiro, nem como coisas e tampouco como pretensões jurídicas, além de não serem reconhecidas por lei alemã como meios legais de pagamento.

No Brasil, no entanto, não há tal dissonância, considerando que a atual legislação não torna inadequada a classificação de criptoativos em "valores" ou até mesmo como "ativos". Em outras palavras, a natureza jurídica das criptomoedas não é, por si só, empecilho para a aplicação da legislação anti-lavagem de dinheiro.

O que prejudica a aplicação prática da lei de combate à lavagem de capitais no país não reside, portanto, na dificuldade em considerar ou não as criptomoedas como objeto do delito, e sim nas suas características intrínsecas, que inviabilizam, diversas vezes, a imputação de sua autoria e de sua materialidade. Se as transações realizadas na rede *blockchain*, além de criptografadas, não registram a identidade de quem vendeu e quem comprou a criptomoeda fruto da prática de lavagem de capitais, como a investigação desse delito será capaz de chegar ao(s) seu(s) autor(es)?

[13] ESTELITTA, Heloísa. **Criptomoedas e lavagem de dinheiro**. Revista de Direito Getúlio Vargas, São Paulo, v. 16, n. 1, p. 1-13, 2020. Disponível em: <https://doi.org/10.1590/2317-6172201955>. Acesso em 26 de nov. 2022.

Outro problema reside na falta de obrigatoriedade das *exchanges*[14] em identificar a autoria das transações nelas realizadas e comunicar ao COAF e às demais autoridades operações suspeitas, nos termos Capítulo V da Lei 9.613/1998, que versa sobre as "pessoas sujeitas ao mecanismo de controle". Isso porque o art. 9º do referido normativo estipula as pessoas físicas e jurídicas que se submetem às determinações legais nele estabelecidos, e de sua leitura depreende-se que as *exchanges* de criptoativos não estão abarcados no rol do dispositivo. Sendo assim, a elas não se exige a observância do art. 10 e art. 11 da Lei 9.613/1998, segundo os quais:

> Art. 10. As pessoas referidas no art. 9º:
>
> I - Identificarão seus clientes e manterão cadastro atualizado, nos termos de instruções emanadas das autoridades competentes;
>
> II - manterão registro de toda transação em moeda nacional ou estrangeira, títulos e valores mobiliários, títulos de crédito, metais, ou qualquer ativo passível de ser convertido em dinheiro, que ultrapassar limite fixado pela autoridade competente e nos termos de instruções por esta expedidas;
>
> III - deverão adotar políticas, procedimentos e controles internos, compatíveis com seu porte e volume de operações, que lhes permitam atender ao disposto neste artigo e no art. 11, na forma disciplinada pelos órgãos competentes; **(Redação dada pela Lei nº 12.683, de 2012)**
>
> IV - deverão cadastrar-se e manter seu cadastro atualizado no órgão regulador ou fiscalizador e, na falta deste, no Conselho de Controle de Atividades Financeiras (Coaf), na forma e condições por eles estabelecidas; **(Incluído pela Lei nº 12.683, de 2012)**
>
> V - deverão atender às requisições formuladas pelo Coaf na periodicidade, forma e condições por ele estabelecidas, cabendo-lhe preservar, nos termos da lei, o sigilo das informações prestadas.
>
> Art. 11. As pessoas referidas no art. 9º:
>
> **I -** dispensarão especial atenção às operações que**, nos termos de instruções emanadas das autoridades competentes,**

[14] *Exchanges* podem ser definidas como "a pessoa jurídica, ainda que não financeira, que oferece serviços referentes a operações realizadas com criptoativos, inclusive intermediação, negociação ou custódia, e que pode aceitar quaisquer meios de pagamento, inclusive outros criptoativos". Definição dada pelo art. 5º, II, da Instrução Normativa RFB n. 1888, de 3 de maio de 2019. Disponível em: <http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?idAto=100592>. Acesso em 26 de nov. 2022.

> possam constituir-se em sérios indícios dos crimes previstos nesta Lei**, ou com eles relacionar-se;**
>
> **II -** deverão comunicar ao Coaf**, abstendo-se de dar ciência de tal ato a qualquer pessoa, inclusive àquela à qual se refira a informação, no prazo de 24 (vinte e quatro) horas, a proposta ou realização: (Redação dada pela Lei nº 12.683, de 2012)**
>
> **a) de** todas as transações referidas no inciso II do art. 10, acompanhadas da identificação de que trata o inciso I **do mencionado artigo; e (Redação dada pela Lei nº 12.683, de 2012)**
>
> **b) das** operações referidas no inciso I**; (Redação dada pela Lei nº 12.683, de 2012)**
>
> **III -** deverão comunicar ao órgão regulador **ou fiscalizador da sua atividade ou, na sua falta, ao Coaf, na periodicidade, forma e condições por eles estabelecidas,** a não ocorrência de propostas, transações **ou operações** passíveis de serem comunicadas **nos termos do inciso II**[15]**. (grifos nossos)**

Rodrigues e Kurtz explicam melhor a problemática de as *exchanges* não serem obrigadas a fornecerem informações sobre clientes e transações suspeitas às autoridades responsáveis pela apuração e investigação da lavagem de capitais:

> As exigências de devida diligência acerca do cliente, um dos eixos do pilar preventivo do combate à lavagem de dinheiro, presumem a possibilidade técnica de análise das transações a partir do acesso ao cliente e às informações a ele relativas. Daí a importância de jurisdições de sigilo para os sujeitos delitivos, sobretudo durante a fase de estratificação. Ao desvincular as identidades das partes na plataforma de qualquer dado que as identifique fora dela, as criptomoedas automatizam o sigilo financeiro de forma que não pode ser revertida pela via regulatória[16].

Com o pseudoanonimato inerente às criptomoedas e a aparente ausência de responsabilidade das *exchanges* em observarem às regras legais atinentes ao *Know Your Costumer* no Brasil, a crescente utilização dos criptoativos para cometimento da lavagem de capitais revela a urgência igualmente crescente em se regulamentar o seu uso pelos usuários e as obrigações a serem atribuídas aos programas

[15] BRASIL. **Lei n. 9.613, de 3 de março de 1998**. Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras - COAF, e dá outras providências. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l9613.htm>. Acesso em: 21 de nov. 2022.

[16].RODRIGUES, Gustavo; KURTZ, Lahis. Criptomoedas e regulação antilavagem de dinheiro no G20. **Instituto de Referência em Internet e Sociedade**, 27 set., 2019. Disponível em: <http://bit.ly/2m9pOz0>. Acesso em: 26 de nov. 2022.

responsáveis pela sua custódia ou operacionalização, tópico que será mais bem analisado no próximo capítulo.

4 A NECESSIDADE DE REGULAÇÃO DAS CRIPTOMOEDAS FRENTE AO SEU USO COMO FACILITADOR À LAVAGEM DE CAPITAIS

Conforme bem apontam Rodrigues e Kurtz, são três as principais possibilidades regulatórias dos criptoativos para viabilizar a efetiva aplicação da política de lavagem de dinheiro: a autorregulação industrial, a regulação nacional/legal e a abordagem baseada em risco.

A autorregulação industrial, como o próprio nome sugere, diz respeito à regulação realizada pelos próprios envolvidos com as transações que envolvam criptomoedas. Por entenderem a dinâmica e o funcionamento desse ativo, e por possuírem a expertise apta a prever as consequências práticas de uma regulação, diz-se que os componentes desse mercado seriam, em tese, os mais adequados para estabelecer políticas de transparência, *duo diligence*[17] e *know your costumer*, todas naturalmente orientadas à mitigação da prática de lavagem de capitais.

Como abordado anteriormente, a tecnologia de *blockchain*, apesar de armazenar informações acerca das pontas da transação de criptomoeda, não armazena dados relativos à identidade de quem a comercializou – característica denominada de pseudoanonimato. Dessa forma, para conter a prática de lavagem de dinheiro e de outros delitos aos quais o pseudoanonimato das criptomoedas beneficia, deve-se atribuir às corretoras, carteiras digitais e outros *softwares* de compra, venda e armazenamento de criptomoedas a obrigação de exigirem de seus clientes documentos que comprovem suas devidas identidades. Apesar de alguns desses *softwares* exigirem atualmente um nível de comprovação, como nome e endereço de e-mail, a ausência de consenso e de padrão nessa exigência tornam

[17] O *due diligence* é uma prática de mercado baseada em análise de informações a ser realizada previamente a tomada de decisões, com o intuito de minimizar os riscos oriundos dessas decisões.
O que é Due Diligence? Entenda o esse conceito financeiro na prática. **EXPENSE ON**. Gestão de Despesas, 2022. Disponível em: <https://expenseon.com/gestao-de-despesas/due-diligence/>. Acesso em 30 de nov. 2022.

usuários mal-intencionados predispostos a realizarem suas transações em algum servidor que seja mais negligente nesse sentido.

Hoje, já existem iniciativas internacionais não-governamentais que visam promover boas práticas no comércio de criptoativos, a fim de prevenir a lavagem de capitais. Desde 2015, por exemplo, a Digital Asset Transfer Authority (DATA ou "Autoridade de Transferência de Ativos Digitais") estabelece[18] quatro pilares anti-lavagem de dinheiro às pessoas jurídicas que lidam com criptoativos, tais como: (i) a indicação de um diretor experiente de *compliance*; ii) o treinamento do corpo diretivo e dos funcionários da organização acerca do que consiste lavagem de dinheiro e financiamentos ilegais, como reconhecê-los e o que fazer se houver suspeitas sobre tais atividades; (iii) a criação de procedimentos para promover o *due diligence* de consumidores, vendedores, empregadores, investidores, limites de contas, transações, acesso à informação e seu respectivo registro; (iv) a revisão anual dos procedimentos e programas implementados independentemente dessas recomendações serem ou não exigidas por lei.

Outra ação semelhante, abrangendo agora a regulação pela abordagem baseada em risco, é promovida pela Financial Action Task Force (FATF). A organização foi criada em 1990 por países do G7 e hoje é subscrita por quase 200 nações[19]. O próprio FATF reconhece que os países participantes possuem diferentes ordenamentos jurídicos e organizações socioeconômicas distintas umas das outras, de forma que seus normativos visam estabelecer apenas padrões internacionais a serem seguidos quando adequados à realidade de cada nação. Segundo o FATF:

> A abordagem baseada no risco permite aos países, no âmbito dos requisitos do GAFI, adotar um conjunto de medidas mais flexível, a fim de direcionar seus recursos de forma mais eficaz e aplicar medidas preventivas proporcionais à natureza

[18] DIGITAL ASSET TRANSFER AUTORITY. Anti-Money Laundery Guidelines. Disponível em: <https://www.slideshare.net/DataSecretariat/data-aml-guidelines-june-2015>. Acesso em 30 de nov. 2022. p. 2-3.

[19] HOUBEN, Robby; SNYERS, Alexander. **Cryptocurrencies and blockchain**: legal context and implications for financial crime, money laundering and tax evasion, 2018. Estudo, União Européia, 2018. Disponível em: <https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf>. P. 58.

> dos riscos, a fim de focar seus esforços da maneira mais eficaz[20].

Algumas das recomendações do FATF para a política anti-lavagem de dinheiro (ALD) são: (i) a identificação dos riscos oriundos dessa prática, cujo grau é decisivo para a definição das ações e dos recursos adequados à sua eficaz mitigação; (ii) a adoção de políticas nacionais com base nos riscos identificados primariamente, cuja revisão deve ocorrer regularmente e orientadas pela(s) autoridade(s) competente(s); (iii) a criminalização da lavagem de capitais com base nas Convenções de Viena e de Palermo; e (iv) a adoção de medidas práticas e legislativas que permitam a apreensão, sem prejuízo dos direitos de terceiros de boa-fé, da propriedade submetida à lavagem de capitais ou dos instrumentos utilizados para tanto, ou que viabilizem tais ações assecuratórias por parte das autoridades.

Quanto à lavagem de dinheiro com criptomoedas, o FATF orienta a adoção de iniciativas nacionais para o enquadramento dos denominados *Virtual Asset Service Providers* (VASPs) nas obrigações estabelecidas pelas legislações ALD em cada país, sob pena de sanções penais, civis e administrativas, extensíveis a seus diretores. Esses VASPs abrangem, por exemplo, as *exchanges* e as plataformas de trocas diretas e armazenamento de criptoativos. Como não é possível alterar a qualidade do pseudoanonimato das criptomoedas, a recomendação é exigir dessas plataformas a obrigatoriedade de identificação dos seus usuários. Além disso, o FATF indica que os VASPs obtenham licenças ou registros oficiais nos países em que operam para legitimar suas operações e facilitar o monitoramento de transações suspeitas pelas autoridades locais.[21]

Como sugerido pelo FATF, no Brasil já foram protocolados alguns projetos de lei destinados a melhor regulamentar as criptomoedas, com o intuito de delimitar as condições para que sejam legitimamente comercializadas e, assim, de prevenir e reprimir ilícitos por meio dela cometidos. Um deles é o Projeto de Lei 3.825/2019

[20] FATF (2012-2022). **International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation**. FATF, Paris, France. Disponível em: <www.fatf-gafi.org/recommendations.html>. Acesso em 30 de nov. 2022. P. 8.

[21] FATF (2012-2022**). International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation**. FATF, Paris, France. Disponível em: <www.fatf-gafi.org/recommendations.html>. Acesso em 30 de nov. 2022. P. 76-77.

(PL 3.825/2019), que visava disciplinar os serviços referentes a operações realizadas com criptoativos eletrônicas de negociação[22].

Apesar de utilizar a mesma denominação de criptoativos daquela que já vigorava com o art. 5º, inciso I, da Instrução Normativa RFB n. 1888/2019, a PL 3.825/2019 estabelecia diretrizes importantes para a regulação do funcionamento dos criptoativos no país no tocante ao combate à lavagem dinheiro. Alguns exemplos são: a submissão do funcionamento das *exchanges* à autorização prévia do Banco Central do Brasil (art. 3º); a obrigação das *exchanges* na implantação das diligências devidas para conhecimento e comprovação da identidade do cliente e de sua capacidade econômico-financeira (art. 9º, IV) e das diligências adequadas contra lavagem de dinheiro e demais crimes financeiros, fomentando a autorregulação (art. 9º, V); a atribuição do Banco Central na orientação e fiscalização das *exchanges* no cumprimento das normas relativas às transações com criptomoedas e às políticas ALD (art. 13); e a inclusão dessas empresas no rol daquelas obrigadas ao mecanismo de controle da Lei 9.613/1998 (art. 15).

Em que pese representar um avanço na regulação jurídica das criptomoedas no país, quando considerado a lacuna legislativa atinente à matéria, o referido projeto foi arquivado em 26 de abril de 2022, em votação em Plenário do Senado Federal. Em seu lugar, um substitutivo foi levado à deliberação na Câmara dos Deputados: o Projeto de Lei 4.401/2021 (PL 4.401/2021)[23].

Nele, o funcionamento das *exchanges* submeter-se-ia à autorização prévia de autoridade da administração pública federal, a ser indicado em ato do Poder Executivo (art. 2º, *caput*) – e não do Banco Central, conforme previa o PL 3.825/2019. As definições de ativos financeiros (art. 3º, parágrafo único), os parâmetros a serem observados por essas empresas (art. 4º, *caput*), o órgão responsável pela supervisão das atividades das *exchanges* e as respectivas atribuições (arts. 6º e 7º) também seriam delegados a ato do Poder Executivo, de

[22] BRASIL. Senado Federal. **Projeto de Lei nº 3.825, de 2019**. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/137512>. Acesso em 30 de nov. 2022.

[23] BRASIL. Senado Federal. **Projeto de Lei nº 4.401, de 2021**. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/151264>. Acesso em 30 de nov. 2022.

forma que o substitutivo não traz mudanças legislativas autossuficientes e substanciais na regulamentação dos criptoativos frente à política ALD no Brasil, quando comparado com o projeto de lei arquivado e com as orientações do FATF, por exemplo.

As alterações mais significativas a serem promovidas no ordenamento pátrio caso o PL 4.401/2021 seja aprovado pelo Congresso Nacional são a inclusão de novo tipo legal no Código Penal (art. 171-A - fraude com a utilização de ativos virtuais, valores mobiliários ou ativos financeiros); a equiparação das *exchanges* às instituições financeiras para fins de aplicação da Lei 7.492/1986, que trata dos crimes contra o sistema financeiro nacional (art. 11); a alteração a causa de aumento de pena do art. 1º, §4º, da Lei 9.613/1998, de forma a incluir, como uma de suas hipóteses de incidência, a utilização de ativo virtual (art. 12); e a inclusão das *exchanges* no rol das pessoas sujeitas ao mecanismo de controle da Lei de Lavagem de Dinheiro, em seu art. 9º, parágrafo único (art. 12)

5 CONSIDERAÇÕES FINAIS

As inovações socioeconômicas oriundas de um mundo globalizado trouxeram inegavelmente inúmeros benefícios para a sociedade e a forma pela qual ela se organiza. Conforme se facilitam relacionamentos e negócios, a humanidade encontra caminhos para se desenvolver de forma próspera. A possibilidade de transações financeiras em ambiente digital certamente encurtou esses caminhos, mas também trouxe uma preocupação legítima para as autoridades e ao Direito: o uso de critpoativos para a prática de lavagem de capitais e de outros delitos em esfera virtual.

Nos termos dos capítulos antecedentes, entidades públicas e privadas ao redor do mundo vêm acompanhando essa nova realidade, com o objetivo de averiguar possíveis soluções (dentre elas, a jurídica) para o enfrentamento desses delitos, que se tornaram mais sofisticados – e, portanto, demandam uma investigação de mesma qualidade – com as características inerentes das criptomoedas, que acabam por facilitar a sua prática e dificultar a atuação das autoridades. A autorregulação, a

abordagem por riscos e a atuação legislativa nacional foram apontadas como os três modelos mais adequados à mitigação da lavagem de capitais com criptoativos.

Concluiu-se que o projeto de lei que melhor contribuiria no início da regulamentação da matéria no país foi arquivado, e o seu substitutivo, encaminhado à deliberação parlamentar, pouco irá contribuir para essa finalidade. Dada a permanência da lacuna regulamentar no país e a ausência de medidas práticas fomentadas pelas autoridades nacionais, percebe-se que o Brasil ainda se encontra distante do propósito de fortalecer o seu ordenamento jurídico e as suas políticas públicas para atender, de forma eficaz e adequada, à regulamentação do uso de criptoativos no país.

REFERÊNCIAS

ANDRADE, Mariana Dionísio de. Tratamento jurídico das criptomoedas: a dinâmica dos bitcoins e o crime de lavagem de dinheiro. **Revista Brasileira de Políticas Públicas**, Brasília, v. 7, n. 3, p. 43-59, dez. 2017.

BRASIL. **Comunicado BACEN 25.306, de 19 de fevereiro de 2014**. Disponível em: <https://www.legisweb.com.br/legislacao/?id=265825>. Acesso em: 21 nov. 2022.

BRASIL. Secretaria da Receita Federal do Brasil. **Instrução Normativa RBF nº 1888, de 03 de maio de 2019**. Disponível em: <http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?idAto=100592>. Acesso em 26 de nov. 2022.

BRASIL. **Lei 9.613/1998, de 3 de março de 1998**. Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras - COAF, e dá outras providências. Disponível em: <https://www.planalto.gov.br/ccivil_03/Leis/L9613.htm>. Acesso em 21 de nov. 2022.

BRASIL. Senado Federal. **Projeto de Lei nº 3.825, de 2019**. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/137512>. Acesso em 30 de nov. 2022.

BRASIL. Senado Federal. **Projeto de Lei nº 4.401, de 2021**. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/151264>. Acesso em 30 de nov. 2022.

BITCOIN. **Google**, 2022. Disponível em: <https://www.google.com/search?q=valor+bitcoin&oq=valor+bitcoin&aqs=chrome..69i57j69i59j0i3j0i512l7.1829j1j7&sourceid=chrome&ie=UTF-8>. Acesso em 30 de nov. 2022.

DIGITAL ASSET TRANSFER AUTORITY. **Anti-Money Laundery Guidelines**. Disponível em: <https://www.slideshare.net/DataSecretariat/data-aml-guidelines-june-2015>. Acesso em 30 de nov. 2022.

ESTELITTA, Heloísa. **Criptomoedas e lavagem de dinheiro**. Revista de Direito Getúlio Vargas, São Paulo, v. 16, n. 1, p. 1-13, 2020. Disponível em: <https://doi.org/10.1590/2317-6172201955>. Acesso em 26 de nov. 2022. p. 14.

FATF (2012-2022). **International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation**. FATF, Paris, France. Disponível em: <www.fatf-gafi.org/recommendations.html>. Acesso em 30 de nov. 2022. p. 8.

GONÇALVES, João; LOPES, Karina. O que é globalização. **Politize**, 2017. Disponível em: <https://www.politize.com.br/globalizacao-o-que-e/>. Acesso em 12 de nov. 2022.

HOUBEN, Robby; SNYERS, Alexander. **Cryptocurrencies and blockchain**: legal context and implications for financial crime, money laundering and tax evasion, 2018. Estudo, União Européia, 2018. Disponível em: <https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf>.

JOSA, Lucas. Bitcoin Pizza Day: a história da refeição mais cara de todos os tempos. **Exame**, 2021. Disponível em: <https://exame.com/future-of-money/criptoativos/bitcoin-pizza-day-a-historia-da-refeicao-mais-cara-de-todos-os-tempos/>. Acesso em: 21 nov. 2022.

Know Your Costumer – Conceito. **KYC BRASIL**. Disponível em: <https://kycbrasil.com/conceito/>. Acesso em 26 de nov. 2022.

MARQUES, Gabriel. Ativo ainda mais escasso: 90% de todos os bitcoins já foram minerados. **Exame**, 2022. Disponível em: <https://exame.com/future-of-money/ativo-ainda-mais-escasso-90-de-todos-os-bitcoins-ja-foram-minerados/>. Acesso em 30 de nov. 2022.

O que é Due Diligence? Entenda o esse conceito financeiro na prática. **EXPENSE ON**. Gestão de Despesas, 2022. Disponível em: <https://expenseon.com/gestao-de-despesas/due-diligence/>. Acesso em 30 de nov. 2022.

RODRIGUES, Gustavo; KURTZ, Lahis. Criptomoedas e regulação antilavagem de dinheiro no G20. **Instituto de Referência em Internet e Sociedade**, 27 set., 2019. Disponível em: <http://bit.ly/2m9pOz0>. Acesso em: 26 de nov. 2022.

ULRICH, Fernando. **Bitcoin: a moeda na era digital**. São Paulo: Instituto Ludwig Von Mises Brasil, 2014. Disponível em: <https://produtos.infomoney.com.br/hubfs/ebook-bitcoin.pdf>. Acesso em: 04 mar. 2023.

BENS JURÍDICOS PENAIS EM CRIMES DIGITAIS: COMPORTAMENTO E PUNIÇÃO

Deividison Alves Lopes[1]

RESUMO

O artigo analisa o sentido protetivo atribuído aos bens jurídicos pela Ciência Penal, especialmente aqueles ligados ao ambiente virtual. Tem como objetivo, a partir de uma construção teórica sobre o tipo, injusto e bem jurídico, examinar os desdobramentos do crime de invasão de dispositivo informático no contexto da criminalidade digital, e identificar o vácuo de tipicidade em uma área de especial relevância social.

Palavras-Chaves: Tipo Penal. Bem jurídico. Crimes digitais.

ABSTRACT

The article analyzes the protective meaning attributed to legal interests by Criminal Science, especially those related to the virtual environment. It aims, from a theoretical construction on the type, unfair and legal, to examine the consequences of the crime of invading a computer device in the context of digital criminality, and to identify the vacuum of typicality in an area of special social relevance.

Keywords: Criminal type. Legal Asset. Cybercrime.

1 INTRODUÇÃO

A utilização cada vez mais diversificada de ferramentas eletrônicas no cotidiano, transformou a internet, considerada primordialmente apenas como mais um instrumento de práticas criminosas, em um verdadeiro cenário de disputa e de relevância penal para o Estado.

Assim, a otimização dos sistemas eletrônicos gerou maior utilidade social, ao passo que a rede de computadores, tornou-se não só um meio efetivo de

[1] Aluno do curso de Pós-graduação *Lato Sensu* do Centro Universitário de Brasília – CEUB/ICPD, Direito e Prática Processual nos Tribunais.

compartilhamento de dados, mas um dos alicerces políticos e econômicos da sociedade atual.

Notadamente, a criminalidade, também um fenômeno social[2], diante de novas perspectivas, também sofreu transformações. Antigos crimes ganharam novos meios e formas de execução, ao passo que surgiram situações lesivas aos bens digitais, que dado o relevante interesse, aperfeiçoaram-se para bens jurídicos e consequentemente, ocasionam novos tipos penais.

Contudo, há lacunas normativas que precisam ser preenchidas, a fim de alinhar o interesse social à efetiva proteção dos bens jurídicos penais mais recentes. A profusão de estelionatos, o aumento de crimes contra a honra, racismo, divulgação da pornografia infantil, danos informáticos, acessos ilegítimos e invasões de dispositivos evidenciam a necessidade do aperfeiçoamento do controle jurídico no mundo virtual.

Nesse aspecto, destaca-se a Lei nº 12.737/12, que dispõe sobre o crime de invasão de dispositivo informático e representa, de certa forma, marco normativo em relação aos crimes digitais propriamente ditos, tipificando condutas que não eram previstas, de forma específica, como infrações penais.

Ressalte-se que, apesar de sua contemporaneidade, ainda há vácuos no ordenamento vigente e o resultado é a sensação de impunidade e aumento da insegurança jurídica.

A possibilidade de interpretação extensiva do crime de invasão de dispositivo informático, o histórico de tipificação por analogia e equiparação para a subsunção de determinadas ações lesivas, são fatores que revelam também a incidência de questões processuais penais e constitucionais ao tema, em específico, a tipicidade, o princípio da legalidade e a vedação à analogia prejudicial ao réu, objetos suficientes para desenvolvimento de outros estudos.

Tema contemporâneo, o assunto ganha destaque não só por questões processuais. A evolução histórica do conceito de tipo dentro da Ciência do Direito

[2] Sobre criminalidade e seus determinantes sociais: DURKHEIM, Emile. **Le crime, phénomène normal**. J.-M. Tremblay, 2006.

Penal, e a teoria do seu sentido protetivo, atribuem a discussão critérios para análises acerca do processo de tipificação e a formação de uma política criminal que efetivamente combata a criminalidade digital.

O objeto do artigo absorve todos esses pensamentos, e os devolve em forma de um exame crítico acerca dos diplomas normativos vigentes. O objetivo é exatamente realizar uma análise integrada e ponderada acerca dos parâmetros principiológicos que sustentam a teoria do crime, e refletir acerca dos desafios atuais que o mundo digital nos impõe.

2 COMPORTAMENTO E PUNIÇÃO: TIPO E INJUSTO PENAL

Definir o comportamento objeto de punição pelo poder estatal é um desafio central não só para o legislador, mas também para a Ciência do Direito Penal. Nesse sentido, Claus Roxin explica "a penalização de um comportamento necessita, em todo o caso, de uma legitimação diferente da simples discricionariedade do legislador"[3].

Antes de traçar ideias sobre o limite do poder de intervenção jurídico-penal e sua relação com os crimes virtuais, é importante entender elementos da teoria do crime, a fim de estabelecer uma base teórica sólida, especialmente quando se discute sobre bens jurídicos penais digitais e condutas atípicas.

Assim, iniciamos por um dos alicerces do desenvolvimento do direito penal como método, o tipo. É o elemento que possibilita externar, em face das exigências da legalidade penal, a avaliação dogmática da imposição de uma pena, razão pela qual é mandamental entender que o direito penal pensa e raciocina por meio de tipos[4].

[3] ROXIN, Claus. **A proteção de bens jurídicos como função do Direito Penal**. 2. ed. Porto Alegre: Livraria do Advogado Editora, 2009.

[4] Como entender e integrar a ação humana, esse é o marco inicial dos grandes sistemas que tentam explicar e teorizar sobre o crime, desde o sistema causal/naturalista até o sistema finalista. Ressalta-se que a ideia do tipo por Ernst von Beling, com a obra A Doutrina do Delito-Tipo, publicada em 1906, marca uma verdadeira revolução na teoria do crime, especialmente a noção de tipo, como um elemento autônomo. VON BELING, Ernst. **A ação punível e a pena**. São Paulo: Rideel, 2007.

A lição é de extrema importância, porque ao tratar de temas recentes, como os crimes digitais, a escassez de respostas jurisprudenciais e legislativas nos faz retornar às bases do direito penal, essencialmente filosófica e sociológica[5].

O tipo, no seu sentido estrito, compõe-se, normalmente, de um núcleo, representado pela ação ou omissão e seu objeto, tendo como base a lesão a um determinado bem jurídico[6].

A categoria teórica do tipo passou por algumas fases de evolução, alterando também as dinâmicas da teoria do crime. Inicialmente, imaginou-se que o delito poderia ser composto unicamente por elementos objetivos, e a culpabilidade, na outra ponta, passaria exclusivamente por elementos subjetivos[7].

Adiante, o reconhecimento de elementos subjetivos do tipo e o entendimento de que a culpabilidade também depende de circunstâncias objetivas revolucionou a definição da tipicidade[8].

O elemento subjetivo especial do tipo está presente em um dos principais tipos relacionados aos crimes informáticos. Conforme a estrutura do art. 154-A, incluído pela Lei nº 12.737, de 2012, é considerado crime a invasão de dispositivo

[5] A dogmática penal distancia-se do positivismo, pois, os pensadores à época, antes de penalistas, eram filósofos do direito, neokantistas, e que introduziram à metodologia penal percepções do materialismo, para além de definições formais ou explicações causalistas, superando o primeiro sistema da teoria do crime, Cezar Roberto Bitencourt complementa: "A insuficiência do positivismo foi constatada no campo jurídico muito antes na ciência jurídico-penal, especialmente em sua modalidade naturalista sociológica iniciada por Von Liszt com sua "direção moderna"; ao contrário da ciência jurídico-civil, não houve necessidade de aguardar a transformação das condições econômico-sociais iniciada com a inflação que destroçou a República de Weimar e consumou-se como segundo pós-guerra. Como destaca Mir Puig, "talvez o precoce abandono do positivismo em nossa ciência penal tenha sido favorecido pela circunstância de que alguns dos filósofos do direito aos quais se deve a introdução do neokantismo na metodologia jurídica, especialmente Radbruch e Sauer, eram, ao mesmo tempo, penalistas. Mas, sem dúvida, foram as exigências específicas da dogmática penal que decidiram o giro do positivismo a um método no qual novamente a valoração e a perspectiva material foram recepcionadas". BITENCOURT, Cezar Roberto. Tratado de Direito Penal. São Paulo: Saraiva Educação SA, 2015.

[6] BITENCOURT, Cezar Roberto. **Tratado de Direito Penal**. São Paulo: Saraiva Educação SA, 2015. p. 344-345.

[7] Sobre a reestruturação das categorias do delito, da fase da Independência por Beling à concepção valorativa desenvolvida por Mezger: BITENCOURT, Cezar Roberto. **Tratado de Direito Penal**. São Paulo: Saraiva Educação SA, 2015. p. 340-341.

[8] A descoberta dos elementos normativos do tipo abala a teoria da neutralidade valorativa penal, e a definição da tipicidade como função meramente descritiva. Roxin, a partir das teses de Mayer e Beling no capítulo intitulado "O descobrimento dos elementos normativos do tipo" traz grandes lições sobre o tema.
ROXIN, Claus. **Teoría del tipo penal**: tipos abiertos y elementos del deber jurídico. Talcahuano: Depalma Bueno Aires, 1979. Versión castellana del Prof. Dr. Enrique Bacigalupo (Universidade de Madrid). p. 60-63.

"com o fim de obter". Essa finalidade está no campo psíquico do agente, e a tipicidade só deve se operar em sua presença[9]. Nessa linha, indispensável a lição de Max Ernst Mayer, que amplia o conceito de tipicidade, considerando também associação entre o tipo e indícios da antijuridicidade, pensamento norteador da segunda fase da evolução do conceito de tipo[10].

Formalmente, tipicidade é o perfeito encaixe do fato à norma penal, ou seja, a subsunção da situação fática à uma moldura anterior e abstrata, prevista na lei penal. Materialmente, a tipicidade é constituída da violação de um bem jurídico digno de proteção penal[11].

São essas definições que traçam ligações com os momentos de crise da tipicidade, e do direito penal como um todo, especificamente aqui, em relação aos crimes informáticos.

A tipicidade ao tratar da perfeita correspondência entre a conduta externa e um modelo comportamental previsto e proibido pela lei penal, encontra limites em si. Primeiro, pois em seu sentido formal, o modelo abstrato, proposto por meio de lei

[9] O desafio da concretização da tipicidade do crime de invasão de dispositivo informático encontra-se pela presença do elemento subjetivo especial. Não basta a invasão, é necessário a finalidade de agir, em certa medida, a intenção do agente. Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita.
BRASIL. **Lei n. 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: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 04 mar. 2023.

[10] Mayer introduz a fase indiciária ou *ratio cognoscendi* da teoria do tipo. A relação do tipo com a ilicitude é sequencial. Assim, a presença do tipo antecipa a ilicitude, entendida como a contrariedade ao sistema normativo como um todo. Roxin complementa: "El tipo guarda respecto de la antijuricidad la misma relación que el homo con el fuego: El humo no es fuego ni contiene fuego, pero mientras no se pruebe lo contrário indica la existencia de fuego".
ROXIN, Claus. **Teoría del tipo penal**: tipos abiertos y elementos del deber jurídico. Talcahuano: Depalma Bueno Aires, 1979. Versión castellana del Prof. Dr. Enrique Bacigalupo (Universidade de Madrid). p. 61.

[11] Winfried Hassemer, em sua teoria sobre o bem jurídico, chama atenção para a necessidade de lesividade social das condutas, e assim explica: "[...] A conduta humana somente pode ser então injusto penal, quando lesiona um bem jurídico- com esta máxima a vítima entrou (novamente) no plano, depois que ela esteve por séculos desaparecida atrás dos princípios da reprovabilidade, da contrariedade à norma, do procedimento criminal. A repreensão à violação de uma norma (moral ou ética) não pode ser suficiente ao legislador como fundamento da conduta humana merecedora de pena. Ele precisa antes provar a lesão de um bem jurídico: apresentar uma vítima desta conduta e indicar quanto a esta a lesão de bens, de interesses".
HASSEMER, Winfried. **Introdução aos fundamentos do Direito Penal** (Einfuhrung in die Grundlagen dês Strafrechts). Porto Alegre: Sergio Antonio Fabris, 2000. p.56.

penal, pode carecer de técnica penal em sua construção[12]. Segundo, materialmente, sua aplicabilidade pode não observar a violação do bem jurídico.

Aqui, supera-se a explicação da tipicidade dentro da teoria causalista ou finalística, pois a atribuição de neutralidade ao tipo o distancia da proteção do bem jurídico, contido na norma penal[13]. A lição é extremamente valiosa, pois ela atribui à tipicidade objetivos comuns com a política criminal, o que permite estipular, por exemplo, metas de combate aos crimes virtuais, à própria definição do tipo.

Na linha histórica, essa concepção faz referência a fase do funcionalismo[14] e da tese do sentido de proteção dos tipos penais, de Roxin. Segundo o autor, o sentido de desenvolver um sistema jurídico-penal funcional está em substituir valores do neokantismo, das primeiras fases, por fundamentos político-criminais das teorias modernas da pena[15]. Cláudio Brand complementa:

> Roxin sintetiza sua ideia afirmando que Direito Penal e Política Criminal não se tratam de opostos, sendo o Direito Penal muito mais a forma através da qual as finalidades político-criminais podem ser transferidas para o modo da vigência jurídica, pelo que só a variedade da vida, com todas as suas transformações, torna possível a concretização de uma solução correta, ou seja, adaptada às peculiaridades do caso[16].

Para Roxin, a ação típica constitui "uma unidade de fatores internos e externos, que não pode ser rompida, apenas compreendida em suas singularidades por meio de seus momentos individualizadores objetivos e subjetivos"[17]. Assim, o injusto penal se materializa com a violação de um bem jurídico, em seu sentido de proteção. Tavares traça críticas a essa perspectiva:

---

[12] BRANDÃO, Cláudio. Tipicidade e interpretação no direito penal. **Seqüência Estudos Jurídicos e Políticos**. v. 35, n. 68, p. 59–90, 2014. Disponível em: <https://periodicos.ufsc.br/index.php/sequencia/article/view/2177-7055.2013v35n68p59>. Acesso em: 4 mar. 2023. p. 59-89.

[13] TAVARES, Juarez. **Teoria do injusto penal**. Belo Horizonte: Del Rey, 2002.

[14] O modelo teórico de ROXIN, ao revitalizar o conceito de bem jurídico a partir de uma tese de política criminal ancorada nos preceitos da Constituição, ligada à restrição ao poder de punir estatal, integra a fase funcionalista do tipo.
PEREIRA, Gabriela Xavier. A evolução histórica do tipo em Direito Penal da Independência por Beling à concepção significativa de Vives Antón. Publicação Universidade de Ponta Grossa, Ponta Grossa, v. 16, n. 2, p. 313-321, 2008.

[15] TAVARES, Juarez. **Teoria do injusto penal**. Belo Horizonte: Del Rey, 2002. p. 205-206.

[16] PEREIRA, Gabriela Xavier. A evolução histórica do tipo em Direito Penal da Independência por Beling à concepção significativa de Vives Antón. Publicação Universidade de Ponta Grossa, Ponta Grossa, v. 16, n. 2, p. 313-321, 2008. p. 319.

[17] ROXIN, Claus. **A proteção de bens jurídicos como função do Direito Penal**. 2. ed. Porto Alegre: Livraria do Advogado Editora, 2009.

> Geralmente, insere-se o bem jurídico como pressuposto do tipo, mas na qualidade de objeto de proteção. Na verdade, não se pode instituir como pressuposto do tipo a proteção de bem jurídico porque essa proteção não possui conteúdo real. Em primeiro lugar, não há demonstração de que, efetivamente, a formulação típica diurna conduta proibida proteja o bem jurídico. Em segundo lugar, a proteção do bem jurídico funciona apenas como mera referência formal, sem fundamento material. Finalmente, inserir a proteção do bem jurídico como pressuposto do tipo significa uma opção por uma política criminal puramente sistêmica, de tomar o tipo não como instrumento de garantia, mas sim como instrumento de manutenção e reprodução da ordem. Este último aspecto é ignorado pela dogmática, que, simplesmente, aceita a finalidade protetiva atribuída ao tipo como dado absolutamente irrefutável"[18].

O pensamento não exclui o sentido de proteção do tipo, mas retira seu caráter de pressuposto. Ainda, segundo Tavares: "A reprodução do tipo como ação indica que a norma jurídica definidora do injusto é uma norma de conduta e não uma norma meramente de reconhecimento"[19].

Enquanto norma de conduta, coaduna a finalidade de delimitação do poder de intervenção do Estado, baseada em um pressuposto material. Por essa razão, ao examinar qualquer tipo, é necessário identificar o bem jurídico que possa ser violado, exatamente para atribuir estabilidade e contornos democráticos à definição da ação típica[20].

Dessa forma, o injusto penal se aperfeiçoaria não só pela relação entre tipo e antijuridicidade, mas sim a partir da estrutura desses dois elementos e à significação dos juízos de valor que necessariamente são emitidos sobre a conduta criminosa[21].

[18] TAVARES, Juarez. **Teoria do injusto penal**. Belo Horizonte: Del Rey, 2002. p. 180.
[19] TAVARES, Juarez. **Teoria do injusto penal**. Belo Horizonte: Del Rey, 2002. p. 179-180.
[20] TAVARES, Juarez. **Teoria do injusto penal**. Belo Horizonte: Del Rey, 2002. p. 179.
[21] Sobre o injusto penal, complementa Roxin: "A categoria central do injusto penal não é, pois, a causação do resultado ou finalidade da ação humana, como se vinha acreditando por muito tempo, senão à realização de um risco não permitido. A causalidade é só uma condição necessária, mas não suficiente do injusto penal. Inclusive, admite-se esta declaração só quando se reconhecesse uma causalidade na omissão".
ROXIN, Claus. **A proteção de bens jurídicos como função do Direito Penal**. 2. ed. Porto Alegre: Livraria do Advogado Editora, 2009. p. 42.

3 OS BENS JURÍDICOS PENAIS EM CRIMES DIGITAIS

A incidência de juízos de valor para o aperfeiçoamento da conduta criminosa exemplifica o ideal da proteção de bens jurídicos como legitimador da intervenção do Direito Penal. Enquanto sistema, ao atrelar o conceito de bem jurídico a uma tese de política criminal, consequentemente, há integração com os princípios constitucionais, voltados à restrição do poder de punição estatal[22].

Para Roxin, o bem jurídico pode ser compreendido como circunstâncias reais ou finalidades necessárias para a vida e liberdade civil. Roxin diferencia as realidades das finalidades a partir de um exame de anterioridade[23]. Enquanto realidades, os bens jurídicos carregam um reconhecimento intrínseco, anterior até mesmo ao legislador, como o caso da vida humana, já as finalidades carregam a possibilidade de criação/reconhecimento de outros bens jurídicos, como no caso, a segurança telemática, a garantia do funcionamento dos sistemas de comunicação e a privacidade de dados no âmbito virtual, bens oriundos do ambiente digital.

Nesse sentido, Marcelo Xavier de Freitas reflete: "não há como deixar de questionar se há novos bens jurídicos referentes ao avanço tecnológico e, ainda, se é o caso de receberem bens tutelados por parte do Direito Penal. Assim, não se pode mais tratar dos crimes digitais relacionados apenas e tão somente aos bens jurídicos tradicionalmente protegidos[24]."

Ressalta-se que essa visão puramente funcionalista do bem jurídico não é totalmente aceita, exatamente pela necessidade de estabelecer teses além das bases teóricas de legitimação dos tipos e dos bens jurídicos, Tavares complementa:

> [...] Sustentando sua definição na Constituição, admite que o conceito de bem jurídico possa derivar tanto de dados anteriores à lei penal - mas não anteriores à Constituição - quanto de deveres criados por ela mesma. Embora o conceito de ROXIN possa ser posto em discussão, porque -ao estilo

[22] Sobre o bem jurídico como parâmetro limitador do poder de punição estatal Roxin comenta: "Eu parto de que as fronteiras da autorização de intervenção jurídico-penal devem resultar de uma função social do Direito Penal. O que está além desta função não deve ser logicamente objeto do Direito Penal". ROXIN, Claus. **A proteção de bens jurídicos como função do Direito Penal**. 2. ed. Porto Alegre: Livraria do Advogado Editora, 2009. p. 16.

[23] ROXIN, Claus. **A proteção de bens jurídicos como função do Direito Penal**. 2. ed. Porto Alegre: Livraria do Advogado Editora, 2009. p. 18-19.

[24] CRESPO, Marcelo Xavier de Freitas; MARQUES, Gil da Costa (Org.). **Crimes Digitais**. São Paulo: Saraiva, 2011.p. 58.

> kantiano - se deixa levar pela normatização globalizada, ao assentar-lhe uma base puramente sistêmica, caminha, em vez disso para a construção de um sistema de garantias, ao desvincular da proteção de um bem jurídico a mera proibição de condutas imorais, a proteção de fins puramente ideológicos e todos os preceitos discriminatórios, bem como ao buscar limitações ao poder de punir na própria evolução do grau de utilidade dos dados e dos objetivos que servem de substrato ao bem jurídico[25].

Portanto, percebe-se que os vetores legitimadores do Direito Penal estão diretamente relacionados à configuração social[26]. Ao superar seu valor apenas de validação da norma penal, o bem jurídico absorve valores materiais e sociais. Nesse âmbito, o bem jurídico, portanto, situa-se no núcleo do tipo penal. É a partir do tipo que se extrai o objeto de proteção, essencial para a avaliação da conduta. É nessa avaliação, de maneira quase indireta, que se reconhece os bens e valores merecedores de proteção, resguardando o caráter fragmentário e finalista do Direito Penal[27].

As associações entre bens jurídicos e injustos penais propiciam melhor avaliação de determinadas ações lesivas à sociedade no âmbito digital. A partir dos pensamentos anteriormente expostos, busca-se a identificação dos comportamentos considerados criminosos e sua aproximação ou distanciamento da lesão dos bens jurídicos protegidos.

3.1 A segurança telemática e a privacidade em ambientes virtuais: desdobramentos do artigo 154-a

Antes da invasão ao dispositivo informático ser considerada crime, vislumbrava-se a conduta do agente que invade computador alheio, sem autorização, para fins ilícitos, como crime, a partir da equiparação ou analogia.

---

[25] TAVARES, Juarez. **Teoria do injusto penal**. Belo Horizonte: Del Rey, 2002. p. 197.

[26] BECHARA, Ana Elisa Liberatore S. O rendimento da teoria do bem jurídico no direito penal atual. **Revista Liberdades**, v. 1, n. 1, p. 16-29, ago. 2009. Disponível em: <https://www.ibccrim.org.br/media/posts/arquivos/1/artigo1.pdf >. Acesso em: 04 mar. 2023. p. 22.

[27] A partir da especial relevância na vida social, Tavarez conceitua o bem jurídico em seu aspecto material da seguinte forma: "Bem jurídico é um elemento da própria condição do sujeito e de sua projeção social, e nesse sentido pode ser entendido como um valor que se incorpora à norma como seu objeto de preferência real e constitui, portanto, o elemento primário da estrutura do tipo, ao qual se devem referir a ação típica e todos os demais componentes.
TAVARES, Juarez. **Teoria do injusto penal**. Belo Horizonte: Del Rey, 2002. p. 198.

Exatamente por não existir tipificação, e consequentemente, o reconhecimento de proteção ao bem jurídico descrito ali, as teses de equiparação vinculavam a subtração de dados de um computador ao crime de furto e da inutilização de dados do computador ao crime de dano[28].

O problema inerente à comparação e analogia, excluindo os argumentos processuais e constitucionais, é que, conforme a teoria de legitimação dos tipos penais com sentido de proteção aos bens jurídicos, determinadas ações seriam notadamente atípicas, por ausência de lesão ou colocação de um bem jurídico em risco.

Inclusive, a diferenciação doutrinária entre crimes virtuais próprios ou impróprios passa essencialmente pela identificação da lesão ou risco ao bem jurídico em questão[29].

Exemplificadamente, quando se equipara a subtração de dados ao crime de furto, infere-se que a conduta só é punível em decorrência da lesão ao patrimônio. Na formação de um sistema penal alinhado às ciências do Direito penal, e em um Estado Democrático de Direito, deveria ser a conduta punível pois ultrapassa o risco permitido da segurança de dados informáticos e lesaria tal bem[30].

---

[28] RAMOS JÚNIOR, Hélio Santiago. **Invasão de Dispositivo Informático e a Lei 12.737/12**: Comentários ao art. 154-A do Código Penal Brasileiro. In: XI Simpósio Argentino de Informática y Derecho 2013. p. 106.

[29] O critério de diferenciação entre crimes próprios e impróprios é de suma importância, ainda mais no exame dos bens jurídicos tutelados, acrescenta-se "Assim é que surge a diferença entre delitos informáticos puros ou próprios, que são aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados); e os delitos informáticos impuros ou impróprios que "já se encontram devidamente tipificados no ordenamento jurídico pátrio, uma vez que o manuseio do computador e da Internet é mero meio, simples codificação no modus operandi do delito, não implicando no delito."
RAMOS JÚNIOR, Hélio Santiago. **Invasão de Dispositivo Informático e a Lei 12.737/12**: Comentários ao art. 154-A do Código Penal Brasileiro. In: XI Simpósio Argentino de Informática y Derecho 2013. p. 107.

[30] No capítulo "Injusto penal e o risco permitido", o autor reflete sobre o equilíbrio entre as liberdades civis e a teoria da imputação objetiva".
ROXIN, Claus. **A proteção de bens jurídicos como função do Direito Penal**. 2. ed. Porto Alegre: Livraria do Advogado Editora, 2009. p. 39-45.

Assim, um dos motivos determinantes para a inclusão do dispositivo 154-A, era a necessidade de normas específicas que protegessem bens jurídicos determinados, reconhecidos pela mudança e transformação social[31].

Não há como negar que o avanço tecnológico estabeleceu novos paradigmas de bens jurídicos tutelados pelo Direito Penal. A informação, os dados, a confiabilidade e segurança dos sistemas e redes informáticas e de comunicação formam um conjunto de valores indispensáveis para a vida atualmente[32].

Nesse sentido, o crime de invasão de dispositivo informático materializa a segurança telemática e a privacidade em âmbito digital, como bens jurídicos penais. O tipo do caput do art. 154-A do CP, descreve a conduta de invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita[33].

Da análise do caput, percebe-se também que o crime de invasão de dispositivo informático é crime formal, logo, ainda que o agente não obtenha, adultere ou destrua dados, ou que obtenha vantagem ilícita com a instalação de vulnerabilidades, o delito já estaria consumado, pois o crime independe do resultado obtido previsto no tipo.

Ao adiantar o estágio da punibilidade, a proteção do bem jurídico é questionada pois o comportamento delituoso poderia estar distante da lesão dos bens

---

[31] Para além da função protetiva do bem jurídico, é importante refletir sobre suas origens, que inequivocamente acompanham as transformações e realidades sociais. Álvaro Mayrink, destaca: "Sabe-se que o conceito de bem jurídico deve ser procurado na realidade social, a qual deve ser conjugada com as plúrimas variantes do progresso e do bem-estar da sociedade. Para a essência dogmática, o bem jurídico assume prevalente significado para um correto entendimento nos planos valorativo, metodológico e normativo. Para estabelecer que bens e valores sejam merecedores de uma norma exige-se a especial relevância na vida social (ultima ratio do controle social)".
Da Costa, Álvaro Mayrink. Direito penal e proteção dos bens jurídicos. 2011. p. 04. DA COSTA, Álvaro Mayrink. Direito penal e proteção dos bens jurídicos. **Revista de EMERJ**, Rio de Janeiro, v. 14, n. 53, p. 7- 15, 2011.

[32] CRESPO, Marcelo Xavier de Freitas; MARQUES, Gil da Costa (Org.). **Crimes Digitais**. São Paulo: Saraiva, 2011. p. 59.

[33] O crime de invasão de dispositivo informático, embora recente, já passou por modificações. Instituído na lei 12.737/2012, a Lei nº14.155/2021 promoveu alterações no tipo do art. 154-A, a mais considerável, em sua redação do caput. Antes de 2021, a ação só seria delituosa se a invasão fosse cometida mediante violação indevida de mecanismo de segurança, atualmente, a conduta prescinde de violação de mecanismo de segurança, expandindo as hipóteses de incidência.

jurídicos[34]. Não é o caso do art. 154-A. Com objetivo de proteger a segurança telemática e a privacidade em meio digital, a ação de invadir com o intuito de obter vantagem ilícita é suficiente para, em certo grau, lesar tais bens.

Superada a leitura do caráter formal da conduta, o tipo do art.154-A da lei 12.737/12 é relevante, pois, no contexto dos crimes digitais, é um dos mais amplos e uma das poucas espécies de crime digital próprios[35]. Dessa forma, simboliza verdadeira inovação jurídica-penal, ao resguardar a confidencialidade de dados, a proteção de acessos ilegítimos e a disponibilidade de serviços informáticos.

Todavia, a série de bens jurídicos provenientes do mundo digital não estão totalmente tutelados pelo crime de invasão de dispositivo informático, portanto, a necessidade de proteção supera o próprio conteúdo do tipo penal, o que eleva potencialmente o risco de aplicação da analogia na resolução de problemas práticos e resulta em ações reconhecidamente prejudiciais, próximas ao núcleo do tipo de invasão, mas que não puníveis na esfera penal.

4 AÇÕES PREJUDICIAIS ATÍPICAS: LESÕES AOS BENS JURÍDICOS QUE NÃO ENCONTRAM PUNIÇÃO

Conforme exame do dispositivo, o legislador optou por não tipificar outras condutas, que de igual forma, lesam e colocam em risco a segurança telemática ou a privacidade no âmbito digital. Existem uma série de ações praticadas através da rede mundial de computadores que representam prejuízo e lesão a bens jurídicos. Podem

[34] Ainda em Roxin, o autor ao teorizar sobre a proteção dos bens jurídicos como legitimação dos tipos penais, trata dos casos de crimes formais, os quais, ao adiantar o estágio de punibilidade, consideram crime a conduta ainda que não lesione o bem, pelo menos de maneira direta: "O problema inerente a estas normas é que o comportamento culpado está ainda bastante distante da verdadeira lesão de bens jurídicos. Do conceito de proteção de bens jurídicos se infere, então, somente que, tratando-se de uma antecipação considerável da punibilidade, necessita-se fundamentar, especialmente porque isto é necessário para a proteção efetiva do bem jurídico".
ROXIN, Claus. **A proteção de bens jurídicos como função do Direito Penal**. 2. ed. Porto Alegre: Livraria do Advogado Editora, 2009. p. 28.

[35] Por outro lado, o Estatuto da Criança e Adolescente avançou em relação ao reconhecimento do ambiente virtual como meio eficaz de consumação de crimes, exemplificadamente: Art. 244-B. Corromper ou facilitar a corrupção de menor de 18 (dezoito) anos, com ele praticando infração penal ou induzindo-o a praticá-la: (Incluído pela Lei nº 12.015, de 2009) Pena - reclusão, de 1 (um) a 4 (quatro) anos. (Incluído pela Lei nº 12.015, de 2009) § 1 º Incorre nas penas previstas no caput deste artigo quem pratica as condutas ali tipificadas utilizando-se de quaisquer meios eletrônicos, inclusive salas de bate-papo da internet.
BRASIL. **Lei n. 8.069, de 13 de julho de 1990**. Dispõe sobre o Estatuto da Criança e do Adolescente. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l8069.htm>. Acesso em: 04 mar. 2023.

figurar nessa lista: intrusão informática, interferência em sistemas[36], violação de bancos de dados privados, vazamento de dados, scamming, utilização de engenharia social e condutas subsequentes a obtenção e transferência ilegal de dados.

Ressalta-se que não se trata necessariamente de um silêncio eloquente, mas de verdadeira falha na percepção de outras ações prejudiciais, e consequentemente, na ausência de prévia cominação legal, atípicas.

Também contribui para a dificuldade de aplicação do tipo, alguns termos e expressões utilizadas no Art. 154-A, especialmente a definição do verbo invadir e da percepção que se faz em relação à autorização do ingresso pela vítima.

Integrando o tipo a partir de uma interpretação restritiva, percebe-se que a invasão de dispositivo informático se difere de acesso ilegítimo. A existência do elemento subjetivo especial modula e exclui o mero ingresso como crime. Se a intenção de obter, adulterar, destruir dados ou informações não estiver presente, o acesso sem autorização não terá repercussão penal, ainda que claramente esteja presente a violação da confidencialidade de dados[37].

Da mesma forma, a ausência de autorização também só terá relevância, se presente o especial fim do agente. Por outro lado, se o agente estiver devidamente autorizado, afasta-se a tipicidade dos núcleos: obter, adulterar ou destruir. Em relação à instalação de vulnerabilidades[38], a presença de autorização é irrelevante.

---

[36] A lei 12.737/12 também inclui a interferência do funcionamento de sistemas como conduta criminosa, a partir do Art. 266 § 1º: Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.
BRASIL. **Lei n. 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: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 04 mar. 2023.

[37] O crime de invasão de dispositivo informático notadamente não contempla outras formas mais recentes de obtenção de dados, além da invasão, em seu sentido estrito, entre elas o spyware, trojans e keyloggers.
XAVIER, Marcelo. **Crimes Digitais**. Saraiva Educação SA, 2017.

[38] Para efeitos de aplicação da norma penal, as vulnerabilidades devem ser entendidas como qualquer código malicioso capaz de expor a risco a segurança dos dados e das informações armazenadas ou o próprio funcionamento do dispositivo informático, pois a lei penal deve ser interpretada teleologicamente, conforme os princípios jurídicos que lhe são próprios, buscando extrair o seu exato alcance e real significado através da busca da vontade da lei, atendendo à sua finalidade que está expressa no art. 1º da Lei 12.737/12, isto é, a tipificação criminal de delitos informáticos.

Enfatiza-se que os conceitos computacionais nem sempre serão harmônicos às definições penais, todavia, para a correta aplicação, prioriza-se sempre a segunda definição.

5 CONSIDERAÇÕES FINAIS

Os bens jurídicos referentes ao espaço tecnológico já são uma realidade social, e estão inseridos no âmbito de proteção do Direito Penal. Os desdobramentos do Art. 154-A da lei 12.737/12 revelam o caminho a ser percorrido em busca do sentido protetivo que o tipo penal tem por atribuição e fundamento.

Ao longo do artigo fica evidente que a formação de conceitos e teses acerca do tipo, bem jurídico e injusto penal passaram e estão em constante evolução. Nesse passo, o marco teórico de que o Direito Penal protege, no limite do alcance de seus tipos penais, os bens jurídicos frente a lesões e riscos não permitidos, demonstra a dissonância entre a política criminal atual e as diversas situações práticas que o desenvolvimento da internet propicia.

Dessa forma, o vácuo normativo das condutas lesivas aos bens jurídicos digitais e a cumulação de critérios para a incidência do crime de invasão de dispositivo informático evidenciam o caráter desafiador que os crimes digitais impõem ao Direito Penal e às Ciências Criminais.

REFERÊNCIAS

BECHARA, Ana Elisa Liberatore S. O rendimento da teoria do bem jurídico no direito penal atual. **Revista Liberdades**, v. 1, n. 1, p. 16-29, ago. 2009. Disponível em: <https://www.ibccrim.org.br/media/posts/arquivos/1/artigo1.pdf >. Acesso em: 04 mar. 2023.

BITENCOURT, Cezar Roberto. Tratado de Direito Penal. São Paulo: Saraiva Educação SA, 2015.

BRANDÃO, Cláudio. Teoria jurídica do crime. Rio de Janeiro: Forense, 2003.

BRANDÃO, Cláudio. Tipicidade e interpretação no direito penal. **Seqüência Estudos Jurídicos e Políticos**. v. 35, n. 68, p. 59–90, 2014. Disponível em: <https://periodicos.ufsc.br/index.php/sequencia/article/view/2177-7055.2013v35n68p59>. Acesso em: 4 mar. 2023. p. 59-89.

BRASIL. Lei n. 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l8069.htm>. Acesso em: 04 mar. 2023.

BRASIL. Lei n. 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: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em 04 mar. 2023.

CRESPO, Marcelo Xavier de Freitas; MARQUES, Gil da Costa (Org.). **Crimes Digitais**. São Paulo: Saraiva, 2011.

DA COSTA, Álvaro Mayrink. Direito penal e proteção dos bens jurídicos. **Revista de EMERJ**, Rio de Janeiro, v. 14, n. 53, p. 7- 15, 2011.

D'AVILA, Fabio Roberto. O modelo de crime como ofensa ao bem jurídico. Elementos para a legitimação do direito penal secundário. **Revista Opinião Jurídica,** Fortaleza, v. 4, n. 7, p. 76-95, 2006.

DURKHEIM, Emile. **Le crime, phénomène normal**. J.-M. Tremblay, 2006.

HASSEMER, Winfried. **Introdução aos fundamentos do Direito Penal** (Einfuhrung in die Grundlagen dês Strafrechts) Porto Alegre: Sergio Antonio Fabris, 2000.

PEREIRA, Gabriela Xavier. **A evolução histórica do tipo em Direito Penal da Independência por Beling à concepção significativa de Vives Antón**. Publicação Universidade de Ponta Grossa, Ponta Grossa, v. 16, n. 2, p. 313-321, 2008.

RAMOS JÚNIOR, Hélio Santiago. **Invasão de Dispositivo Informático e a Lei 12.737/12**: Comentários ao art. 154-A do Código Penal Brasileiro. Simpósio Argentino de Informática y Derecho, 2013.

ROXIN, Claus. **A proteção de bens jurídicos como função do Direito Pen**al. 2. ed. Porto Alegre: Livraria do Advogado Editora, 2009.

ROXIN, Claus. **Teoría del tipo penal**: tipos abiertos y elementos del deber jurídico. Talcahuano: Depalma Bueno Aires, 1979.

SMANIO, Gianpaolo Poggio. O conceito de bem jurídico penal difuso. **Revista do Tribunal Regional Federal da 1ª Região**, Brasília, v. 16, n. 11, p. 54-59, 2004.

TAVARES, Juarez. **Teoria do injusto penal**. Belo Horizonte: Del Rey, 2002.

VON BELING, Ernst. **A ação punível e a pena**. São Paulo: Rideel, 2007.

XAVIER, Marcelo. **Crimes Digitais**. Saraiva Educação SA, 2017.

RESPONSABILIDADE PENAL DA PESSOA JURÍDICA NO CONTEXTO DOS CRIMES CIBERNÉTICOS

Gabriela Freire Martins[1]

RESUMO

A Convenção de Budapeste, cujo texto foi recentemente aprovado pelo Senado Federal, prevê em seu escopo a necessidade de responsabilização da pessoa jurídica por crimes cibernéticos. Em face disso, o presente artigo discute os novos problemas trazidos pela revolução digital e os danos provocados pela criminalidade cibernética perpetrada pelos entes morais, além de revisitar as discussões doutrinárias sobre a responsabilidade penal da pessoa jurídica no âmbito das teorias penais desenvolvidas da tradição do *Civil Law*.

Palavras-chave: Crime Cibernético. Responsabilidade Penal da Pessoa Jurídica. *Civil Law*.

ABSTRACT

Recently, the Senate of Brazil approved accession to the Budapest Convention on cybercrime, which requires that each Party takes measures to hold legal entities accountable for those crimes. The present article discusses problems arising from the digital revolution, provides an overview of the damage caused by corporate cybercrime, and reviews doctrinal discussions about corporate criminal liability in the scope of the *Civil Law* legal system.

Keywords: Cybercrime. Corporate Criminal Liability. *Civil Law*

1 INTRODUÇÃO

Os institutos do Direito Penal foram inicialmente desenvolvidos para lidar com a criminalidade perpetrada por pessoas naturais em um mundo fisicamente palpável. Ocorre que, na sociedade contemporânea, as relações e os conflitos

[1] Aluna do curso de pós-graduação lato sensu do Centro Universitário de Brasília – CEUB/ICPD. E-mail: gabriela.martins@sempreceub.com.

travados no mundo virtual desafiam os Estados a encontrar respostas adequadas à criminalidade cibernética.

Os dados e as informações armazenadas em meios digitais podem ser explorados para fins econômicos, políticos, sociais ou de inteligência. No ano de 2009, uma única rede de espionagem infectou pelo menos 1.295 computadores, localizados em 103 países, com o agravante de que cerca de 30% deles pertenciam às classes diplomática, política, econômica ou militar[2]. Em 2011, a empresa de segurança Norton afirmou que 431 milhões de pessoas haviam sido vítimas de crimes cibernéticos no ano anterior e que o proveito ilícito obtido ultrapassava as receitas somadas do mercado global de maconha, cocaína e heroína[3]. Dado o crescimento da rede mundial de computadores, é provável que, desde então, esses números tenham alcançado proporções ainda mais alarmantes.

Diante da cadeia de valor existente nos meios digitais, não são apenas os indivíduos que podem ser tentados a cometerem atos ilícitos em proveito próprio, mas também as pessoas jurídicas. Afinal, como bem observou Manuel Castells, "a geração de conhecimentos e a capacidade tecnológica são ferramentas fundamentais para a concorrência entre empresas, organizações de todos os tipos e, por fim, países"[4]. A História já demonstrou o impacto que os entes morais são capazes de causar por meio de suas atividades no mundo cibernético. Vale lembrar que a *Wikileaks* vazou mais de 1 milhão de documentos diplomáticos sensíveis[5], a *Cambridge Analytica* e o *Facebook* interferiram no processo eleitoral americano[6] e o

[2] DEIBERT, Ronald *et al*. **Tracking GhostNet:** Investigating a Cyber Espionage Network. 2009. Information Warfare Monitor - Universidade de Toronto e The SecDev Group. Canadá, 2009. Disponível em: <https://citizenlab.ca/wp-content/uploads/2017/05/ghostnet.pdf>. Acesso em: 15 nov. 2022.

[3] GLOBAL cybercrimes cost $114 billion annually – Symantec. **Reuters**, 2011. Disponível em: <https://www.reuters.com/article/oukin-uk-symantec-idUKTRE7861XQ20110907>. Acesso em: 17 nov. 2022.

[4] CASTELLS, Manuel. **A sociedade em rede**. 6 ed. São Paulo: Paz e Terra, 2002. p. 165.

[5] PARLAMENTO EUROPEU. **Did the WikiLeaks incidents create more or less democracy in the world?** 2011. Disponível em: <https://www.europarl.europa.eu/news/en/headlines/society/20110131STO12842/did-the-wikileaks-incidents-create-more-or-less-democracy-in-the-world>. Acesso em 16 nov. 2022.

[6] NGUYEN, Michael. Cambridge Analytica – the true implications for the future of democracy. **Australian Institute of International Affairs,** 2018. Disponível em: <https://www.internationalaffairs.org.au/resource/cambridge-analytica-what-the-event-actually-illustrates-for-the-future-of-democracy/>. Acesso em 16 nov. 2022.

Telegram foi alvo de polêmicas ao se recusar a cooperar com as investigações de atividades criminosas ocorridas no seio da plataforma[7].

Antes mesmo da revolução digital, a associação entre pessoas jurídicas e delitos já era discutida nos contextos dos crimes ambientais, econômicos e transnacionais, motivo pelo qual países como França, Itália, Espanha e Estados Unidos adotaram políticas criminais destinadas à responsabilização desses entes[8]. No Brasil, conquanto haja propostas visando à ampliação da responsabilidade penal da pessoa jurídica[9], ainda há grande resistência política, jurídica e social no que se refere ao tema.

Feitas essas considerações, o presente artigo tem por objetivo revisitar as discussões sobre a responsabilidade penal da pessoa jurídica à luz dos problemas trazidos pelos crimes cibernéticos.

2 CONVENÇÃO DE BUDAPESTE

A Convenção de Budapeste, cujo texto foi aprovado recentemente pelo Senado Federal[10], prevê diretrizes e mecanismos de cooperação para que os Estados nacionais consigam responder adequadamente aos crimes cibernéticos. Em síntese, o instrumento previu as seguintes espécies delitivas (artigos 2º a 10): infrações contra a confidencialidade, integridade e disponibilidade de sistemas e dados informáticos; infrações relacionadas com computadores; infrações relacionais com o conteúdo

[7] OLIVEIRA, Michele. Como a Alemanha cercou o Telegram e conseguiu banir contas por crime de ódio. **Folha de São Paulo**, 2022. Disponível em: <https://www1.folha.uol.com.br/mundo/2022/03/como-a-alemanha-cercou-o-telegram-e-conseguiu-banir-contas-por-crime-de-odio.shtml>. Acesso em: 16 nov. 2022.

[8] SANTOS, Ílison Dias dos; MELO, Jhonatas Péricles Oliveira de. A responsabilidade penal da pessoa jurídica: análise exploratória do modelo espanhol e do modelo proposto pelo projeto de novo código penal brasileiro. **Revista de Derecho Procesal de la Asociación Iberoamericanade la Universidad de Salamanca**, Salamanca, p. 121-137, 2017. Disponível em: <https://iudicium.usal.es/numeros/2/files/assets/basic-html/page-121.html>. Acesso em: 14 nov. 2022.

[9] A título de exemplo, o Projeto de Lei do Senado n° 236, de 2012, que dispõe sobre o novo Código Penal brasileiro, propõe dois artigos que acrescentam novas hipóteses de responsabilização criminal da pessoa jurídica.

[10] BRASIL. **Decreto Legislativo n. 37, de 2021**. Aprova o texto da Convenção sobre o Crime Cibernético, celebrada em Budapeste, em 23 de novembro de 2001. Diário do Senado Federal, 14 out. 2021. Disponível em: <https://legis.senado.leg.br/norma/35289207/publicacao/35300588>. Acesso em: 15 nov. 2022.

(pornografia infantil); e infrações relacionadas com o direito do autor e direitos conexos[11].

Além disso, os artigos 12 e 13 instam as partes a adotar medidas legislativas, entre outras, para assegurar que as pessoas coletivas sejam responsabilizadas por atos cometidos por seus próprios integrantes ou por atos cometidos por outros indivíduos a fim de beneficiá-las. Para tanto, os Estados poderão se valer de sanções e medidas, penais ou não penais, desde que sejam eficazes, proporcionais e dissuasivas[12]. Em face disso, surge a seguinte indagação: a responsabilização de uma pessoa jurídica por atos ilícitos em âmbito cibernético deveria ocorrer em sede penal ou deveria se restringir somente às esferas civil e administrativa?

3 RESPONSABILIDADE PENAL DA PESSOA JURÍDICA

Segundo Ílison dos Santos e Jhonatas de Melo, por motivos de natureza político-criminal, a responsabilidade penal de pessoas jurídicas é mais difundida em países que adotam o sistema *Common Law* do que naqueles que adotam o *Civil Law*[13]. A hipótese dos autores é de que a dogmática penal da Europa continental se desenvolveu simultaneamente à ascensão da classe burguesa ao poder, diferentemente da Inglaterra, em que a burguesia prescindiu de proteção especial porque a teoria do delito fora estabelecida antes da Revolução Industrial e da ascensão do capital[14].

Tradicionalmente, o direito brasileiro, derivado do *Civil Law*, se ateve ao paradigma que rejeita a responsabilização de pessoas jurídicas na seara penal

[11] CONSELHO DA EUROPA. ETS nº 185. **Convenção sobre o Crime Cibernético.** Budapeste: 23 nov. 2001. Disponível em: <https://rm.coe.int/16802fa428>. Acesso em: 15 nov. 2022.

[12] CONSELHO DA EUROPA. ETS nº 185. **Convenção sobre o Crime Cibernético.** Budapeste: 23 nov. 2001. Disponível em: <https://rm.coe.int/16802fa428>. Acesso em: 15 nov. 2022.

[13] SANTOS, Ílison Dias dos; MELO, Jhonatas Péricles Oliveira de. A responsabilidade penal da pessoa jurídica: análise exploratória do modelo espanhol e do modelo proposto pelo projeto de novo código penal brasileiro. **Revista de Derecho Procesal de la Asociación Iberoamericanade la Universidad de Salamanca**, Salamanca, p. 121-137, 2017. Disponível em: <https://iudicium.usal.es/numeros/2/files/assets/basic-html/page-121.html>. Acesso em: 14 nov. 2022.

[14] SANTOS, Ílison Dias dos; MELO, Jhonatas Péricles Oliveira de. A responsabilidade penal da pessoa jurídica: análise exploratória do modelo espanhol e do modelo proposto pelo projeto de novo código penal brasileiro. **Revista de Derecho Procesal de la Asociación Iberoamericanade la Universidad de Salamanca**, Salamanca, p. 121-137, 2017. Disponível em: <https://iudicium.usal.es/numeros/2/files/assets/basic-html/page-121.html>. Acesso em: 14 nov. 2022.

(princípio *societas delinquere non potest*). Nada obstante, a Constituição de 1988[15] conferiu certa abertura para a responsabilização dos entes morais nos crimes ambientais (art. 225, § 3°)[16] e nos crimes contra a ordem econômica e financeira e contra a economia popular (art. 173, § 5º)[17]. Por uma série de razões, o legislador ordinário editou apenas a Lei de Crimes Ambientais (Lei nº 9.605/1998), a qual se tornou alvo de críticas severas.

Juarez Cirino dos Santos documentou a divergência sobre o tema. Na hipótese do art. 173, § 5º, da Constituição, alguns afirmavam que a expressão "punições compatíveis com sua natureza" se referia à responsabilidade penal, enquanto outros alegavam que a melhor interpretação apontava para sanções aplicáveis em outros ramos do Direito[18]. Igualmente, havia quem afirmasse que o art. 225, § 3°, referir-se-ia à aplicação de sanções penais e administrativas a pessoas físicas e jurídicas indistintamente, ao passo que uma segunda corrente argumentava que o dispositivo deveria ser lido da seguinte forma: as condutas de pessoas físicas as sujeitam a sanções penais, e as atividades de pessoas jurídicas implicam sanções administrativas[19].

Ferrenhos defensores da dogmática penal, os críticos da responsabilidade da pessoa jurídica sustentam, até hoje, a existência de obstáculos insuperáveis nos ordenamentos jurídicos derivados do sistema *Civil Law*, sobretudo em virtude da alegada incompatibilidade da medida com os elementos que compõem o conceito analítico de crime (ato típico, ilícito e culpável).

[15] BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República. Diário Oficial da União, 5 out. 1988. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 15 nov. 2022.

[16] "Art. 225 [...] § 3º As condutas e atividades consideradas lesivas ao meio ambiente sujeitarão os infratores, pessoas físicas ou jurídicas, a sanções penais e administrativas, independentemente da obrigação de reparar os danos causados."

[17] "Art. 173 [...] § 5º A lei, sem prejuízo da responsabilidade individual dos dirigentes da pessoa jurídica, estabelecerá a responsabilidade desta, sujeitando-a às punições compatíveis com sua natureza, nos atos praticados contra a ordem econômica e financeira e contra a economia popular."

[18] SANTOS, Juarez Cirino dos. A Responsabilidade Penal da Pessoa Jurídica. **Fórum Administrativo**: Direito Público, Belo Horizonte, v. 2, n. 17, jul. 2002. p.1-3.

[19] SANTOS, Juarez Cirino dos. A Responsabilidade Penal da Pessoa Jurídica. **Fórum Administrativo**: Direito Público, Belo Horizonte, v. 2, n. 17, jul. 2002. p.1-3.

Em relação à tipicidade, alega-se que as pessoas jurídicas seriam incapazes de praticar uma ação voluntária[20] e consciente, pois tais atributos são exclusivamente humanos, e, ao mesmo tempo, por serem desprovidos de psique, os entes morais não preencheriam o pressuposto subjetivo do tipo (conduta eivada de dolo ou culpa)[21]. As pessoas jurídicas também não teriam aptidão para agir com culpabilidade, pois esta constitui um juízo de reprovação que recai sobre a vontade individual de realizar atos contrários ao Direito[22]. Além disso, tais entes não poderiam ser avaliados quanto à sua maturidade ou sanidade mental (imputabilidade), não possuiriam capacidade de reflexão sobre a ilicitude de seus atos e não seriam afetados por perturbações emocionais que tornam inexigíveis a adoção de condutas diversas[23]. Em face disso, estariam igualmente ausentes os seguintes pressupostos para a aplicação da pena: a existência de uma ação antijurídica e culpável, a capacidade psicofísica de experimentar a dor ou aflição e a possibilidade de reorientação da vontade humana para os fins de prevenção dos delitos[24].

Conquanto a responsabilidade penal de entes morais seja incompatível com o raciocínio metodológico adotado pela maioria das escolas penais, Davi Tangerino entende que o funcionalismo de Claus Roxin conferiu abertura para novas abordagens, na medida em que o poder de punir passa a se justificar na função preventiva da pena, e não na culpabilidade, ou seja, "ao paradigma da pena justa se seguiu um de pena útil"[25]. Soma-se a isso as tentativas de resolver os problemas supramencionados por meio de modelos teóricos alternativos, a saber: a) a

[20] A esse respeito, Luis Gracia Martín esclarece: "*um ato voluntário, isto é, constituído no mínimo por um movimento corporal gerado a partir de uma sinapse neuronal e conduzido por uma ordem cerebral, e é evidente que nada disso pode estar presente em qualquer ser que não seja o humano".*
MARTÍN, Luis Gracia. Crítica de las modernas construcciones de una mal llamada responsabilidad penal de la persona jurídica. **Revista Electrónica de Ciencia Penal y Criminología**, n. 18, p. 1-95, 2016. p. 8.

[21] SANTOS, Juarez Cirino dos. A Responsabilidade Penal da Pessoa Jurídica. **Fórum Administrativo**: Direito Público, Belo Horizonte, v. 2, n. 17, jul. 2002. p.3.

[22] MARTÍN, Luis Gracia. Crítica de las modernas construcciones de una mal llamada responsabilidad penal de la persona jurídica. **Revista Electrónica de Ciencia Penal y Criminología**, n. 18, p. 1-95, 2016. p. 10.

[23] SANTOS, Juarez Cirino dos. A Responsabilidade Penal da Pessoa Jurídica. **Fórum Administrativo**: Direito Público, Belo Horizonte, v. 2, n. 17, jul. 2002. p. 5-6.

[24] MARTÍN, Luis Gracia. Crítica de las modernas construcciones de una mal llamada responsabilidad penal de la persona jurídica. **Revista Electrónica de Ciencia Penal y Criminología**, n. 18, p. 1-95, 2016. p. 10-12.

[25] TANGERINO, Davi de Paiva. Culpabilidade e responsabilidade penal da pessoa jurídica. **Revista logos ciencia y tecnología,** v. 3, n. 1, p. 186-202, dez. 2011. Disponível em: <https://dialnet.unirioja.es/descarga/articulo/4166920.pdf>. Acesso em: 15 nov. 2022.

culpabilidade por defeito de organização, de Klaus Tiedemann, segundo a qual a responsabilidade decorre de falha nas medidas de cuidado ou vigilância que poderiam evitar o delito[26]; b) o injusto de sistema, de Ernst Lampe, em que a culpabilidade decorre de uma filosofia criminógena ou de organização deficiente no âmbito da pessoa jurídica[27]; c) a culpabilidade por ausência de supervisão, de Günter Heine, que consiste na responsabilização por déficits organizacionais capazes de criar riscos empresariais[28].

A despeito disso, os defensores da dogmática tradicional não se convenceram. Em primeiro lugar, porque a punição se justificaria na violação de uma norma preventiva (deveres de cuidado, organização, vigilância etc.), e não na norma penal, o que importaria em violação ao princípio da legalidade[29]. Em segundo lugar, porque a desorganização e a falta de controle dependeriam de condutas praticadas por sujeitos que compõem a pessoa jurídica, de modo que esta acabaria sendo punida por ações daqueles[30].

Em âmbito jurisprudencial, o Superior Tribunal de Justiça (STJ) tentou compatibilizar as previsões da Lei de Crimes Ambientais com as regras e princípios que regem o direito penal brasileiro[31]. No *RESP n. 564.960/SC,* por exemplo, a Corte destacou que a responsabilização penal de pessoas jurídicas por crimes ambientais foi uma escolha política do constituinte originário, representando não só

[26] TIEDEMANN, 1998 apud TANGERINO, Davi de Paiva. Culpabilidade e responsabilidade penal da pessoa jurídica. **Revista logos ciencia y tecnología,** v. 3, n. 1, p. 186-202, dez. 2011. Disponível em: <https://dialnet.unirioja.es/descarga/articulo/4166920.pdf>. Acesso em: 15 nov. 2022.

[27] LAMPE, 1994 apud TANGERINO, Davi de Paiva. Culpabilidade e responsabilidade penal da pessoa jurídica. **Revista logos ciencia y tecnología,** v. 3, n. 1, p. 186-202, dez. 2011. Disponível em: <https://dialnet.unirioja.es/descarga/articulo/4166920.pdf>. Acesso em: 15 nov. 2022.

[28] HEINE, 2006 apud TANGERINO, Davi de Paiva. Culpabilidade e responsabilidade penal da pessoa jurídica. **Revista logos ciencia y tecnología,** v. 3, n. 1, p. 186-202, dez. 2011. Disponível em: <https://dialnet.unirioja.es/descarga/articulo/4166920.pdf>. Acesso em: 15 nov. 2022.

[29] MUÑOZ**,** Afonso Galán. Ação, tipicidade e culpabilidade penal da pessoa jurídica em tempos de *compliance*: uma proposta interpretativa**. Revista de Direitos Fundamentais & Democracia**, Curitiba, v. 25, n. 3, p. 179, set./dez. 2020. Disponível em: <https://web.s.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=1&sid=d9bf8c83-7f5b-497e-8b5a-84906fce075c%40redis>. Acesso em: 16 nov. 2022.

[30] MUÑOZ**,** Afonso Galán. Ação, tipicidade e culpabilidade penal da pessoa jurídica em tempos de *compliance*: uma proposta interpretativa**. Revista de Direitos Fundamentais & Democracia**, Curitiba, v. 25, n. 3, p. 179, set./dez. 2020. Disponível em: <https://web.s.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=1&sid=d9bf8c83-7f5b-497e-8b5a-84906fce075c%40redis>. Acesso em: 16 nov. 2022.

[31] TANGERINO, Davi de Paiva. Culpabilidade e responsabilidade penal da pessoa jurídica. **Revista logos ciencia y tecnología,** v. 3, n. 1, p. 186-202, dez. 2011. Disponível em: <https://dialnet.unirioja.es/descarga/articulo/4166920.pdf>. Acesso em: 15 nov. 2022.

uma medida repressiva, mas também preventiva[32]. Quanto aos elementos do conceito de crime, o STJ considerou que a pessoa física que age em nome e em benefício da pessoa jurídica pratica uma ação que fundamenta a existência de uma conduta típica. Outrossim, a culpabilidade se confundiria com o conceito de responsabilidade social e poderia ser evidenciada a partir da análise da conduta do representante legal ou administrador do ente moral[33]. Finalmente, no *RESp n. 989.089/SC,* o STJ buscou solucionar o problema do elemento subjetivo do tipo por intermédio da dupla imputação (obrigatoriedade de responsabilização simultânea do ente moral e da pessoa física que atua em seu nome ou benefício), de modo que o elemento subjetivo da pessoa natural suprisse a carência deste elemento na pessoa jurídica[34].

Em que pesem os aludidos esforços, Davi Tangerino chama atenção para duas questões: a falha em responsabilizar diretamente a pessoa jurídica, pois o STJ buscou elementos do conceito de crime no representante legal para, em seguida, transferir a responsabilidade ao ente moral; e o fato de a Corte ter ratificado a responsabilização penal objetiva por crimes ambientais[35], baseada exclusivamente

[32] BRASIL. Superior Tribunal de Justiça (5. Turma**)**. Recurso Especial. **REsp n. 564960/SC**. I. Hipótese em que pessoa jurídica de direito privado, juntamente com dois administradores, foi denunciada por crime ambiental, consubstanciado em causar poluição em leito de um rio, através de lançamento de resíduos, tais como, graxas, óleo, lodo, areia e produtos químicos, resultantes da atividade do estabelecimento comercial [...]. Relator: Min. Gilson Dipp. Brasília, 02 jun. 2005. Disponível em: <https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=200301073684&dt_publicacao=13/06/2005>. Acesso em: 15 nov. 2022.

[33] BRASIL. Superior Tribunal de Justiça (5. Turma**)**. Recurso Especial. **REsp n. 564960/SC**. I. Hipótese em que pessoa jurídica de direito privado, juntamente com dois administradores, foi denunciada por crime ambiental, consubstanciado em causar poluição em leito de um rio, através de lançamento de resíduos, tais como, graxas, óleo, lodo, areia e produtos químicos, resultantes da atividade do estabelecimento comercial [...]. Relator: Min. Gilson Dipp. Brasília, 02 jun. 2005. Disponível em: <https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=200301073684&dt_publicacao=13/06/2005>. Acesso em: 15 nov. 2022.

[34] BRASIL. Superior Tribunal de Justiça (5. Turma**)**. Recurso Especial. **Recurso Especial n. 989089/SC**. 1. Consoante entendimento do Superior Tribunal de Justiça, "Admite-se a responsabilidade penal da pessoa jurídica em crimes ambientais desde que haja a imputação simultânea do ente moral e da pessoa física que atua em seu nome ou em seu benefício, uma vez que não se pode compreender a responsabilização do ente moral dissociada da atuação de uma pessoa física, que age com elemento subjetivo próprio" (REsp 889.528/SC, Rel. Min. FELIX FISCHER, DJ 18/6/07) [...]. Relator: Min. Arnaldo Esteves Lima. Brasília, 18 ago. 2009. Disponível em: <https://processo.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=200702310357&dt_publicacao=28/09/2009>. Acesso em: 15 nov. 2022.

[35] Davi Tangerino cita como exemplos as decisões do Recurso Especial n. 969.160/RJ e do Recurso Especial n. 610.114/RN.

no dano e no nexo causal, em detrimento de garantias constitucionais fundamentais[36].

Para Luis Gracia Martín, são infrutíferas as tentativas de instituir uma dogmática penal própria para as pessoas jurídicas mediante novos conceitos de ação e culpabilidade, uma vez que o ser humano foi o ponto de partida da teoria do delito e as bases metodológicas da Ciência Penal não comportam a adaptação dos institutos jurídicos às características dos entes morais tão somente para atender demandas pragmáticas ou de política criminal[37].

Por fim, convém registrar que a dificuldade em lidar com o problema posto não é exclusiva do Brasil. Na Alemanha, país resistente à responsabilidade penal dos entes morais, o *Bundesgerichtshof*, órgão de atribuições semelhantes ao STJ, já caminhou em direção à imputação de ilícitos empresariais diretamente ao chefe da organização, o que causou certa controvérsia, conforme relatado por Bernd Schünemann[38].

4 PESSOAS JURÍDICAS E CRIMES CIBERNÉTICOS

O envolvimento de pessoas jurídicas em crimes de natureza eleitoral, econômica, e ambiental é amplamente documentado na literatura, sendo que as organizações criminosas, o tráfico de drogas, o terrorismo e a lavagem de dinheiro não raro contam com a participação desses entes[39]. Mais recentemente, se tornou comum a exploração econômica de atividades ilícitas por pessoas jurídicas, a exemplo das que oferecem o serviço *hack-for-hire*, consubstanciado na

[36] TANGERINO, Davi de Paiva. Culpabilidade e responsabilidade penal da pessoa jurídica. **Revista logos ciencia y tecnología,** v. 3, n. 1, p. 186-202, dez. 2011. Disponível em: <https://dialnet.unirioja.es/descarga/articulo/4166920.pdf>. Acesso em: 15 nov. 2022.

[37] MARTÍN, Luis Gracia. Crítica de las modernas construcciones de una mal llamada responsabilidad penal de la persona jurídica. **Revista Electrónica de Ciencia Penal y Criminología**, n. 18, p. 1-95, 2016. p. 12-17.

[38] SCHÜNEMANN, Bernd. O direito penal é a *ultima ratio* da proteção de bens jurídicos! – Sobre os limites invioláveis do direito penal em um Estado de Direito liberal. **Revista Brasileira de Ciências Criminais**: RBCCrim, v. 13, n. 53, p. 11, mar./abr. 2005.

[39] A esse respeito, convém citar Klaus Tiedemann, segundo o qual a maior parte dos delitos socioeconômicos são cometidos com o auxílio de uma empresa, assim como os crimes organizados que se servem de instituições econômicas como estabelecimentos financeiros, sociedades de exportação e importação, entre outras. TIEDEMANN, Klaus. Responsabilidad penal de las personas jurídicas. **Anuario de Derecho Penal**, Espanha, p. 97-126, 1997. Disponível em: <https://perso.unifr.ch/derechopenal/assets/files/anuario/an_1996_07>.pdf Acesso em: 15 nov. 2022. p. 102.

comercialização de ataques cibernéticos a alvos escolhidos por seus clientes[40]. Uma pesquisa da Associação para Maquinaria da Computação revelou que, por valores entre 100 e 400 dólares americanos, é possível firmar contratos visando à obtenção de informações de terceiros a partir de ataques sofisticados, persistentes, personalizados e capazes de burlar os sistemas de segurança baseados em autenticação de dois fatores[41]. Ademais, o *Citizen Lab* da Universidade de Toronto revelou que milhares de alvos (incluindo políticos, promotores de justiça, dirigentes empresariais, jornalistas e defensores de direitos humanos) foram atacados por *hackers* mercenários possivelmente ligados à empresa indiana de tecnologia BellTroX InfoTech Services, os quais comercializavam informações sobre organizações ambientais, instituições financeiras, veículos de comunicação, escritórios de advocacia, entidades governamentais, entre outras[42].

Há, ainda, empresas de tecnologia que disponibilizam ferramentas que permitem a seus clientes executar, eles próprios, as atividades de *hacking*. A esse respeito, cita-se o caso em que a empresa israelense NSO Group foi acusada de disseminar um código malicioso por intermédio do aplicativo *Whatsapp*, a fim de interceptar mensagens, contatos e dados disponíveis na plataforma, facilitando, assim, as atividades de vigilância e segurança nacional executadas por agências governamentais[43]. Segundo o Citizen Lab, empresas de tecnologia como a NSO Group operam sem transparência ou mecanismos de responsabilidade públicos, na medida em que o mercado de *spywares* carece de regulamentação apropriada em vários países do mundo[44].

[40] MIRIAN, Ariana. Hack for hire. **Communications of The Acm**, v. 62, n. 12, p. 32-37, 21 nov. 2019. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/3359386>. Acesso em: 15 nov. 2022

[41] MIRIAN, Ariana. Hack for hire. **Communications of The Acm**, v. 62, n. 12, p. 32-37, 21 nov. 2019. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/3359386>. Acesso em: 15 nov. 2022

[42] SCOTT-RAILTON, John et al. **Dark Basin**: uncovering a massive hack-for-hire operation. 2020. Relatório Citizen Lab n. 128 – Universidade de Toronto, Canadá, 2020. Disponível em: <https://tspace.library.utoronto.ca/bitstream/1807/106038/1/Report%23128--dark-basin.pdf>. Acesso em: 15 nov. 2022.

[43] UNITED STATES. District Court Northern District of California. Appeal. **Appeal n. 19-7123**. Apelante: Whatsapp Inc. e outros Apelado: NSO Group Technologies Limited e outros. Administrative Office of the United States Courts. California, 2021. Disponível em: <https://cdn.ca9.uscourts.gov/datastore/opinions/2021/11/08/20-16408.pdf>. Acesso em: 15 nov. 2022. p. 2-7.

[44] MARCZAK, Bill *et al.* **Hooking Candiru**: Another Mercenary Spyware Vendor Comes into Focus. 2021. Relatório Citizen Lab n. 139 – Universidade de Toronto, Canadá, 2021. Disponível em:

Assim, existe um risco provável de que os mesmos programas desenvolvidos para auxiliar nas atividades estatais possam ser desvirtuados e comercializados em mercados paralelos para outras finalidades. De fato, há notícias de programas piratas que permitem que indivíduos e organizações executem operações complexas – outrora restritas a agências de governamentais – com o objetivo de coletar informações de alto valor destinadas à comercialização para agentes do setor privado[45].

Por conseguinte, as pessoas jurídicas podem figurar, ao menos em tese, como autoras, partícipes ou beneficiárias de crimes cibernéticos que põem em risco bens jurídicos transindividuais e coletivos – situação que reclamaria tratamento semelhante ao já conferido aos crimes ambientais.

5 NATUREZA DA RESPONSABILIDADE

Conforme mencionado anteriormente, a Convenção de Budapeste confere abertura para que os signatários adotem medidas penais ou não penais em resposta aos crimes cibernéticos praticados por pessoas jurídicas. Considerando que a aprovação do texto do tratado pelo Senado Federal sinaliza a provável incorporação do diploma ao ordenamento jurídico brasileiro, é importante que se discuta se a resposta estatal deve ocorrer pela via penal ou por meio de outros ramos do Direito.

É certo que os críticos da responsabilização penal das pessoas jurídicas não ignoram a necessidade de buscar soluções para a criminalidade cibernética corporativa. Sérgio Salomão Shecaira, por exemplo, ponderou que o Direito Penal tradicional se mostrou insuficiente para responder ao injusto empresarial, visto que a punição de funcionários não produz os efeitos pretendidos, seja porque possuem poder limitado sobre as decisões da empresa, seja porque podem ser substituídos com relativa facilidade[46]. Luis Gracia Martín, por sua vez, defendeu que o

<https://tspace.library.utoronto.ca/bitstream/1807/123967/1/Report%23139--hooking-candiru.pdf>. Acesso em: 15 nov. 2022.

[45] DEIBERT, Ronald *et al*. **Tracking GhostNet:** Investigating a Cyber Espionage Network. 2009. Information Warfare Monitor - Universidade de Toronto e The SecDev Group. Canadá, 2009. Disponível em: <https://citizenlab.ca/wp-content/uploads/2017/05/ghostnet.pdf>. Acesso em: 15 nov. 2022.

[46] SHECAIRA, Sérgio Salomão. Responsabilidade penal das pessoas jurídicas: uma perspectiva do direito brasileiro. **Revista dos Tribunais**, São Paulo, v. 101, n. 921, p. 289, jul. 2012.

ordenamento jurídico deve intervir contra as pessoas jurídicas quando sua existência é instrumentalizada para cometer delitos, ressaltando, todavia, que as estruturas de responsabilidade e as respectivas consequências deveriam ser tratadas fora da esfera penal ou sancionadora, restringindo-se, portanto, aos mecanismos coercitivos do Direito Civil ou do Direito Administrativo não sancionador[47].

Tomando por base a Lei de Crimes Ambientais, seria possível perseguir resultados semelhantes aos das sanções ali preconizadas mediante a aplicação de medidas civis ou administrativas. De fato, Klaus Tiedemann observa que a Criminologia moderna reconheceu que as sanções de diferentes espécies (medidas mistas, penais, administrativas ou civis) são intercambiáveis, produzindo praticamente os mesmos efeitos práticos[48]. A título ilustrativo, Schünemann destaca que a polícia de trânsito alemã exerce com tanta intensidade os poderes da esfera administrativa que a penalização dos cidadãos acaba sendo mais rigorosa do que a esperada na esfera penal e, ao mesmo tempo, o Direito Administrativo falhou em controlar a bolsa de valores *Neuer Markt*, cujo fracasso levou a um prejuízo de 200 bilhões de euros, ao passo que o livre mercado de capitais na Alemanha funciona por meio da intervenção do Direito Penal[49].

Ao nosso ver, transferir para o Direito Civil ou para o Direito Administrativo a incumbência de responder à criminalidade das pessoas jurídicas talvez não seja a melhor solução, pois surgirão outros problemas decorrentes das teorias que fundamentam aquelas disciplinas. Cita-se como exemplo o fato de que a responsabilidade civil punitiva ainda é tratada com muitas ressalvas no Brasil e que a função compensatória das indenizações é insuficiente para lidar com o fenômeno em questão. Se a estrutura de responsabilização do ente moral não produzir um risco econômico considerável, talvez o retorno obtido com o ato ilícito se mostre

[47] MARTÍN, Luis Gracia. Crítica de las modernas construcciones de una mal llamada responsabilidad penal de la persona jurídica. **Revista Electrónica de Ciencia Penal y Criminología**, n. 18, p. 1-95, 2016. p. 80-82.

[48] TIEDEMANN, Klaus. Responsabilidad penal de las personas jurídicas. **Anuario de Derecho Penal**, Espanha, p. 97-126, 1997. Disponível em: <https://perso.unifr.ch/derechopenal/assets/files/anuario/an_1996_07>.pdf Acesso em: 15 nov. 2022. p. 103.

[49] SCHÜNEMANN, Bernd. O direito penal é a *ultima ratio* da proteção de bens jurídicos! – Sobre os limites invioláveis do direito penal em um Estado de Direito liberal. **Revista Brasileira de Ciências Criminais**: RBCCrim, v. 13, n. 53, p. 21-22, mar./abr. 2005.

vantajoso diante do risco esperado, esvaziando o propósito da resposta estatal[50]. Outrossim, a doutrina alemã observa que o controle administrativo só atinge a eficiência esperada se for exercido com excessivo rigor, tornando-o um fardo pesado para toda a coletividade, ao passo que o controle penal se foca em comportamentos verdadeiramente perigosos e produz menos interferências na vida dos cidadãos que agem conforme a lei[51].

Partindo do pressuposto que há certa similaridade entre algumas sanções adotadas nas esferas penal, civil e administrativa, talvez a opção pelo Direito Penal não decorra necessariamente das questões atinentes ao direito material, e sim das possibilidades oferecidas pelo direito processual. Isso porque a jurisdição penal possibilita o uso de meios de investigação mais eficazes e, devido à sua repercussão, é capaz de produzir um efeito intimidador que vai além da sanção propriamente dita[52].

A importância de se analisar a questão sob o prisma do direito formal é que as peculiaridades do meio cibernético dificultam sobremaneira a apuração dos fatos utilizando somente os instrumentos destinados à instrução de processos civis e administrativos. O sistema de atribuição de endereços (*Internet Protocols*) permite aos usuários a ocultação de sua identidade e localização, e as rotas pelas quais circulam as informações (*packet flows*) podem ser redirecionais com a utilização de múltiplos servidores[53]. Aliás, as condutas e os resultados dos crimes cibernéticos não raro ocorrem em locais distintos, o que requer a cooperação entre as autoridades nacionais e internacionais na realização de diligências e no compartilhamento de provas.

---

[50] TIEDEMANN, Klaus. Responsabilidad penal de las personas jurídicas. **Anuario de Derecho Penal**, Espanha, p. 97-126, 1997. Disponível em: <https://perso.unifr.ch/derechopenal/assets/files/anuario/an_1996_07>.pdf Acesso em: 15 nov. 2022. p. 106.

[51] SCHÜNEMANN, Bernd. O direito penal é a *ultima ratio* da proteção de bens jurídicos! – Sobre os limites invioláveis do direito penal em um Estado de Direito liberal. **Revista Brasileira de Ciências Criminais**: RBCCrim, v. 13, n. 53, p. 21, mar./abr. 2005.

[52] TIEDEMANN, Klaus. Responsabilidad penal de las personas jurídicas. **Anuario de Derecho Penal**, Espanha, p. 97-126, 1997. Disponível em: <https://perso.unifr.ch/derechopenal/assets/files/anuario/an_1996_07>.pdf Acesso em: 15 nov. 2022. p. 106.

[53] DEIBERT, Ronald *et al*. **Tracking GhostNet:** Investigating a Cyber Espionage Network. 2009. Information Warfare Monitor - Universidade de Toronto e The SecDev Group. Canadá, 2009. Disponível em: <https://citizenlab.ca/wp-content/uploads/2017/05/ghostnet.pdf>. Acesso em: 15 nov. 2022.

Nesse cenário, os meios de produção de prova podem ser decisivos para a elucidação dos fatos ilícitos. No ordenamento jurídico brasileiro essa constatação é especialmente relevante, haja vista que certos instrumentos são próprios da persecução penal, a exemplo das interceptações de comunicações, da ação controlada, da infiltração de agentes, da prisão temporária etc. Soma-se a isso o fato de que as autoridades devem possuir o conhecimento altamente especializado, sendo difícil identificar na atual estrutura institucional brasileira órgãos capazes de desempenhar adequadamente essa função fora do contexto da justiça criminal.

Embora nenhuma das três esferas – penal, civil ou administrativa – esteja completamente preparada para lidar com a complexidade do fenômeno em questão, é tentador recorrer ao Direito Penal como a solução mais factível em curto prazo. Porém, se, por um lado, o Direito Penal é tentador por questões pragmáticas, por outro lado, o preço a se pagar ao desvirtuar a tradição jurídica cuidadosamente desenvolvida ao longo de séculos pode ser alto, sobretudo quando se considera o delicado equilíbrio o exercício da punibilidade e a proteção de direitos fundamentais.

6 CONSIDERAÇÕES FINAIS

A revolução digital modificou a dinâmica das sociedades contemporâneas, de modo que os crimes cibernéticos ganharam relevância. Ao mesmo tempo, a associação entre pessoas jurídicas e essas espécies delitivas desperta preocupação, entre outros motivos, pelo grave impacto produzido pela utilização indevida de informações e dados obtidos por meios ilícitos.

No plano internacional, a Convenção de Budapeste buscou estabelecer diretrizes para que os países sejam capazes de responder adequadamente à criminalidade cibernética. No entanto, o diploma adotou uma cláusula aberta segundo a qual cada um dos signatários pode optar por diferentes estruturas de responsabilização de pessoas jurídicas, sejam elas penais ou não penais. Naturalmente, esse quadro suscita o debate sobre a responsabilidade penal dos entes morais nos países cuja teoria do delito se desenvolveu na tradição do sistema *Civil Law*, como é o caso do Brasil.

Após o levantamento bibliográfico, foram colhidos argumentos contundentes no sentido de que o estabelecimento da responsabilidade penal da pessoa jurídica é incompatível com os institutos jurídicos penais. Embora o Direito não possa ser encarado como um fim em si mesmo, a distorção das regras e princípios da teoria do delito poderia levar, em última análise, à arbitrariedade e ao casuísmo – situações rechaçadas por regras e princípios insertos na Constituição da República.

Não se pode ignorar que o sistema de justiça criminal, que conta com mecanismos próprios e instituições especializadas, é aquele que apresenta as melhores condições, ao menos no estado atual da arte, de promover a apuração dos crimes cibernéticos, os quais contam com mecanismos sofisticados para ocultar a identidade e a localização de seus autores. Ao mesmo tempo, as sanções civis, administrativas e criminais aplicáveis às pessoas jurídicas possuem tamanha semelhança entre si que a doutrina menciona a possibilidade de intercambiá-las sem que isso implique mudança substancial nos efeitos práticos produzidos.

Ocorre que a exclusão da responsabilização penal da pessoa jurídica por crimes cibernéticos significaria transferir outros impasses teóricos para a dogmática civil e administrativa. Em face disso, tudo indica que as estruturas jurídicas tradicionais são limitadas quando se trata dos problemas advindos da sociedade digital. Eventualmente, a adoção de um microssistema multidisciplinar, com medidas de natureza mista, seja uma opção viável para promover a tutela adequada dos bens jurídicos ameaçados no contexto virtual. Não sendo esse o caso, talvez a Ciência do Direito opte, em um momento futuro, pelo desenvolvimento de uma nova disciplina jurídica, com pressupostos radicalmente distintos, haja vista as diferenças significativas entre os fatos sociais que ocorrem no mundo físico e os que ocorrem no mundo cibernético.

REFERÊNCIAS

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República. Diário Oficial da União, 5 out. 1988. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 15 nov. 2022.

BRASIL. **Decreto Legislativo n. 37, de 2021**. Aprova o texto da Convenção sobre o Crime Cibernético, celebrada em Budapeste, em 23 de novembro de 2001. Diário do Senado Federal, 14 out. 2021. Disponível em: <https://legis.senado.leg.br/norma/35289207/publicacao/35300588>. Acesso em: 15 nov. 2022.

BRASIL. Superior Tribunal de Justiça (5. Turma**)**. Recurso Especial. **REsp n. 564960/SC**. I. Hipótese em que pessoa jurídica de direito privado, juntamente com dois administradores, foi denunciada por crime ambiental, consubstanciado em causar poluição em leito de um rio, através de lançamento de resíduos, tais como, graxas, óleo, lodo, areia e produtos químicos, resultantes da atividade do estabelecimento comercial [...]. Relator: Min. Gilson Dipp. Brasília, 02 jun. 2005. Disponível em: <https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=200301073684&dt_publicacao=13/06/2005>. Acesso em: 15 nov. 2022.

BRASIL. Superior Tribunal de Justiça (5. Turma**)**. Recurso Especial. **Recurso Especial n. 989089/SC**. 1. Consoante entendimento do Superior Tribunal de Justiça, "Admite-se a responsabilidade penal da pessoa jurídica em crimes ambientais desde que haja a imputação simultânea do ente moral e da pessoa física que atua em seu nome ou em seu benefício, uma vez que não se pode compreender a responsabilização do ente moral dissociada da atuação de uma pessoa física, que age com elemento subjetivo próprio" (REsp 889.528/SC, Rel. Min. FELIX FISCHER, DJ 18/6/07) [...]. Relator: Min. Arnaldo Esteves Lima. Brasília, 18 ago. 2009. Disponível em: <https://processo.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=200702310357&dt_publicacao=28/09/2009>. Acesso em: 15 nov. 2022.

CASTELLS, Manuel. **A sociedade em rede**. 6 ed. São Paulo: Paz e Terra, 2002.

CONSELHO DA EUROPA. ETS nº 185. **Convenção sobre o Crime Cibernético.** Budapeste: 23 nov. 2001. Disponível em: <https://rm.coe.int/16802fa428>. Acesso em: 15 nov. 2022.

DEIBERT, Ronald *et al*. **Tracking GhostNet:** Investigating a Cyber Espionage Network. 2009. Information Warfare Monitor - Universidade de Toronto e The SecDev Group. Canadá, 2009. Disponível em: <https://citizenlab.ca/wp-content/uploads/2017/05/ghostnet.pdf>. Acesso em: 15 nov. 2022.

GLOBAL cybercrimes cost $114 billion annually – Symantec. **Reuters**, 2011. Disponível em: <https://www.reuters.com/article/oukin-uk-symantec-idUKTRE7861XQ20110907>. Acesso em: 17 nov. 2022.

MARCZAK, Bill *et al*. **Hooking Candiru**: Another Mercenary Spyware Vendor Comes into Focus. 2021. Relatório Citizen Lab n. 139 – Universidade de Toronto, Canadá, 2021. Disponível em: <https://tspace.library.utoronto.ca/bitstream/1807/123967/1/Report%23139--hooking-candiru.pdf>. Acesso em: 15 nov. 2022.

MARTÍN, Luis Gracia. Crítica de las modernas construcciones de una mal llamada responsabilidad penal de la persona jurídica. **Revista Electrónica de Ciencia Penal y Criminología**, n. 18, p. 1-95, 2016.

MIRIAN, Ariana. Hack for hire. **Communications Of The Acm**, v. 62, n. 12, p. 32-37, 21 nov. 2019. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/3359386>. Acesso em: 15 nov. 2022.

MUÑOZ**,** Afonso Galán. Ação, tipicidade e culpabilidade penal da pessoa jurídica em tempos de *compliance*: uma proposta interpretativa**. Revista de Direitos Fundamentais & Democracia**, Curitiba, v. 25, n. 3, p. 176-208, set./dez. 2020. Disponível em: <https://web.s.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=1&sid=d9bf8c83-7f5b-497e-8b5a-84906fce075c%40redis>. Acesso em: 16 nov. 2022.

NGUYEN, Michael. Cambridge Analytica – the true implications for the future of democracy. **Australian Institute of International Affairs,** 2018. Disponível em: <https://www.internationalaffairs.org.au/resource/cambridge-analytica-what-the-event-actually-illustrates-for-the-future-of-democracy/>. Acesso em 16 nov. 2022.

OLIVEIRA, Michele. Como a Alemanha cercou o Telegram e conseguiu banir contas por crime de ódio. **Folha de São Paulo**, 2022. Disponível em: <https://www1.folha.uol.com.br/mundo/2022/03/como-a-alemanha-cercou-o-telegram-e-conseguiu-banir-contas-por-crime-de-odio.shtml>. Acesso em: 16 nov. 2022.

PARLAMENTO EUROPEU. **Did the WikiLeaks incidents create more or less democracy in the world?** 2011. Disponível em: <https://www.europarl.europa.eu/news/en/headlines/society/20110131STO12842/did-the-wikileaks-incidents-create-more-or-less-democracy-in-the-world>. Acesso em 16 nov. 2022.

SANTOS, Ílison Dias dos; MELO, Jhonatas Péricles Oliveira de. A responsabilidade penal da pessoa jurídica: análise exploratória do modelo espanhol e do modelo proposto pelo projeto de novo código penal brasileiro. **Revista de Derecho Procesal de la Asociación Iberoamericanade la Universidad de Salamanca**, Salamanca, p. 121-137, 2017. Disponível em: <https://iudicium.usal.es/numeros/2/files/assets/basic-html/page-121.html>. Acesso em: 14 nov. 2022.

SANTOS, Juarez Cirino dos. A Responsabilidade Penal da Pessoa Jurídica. **Fórum Administrativo**: Direito Público, Belo Horizonte, v. 2, n. 17, jul. 2002.

SCHÜNEMANN, Bernd. O direito penal é a *ultima ratio* da proteção de bens jurídicos! – Sobre os limites invioláveis do direito penal em um Estado de Direito liberal. **Revista Brasileira de Ciências Criminais**: RBCCrim, v. 13, n. 53, p. 9-37, mar./abr. 2005.

SCOTT-RAILTON, John et al. **Dark Basin**: uncovering a massive hack-for-hire operation. 2020. Relatório Citizen Lab n. 128 – Universidade de Toronto, Canadá, 2020. Disponível em: <https://tspace.library.utoronto.ca/bitstream/1807/106038/1/Report%23128--dark-basin.pdf>. Acesso em: 15 nov. 2022.

SHECAIRA, Sérgio Salomão. Responsabilidade penal das pessoas jurídicas: uma perspectiva do direito brasileiro. **Revista dos Tribunais**, São Paulo, v. 101, n. 921, p. 281-294, jul. 2012.

TANGERINO, Davi de Paiva. Culpabilidade e responsabilidade penal da pessoa jurídica. **Revista logos ciencia y tecnología,** v. 3, n. 1, p. 186-202, dez. 2011. Disponível em: <https://dialnet.unirioja.es/descarga/articulo/4166920.pdf>. Acesso em: 15 nov. 2022.

TIEDEMANN, Klaus. Responsabilidad penal de las personas jurídicas. **Anuario de Derecho Penal**, Espanha, p. 97-126, 1997. Disponível em: https://perso.unifr.ch/derechopenal/assets/files/anuario/an_1996_07.pdf Acesso em: 15 nov. 2022.

UNITED STATES. District Court Northern District of California. Appeal. **Appeal n. 19-7123**. Apelante: Whatsapp Inc. e outros Apelado: NSO Group Technologies Limited e outros. Administrative Office Of The United States Courts. California, 2021. Disponível em: <https://cdn.ca9.uscourts.gov/datastore/opinions/2021/11/08/20-16408.pdf>. Acesso em: 15 nov. 2022

A ERA DIGITAL E A NECESSIDADE DE RECONHECIMENTO DE NOVOS BENS JURÍDICOS A SEREM PENALMENTE TUTELADOS

Rafael Vieira Lopes[1]

RESUMO

Este estudo demonstra que a evolução tecnológica do século XXI não consegue ser acompanhada pela legislação. A era digital trouxe novos bens que merecem receber a tutela do direito penal. Após breve estudo sobre a teoria do bem jurídico, demonstra-se que a inserção do artigo 154-A ao Código Penal, é ineficiente pois ainda não reconhece novos bens jurídicos a serem penalmente tutelados.

Palavras-chave: Bem jurídico. Crimes cibernéticos. Dados informáticos.

ABSTRACT

This study demonstrates that the technological evolution of the 21st century has outpaced legislation. The digital age has brought many advances that need to be acknowledged and protected by law. After a brief investigation of the theory of legal interest, the insertion of article 154-A into the Brazilian Penal Code is insufficient, as it doesn't recognize new technological interests that need to be preserved under criminal law.

Keywords: Legal interest. Cybercrimes. Computer data

1 INTRODUÇÃO

Desde o início dos tempos o ser humano vem aperfeiçoando suas tecnologias, adequando-as às suas necessidades para facilitar a execução das mais diversas tarefas.

[1] Graduado em Direito pelo CEUB (2018); Pós-Graduando em Direito Penal e Controle Social pelo CEUB. E-mail: rafaelvieiralopes@hotmail.com.

É possível ver grandes revoluções que remontam até 70 mil anos atrás, quando a humanidade se tornou capaz de se comunicar e transmitir ideias e pensamentos, na chamada Revolução Cognitiva. Ela foi sucedida pela Revolução Agrícola, quando o ser humano passou a dominar técnicas de plantio e de domesticação de animais. Já ao final do século XV, a humanidade experimentou a Revolução Científica, passando a entender as leis que regem o universo, inicialmente com publicações como a de Nicolau Copérnico, e perdurando até a atualidade com a rede mundial de computadores[2].

A evolução da ciência traz novas facilidades e soluções para o ser humano, cria novos desafios e novas demandas. Não é por outra razão que o direito é alvo de constante evolução para adequação à sociedade e período em que está inserido.

Nesse sentido, a sociedade possui "bens", que consiste em tudo aquilo que satisfaz a necessidade humana. Aqueles que são relevantes, mais importantes para a vida em sociedade, recebem a tutela do direito e passam a ser considerados bens jurídicos; dentre esses há aqueles de importância ainda mais relevante, que passam a ser tutelados por ramo específico do direito, o direito penal, promovendo-os a bens jurídicos penalmente tutelados.

É exatamente sobre os bens jurídicos penalmente tutelados que reside o presente estudo. Isso porque, com a evolução da ciência e da sociedade, surge o anseio pela tutela de novos bens jurídicos, antes inexistentes, ou ao menos desconhecidos.

Se no século passado, e início do presente, um dos bens mais preciosos para o mundo era o petróleo, a era digital, que veio para revolucionar a forma como vemos o mundo, transformou os dados como um dos bens mais importantes para o planeta.

Tanto é assim que as cinco empresas mais valiosas do mundo, atualmente, são gigantes da tecnologia: Alphabet, Amazon, Apple, Facebook e Microsoft, segundo matéria publicada na revista *The Economist*, em matéria intitulada

[2] BARROSO, Luís Roberto. **Sem data venia**: um olhar sobre o Brasil e o mundo. Rio de Janeiro: História Real, 2020. p. 79-80.

(traduzido do inglês): O recurso mais valioso do mundo não é mais o petróleo, mas sim os dados[3].

Aparentemente o legislador não consegue acompanhar a evolução exponencial da era digital, deixando de tutelar bens que devem receber não apenas a tutela do direito, mas a tutela do direito penal, por se tornarem cada vez mais relevantes ao mundo.

Este artigo, inicialmente, contextualizará o leitor acerca das teorias em torno do estudo bem jurídico penalmente tutelado.

Após, será feita uma análise crítica à legislação vigente no país, especialmente o artigo 154-A do Código Penal, com enfoque na demonstração do apego ao legislador por bens jurídicos "tradicionais", como a vida, saúde, patrimônio, etc., com consequente demonstração da necessidade de elevar os dados e sistemas informáticos à categoria de bens jurídicos penalmente tutelados, sob pena de existência de vácuos legislativos.

Por fim, serão feitas propostas de tipos penais a serem incluídos em nosso ordenamento jurídico, de acordo com conceitos doutrinários modernos, para suprimento do vácuo jurídico existente no direito penal cibernético.

2 BEM JURÍDICO PENALMENTE TUTELADO

Inicialmente, tinha-se a ideia de objeto do delito (bem jurídico) apenas um direito subjetivo natural da pessoa, que consistia nos meios necessários para preservá-la, tais como a liberdade, saúde, vida, integridade física, etc. Entretanto, essa ideia perdeu força dando espaço para que valores ético-culturais se tornassem bem jurídicos tutelados penalmente[4].

A definição do conceito de bem jurídico é alvo de constante discussão, e ainda há divergência na doutrina.

[3] THE world's most valuable resource is no longer oil, but data. **The Economist**, 2017. Disponível em: <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>. Acesso em 21 nov. 2022.

[4] FERRAJOLI, Luigi. **Direito e Razão:** Teoria do Garantismo. 4ª. ed. rev. São Paulo: Editora Revista dos Tribunais, 2014.

Segundo o autor Luís Greco, há uma distinção entre dois conceitos de bem jurídico, um sendo de uma perspectiva dogmática e outro de uma perspectiva político-criminal. Este último de maior interesse para o presente estudo, já que o primeiro se restringe à conclusão de que toda norma possui um bem jurídico que só pode ser identificado após a existência dela. A adoção dessa perspectiva significaria dizer que "só se pode dizer se algo é um bem jurídico se o legislador assim houver decidido"[5].

No que concerne à perspectiva político-criminal, somente deve receber o *status* de bem jurídico aquilo que tenha importância significativa para garantir o bem-estar ou a existência de alguém, seja esse alguém um indivíduo ou a própria coletividade[6]; e pode ser entendido como uma *realidade fática* (conceito material) ou uma *entidade meramente ideal*, onde o bem jurídico possui íntima relação com os valores[7].

Assim, para definição de um conceito de bem jurídico, resta definir como ele deve ser entendido, se como uma realidade fática ou meramente ideal. Adotar o segundo entendimento, é dar ao legislador carta branca, que poderá incriminar toda e qualquer conduta, bastando vinculá-la a um valor abstrato não verificável no mundo concreto.

Adotar o entendimento da realidade fática, também não significa vincular a existência do bem jurídico àquela realidade empírica, que pode ser observada, pois o mundo real não se esgota naquilo que as ciências naturais podem verificar. Exemplo disso é a honra como bem jurídico penalmente tutelado, que apesar de existente na nossa realidade, não pode ser constatada empiricamente.

Ademais, tendo em vista o caráter fragmentário do direito penal, parece ser mais prudente adotar conceitos capazes de restringir o poder punitivo estatal, devendo o bem jurídico servir como critério de limitação deste poder, mesmo

[5] GRECO, Luís. **Modernização do direito penal, bens jurídicos coletivos e crimes de perigo abstrato.** Rio de Janeiro: Lumen Juris, 2011. p. 77.

[6] A corrente dualista – majoritariamente aceita – reconhece os bens jurídicos em individuais e coletivos; são minoritárias a corrente monista-estatal, que defende que o bem jurídico é mero reflexo do interesse do Estado, e a monista-pessoal, que apenas reconhece os bens jurídicos relativos à coletividade quando se referir a indivíduos singulares.

[7] GRECO, Luís. **Modernização do direito penal, bens jurídicos coletivos e crimes de perigo abstrato.** Rio de Janeiro: Lumen Juris, 2011. p. 85-88.

porque, repita-se, a ideia de bem jurídico material não exclui a possibilidade de uma norma penal tutelar bens jurídicos imateriais (valores). Nas palavras de Luiz Regis Prado:

> O conceito material de bem jurídico reside na realidade ou experiência social, sobre a qual incidem juízos de valor, primeiro do constituinte, depois do legislador ordinário. Trata-se de um conceito necessariamente valorado e relativo, isto é, válido para determinado sistema social em um dado momento histórico-cultural[8].

Este ensinamento vai ao encontro do conceito trazido linhas acima. Isto é, deve receber a tutela do direito os bens que tiverem importância significativa para garantir o bem-estar ou a existência de alguém (indivíduo ou coletividade). Naturalmente o que é ou não bem jurídico sofrerá alterações de acordo com cada sociedade e momento histórico, é o que leciona Ferrajoli:

> Tampouco pode-se dizer que existem delitos castigados em todo tempo e lugar por se oporem à moralidade média, ao sentimento comum ou a critérios similares. Ao contrário, não existe conduta delituosa que não tenha sido permitida em outros tempos, nem conduta lícita que não tenha sido, outrora, proibida[9].

Por fim, para perfeita compreensão do estudo proposto no presente artigo, resta descontruir o que o senso comum pode nos levar a crer.

É possível entender que uma vez positivado, o bem jurídico se resume a um direito do indivíduo (ou coletividade), todavia, esse entendimento é, no mínimo, incompleto. Além de consistir em um direito do indivíduo, o bem jurídico consiste na possibilidade de o titular dispor dele da forma que bem entender[10].

Assim, a lesão a um bem jurídico não consiste apenas na violação de um direito em si, mas também no impedimento da disposição deste direito por seu titular da forma que melhor lhe convier. Para melhor compreensão, analisemos o caso do homicídio.

---

[8] PRADO, Luiz Regis. **Curso de direito penal brasileiro.** 13ª ed. rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2014. p. 114

[9] FERRAJOLI, Luigi. **Direito e Razão:** Teoria do Garantismo. 4ª. ed. rev. São Paulo: Editora Revista dos Tribunais, 2014. p. 429-430

[10] ZAFFARONI, Eugenio Raúl; PIERANGELI, José Henrique. **Manual de Direito Penal Brasileiro:** Parte Geral. 10ª ed. rev. atual. São Paulo: Revista dos Tribunais, 2013. p. 416.

Neste crime diz-se que o bem jurídico tutelado é a vida, o que não passa de mera abreviação. O bem jurídico nesse caso é o direito de dispor de sua vida; a partir do momento que alguém mata outra pessoa, o homicida impediu que o titular do direito pudesse dispor dele. É por isso que a tentativa de suicídio não é punida, já que o indivíduo pode dispor do seu direito à vida como bem entender.

3 A NECESSIDADE DE ELEVAÇÃO DOS DADOS INFORMÁTICOS AO *STATUS* DE BEM JURÍDICO PENALMENTE TUTELADO

A evolução tecnológica dos últimos tempos, especialmente do século XXI, trouxe o mundo digital ao cotidiano da sociedade. Atualmente as pessoas possuem um computador à palma da sua mão (*smartphones*), que por sua vez está conectado ao mundo inteiro por meio da *internet*.

Não para por aí, a digitalização vem afetando sobremaneira a vida das pessoas, seja com a criação de *gadgets*, tais como relógios, pulseiras, fones de ouvido inteligentes; seja com a *internet* das coisas transformando uma geladeira, ar condicionado, televisão, etc., em dispositivos autônomos, capazes de aprender a rotina do usuário para prever necessidades e oferecer soluções mesmo sem comando prévio.

A velocidade de evolução da tecnologia nos dias atuais é assustadora. Atualmente é possível, por exemplo, o seguinte cenário: ao sair do seu local de trabalho, um dos dispositivos do indivíduo (*smartphone*, relógio, etc.) identifica a saída, seja por meio de geolocalização ou pelo simples fato de perder conexão com a rede de *internet* daquele local, sugere a requisição de um carro por aplicativo para levá-lo até a sua casa, inclusive estimando tempo de trajeto com base em dados colhidos de outros usuários. O usuário, com apenas um clique, confirma a solicitação do veículo autônomo, que chega e o leva até o destino final.

Veja que o cenário acima proposto exige única e exclusivamente uma intervenção humana, o clique para confirmar a solicitação do veículo (que já opera até mesmo sem um motorista). Todas as outras soluções para as necessidades do usuário foram sugeridas e concluídas por inteligência artificial, o que se torna

possível não apenas pela conexão dos aparelhos à rede mundial, mas sim pelos dados armazenados em cada um dos sistemas.

Utilizemos o mesmo cenário acima, mas agora, um criminoso de posse dos dados armazenados, utiliza-os para interceptar o indivíduo que apenas queria chegar na sua casa. Ou mesmo que, por meio da infecção de sistemas ou aparelhos com códigos maliciosos, solicite o veículo não para a residência do indivíduo, mas sim para um local que será utilizado para o cometimento de um crime. Neste cenário podemos perceber a importância dos dados informáticos.

Muitas vezes não percebemos, mas os dados informáticos estão mais presentes em nossas vidas do que imaginamos. Eles vêm ganhando cada vez mais relevância na nossa sociedade, podendo ser utilizados para agregar na vida do indivíduo, mas também podem ser utilizados com intenções espúrias. Sobre a íntima relação atual da sociedade com a informática bem descreveu Spencer Toth Sydow:

> A informática e seus deslindes afetam de maneira uniforme toda a sociedade global, uma vez que a tecnologia mostra-se imprescindível para o evoluir humano. Exceção feita a segmentos cada dia mais diminutos que a informática não atinge, todos estamos permeados pelos conceitos da tecnologia, que apresenta suas vantagens inquestionáveis. Direta ou indiretamente, todos estão vinculados às máquinas, e a violação deste segmento cria dificuldade sobremaneira ao desenvolvimento[11].

É por essa razão que o questionamento acerca da necessidade de intervenção estatal no ambiente informático vem tomando força no mundo. Na Convenção de Budapeste, realizada no Conselho da Europa, firmou-se tratado com a finalidade de combater especificamente os crimes eletrônicos. O tratado foi firmado em 2001 por países da União Europeia, mas já conta com ratificação de países como Austrália, Japão e Estados Unidos[12].

Por meio de nota técnica enviada ao Ministério das Relações Exteriores em 2018, o Ministério Público Federal defendeu a adesão do Brasil à convenção, o que

[11] Sydow, Spencer Toth. **Crimes informáticos e suas vítimas**. 2ª Edição. São Paulo: Editora Saraiva, 2015. p. 31.
[12] BERTHOLDI, Juliana. **Crimes cibernéticos**. 1ª edição. Curitiba: Contentus, 2020. p. 33.

ocorreu somente em 2021, por meio do Decreto Legislativo nº 37, de 2021[13]. Todavia, o nosso ordenamento indica singela adequação ao tratado aderido, já que diversos crimes cibernéticos lá previstos permanecem sem qualquer previsão legal.

Como já dito, o bem jurídico está ligado à ideia de valores necessários ao desenvolvimento e coexistência pacífica dos cidadãos. Serve, pois, como verdadeiro garantidor da ordem social. Nesta linha, Francisco de Assis Toledo aponta que: "bens jurídicos são valores ético-sociais que o direito seleciona, com o objetivo de assegurar a paz social, e coloca sob sua proteção para que não sejam expostos a perigo de ataque ou a lesões efetivas"[14].

É evidente a importância da *internet* e das tecnologias na vida em sociedade atualmente. A evolução do ser humano hoje depende da evolução da tecnologia, que afeta a sociedade global sem distinção, mesmo que indiretamente. Na linha do que leciona Sydow, mesmo que não estejamos próximos a rios e florestas, a sociedade e o Estado entendem que a sua preservação é essencial ao ser humano[15].

O mesmo deve ocorrer com o novo mundo tecnológico, o que somente será possível com o reconhecimento de novos bens jurídicos, tais como os sistemas e dados informáticos, cujas definições trazidas na Convenção de Budapeste se mostram bastante eficientes:

> "Sistema informático" significa qualquer dispositivo isolado ou grupo de dispositivos relacionados ou interligados, em que um ou mais de entre eles, desenvolve, em execução de um programa, o tratamento automatizado de dados.
>
> "Dados informáticos" significa qualquer representação de factos, de informações ou de conceitos sob uma forma susceptível de processamento num sistema de computadores, incluindo um programa, apto a fazer um sistema informático executar uma função[16].

[13] BRASIL. **Decreto Legislativo n. 37, de 2021**. Aprova o texto da Convenção sobre o Crime Cibernético, celebrada em Budapeste, em 23 de novembro de 2001. Disponível em: <https://legis.senado.leg.br/norma/35289207/publicacao/35300588>. Acesso em: 22 nov. 2022.

[14] TOLEDO, Francisco de Assis. **Princípios Básicos de Direito Penal**. 5ª edição. São Paulo: Saraiva. 1994. p. 16.

[15] Sydow, Spencer Toth. **Crimes informáticos e suas vítimas**. 2ª Edição. São Paulo: Editora Saraiva, 2015. p. 31.

[16] CONSELHO DA EUROPA. ETS nº 185. **Convenção sobre o Crime Cibernético.** Budapeste: 23 nov. 2001. Disponível em: <https://rm.coe.int/16802fa428>. Acesso em: 15 nov. 2022. p. 3.

O nosso ordenamento jurídico caminha a passos lentos, estando apegado ao momento histórico-cultural do século passado, onde apenas recebem a tutela do direito penal os bens jurídicos tidos como tradicionais. Embora necessário, parece que o legislador ainda não conseguiu compreender sistemas e dados informáticos como bens jurídicos por si sós, apenas prevendo circunstâncias agravantes ou majorantes para crimes cibernéticos impróprios[17].

A maior evolução experimentada no Brasil no que tange aos crimes informáticos reside na Lei nº 12.737/2012, proposta com o objetivo de tipificar criminalmente delitos informáticos, acrescentando ao Código Penal o artigo 154-A, além de fazer outras singelas alterações. Todavia a tentativa foi um fracasso, pois, como dito, o legislador parece não reconhecer dados e sistemas informáticos como bens jurídicos a serem tutelados, tutelando apenas condutas que geram repercussão no mundo real.

Os crimes cibernéticos podem ser próprios[18] ou impróprios. Nesse último, por mais que o delinquente se utilize de técnicas ou ferramentas digitais, seus efeitos repercutem no mundo real, fora do ambiente digital. Dessa forma, o bem jurídico lesionado acaba não sendo a informática ou os dados em si, facilitando ao legislador a sua tipificação. Em razão dessa facilidade, a nossa legislação tipifica, em sua maioria, crimes cibernéticos impróprios[19].

Quando há tentativa de tutela da informação cibernética o legislador falha, pois parece não compreender o mundo digital em si, para que possa tipificar uma conduta de forma adequada. O artigo 154-A do Código Penal, acrescido pela lei acima mencionada, tipifica a invasão de dispositivo informático e sua redação original assim previa:

> 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

[17] São crimes geram repercussão na vida real, sendo o ambiente digital mera ferramenta (meio) para a prática delituosa.
[18] A prática e a consumação do crime ocorrem dentro do meio digital, atingindo um sistema informático em si.
[19] BERTHOLDI, Juliana. **Crimes cibernéticos**. 1ª edição. Curitiba: Contentus, 2020. p. 25.

> tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita[20].

Veja que o tipo penal é precário. Num primeiro momento exige que o acesso a dispositivo informático de outrem se dê mediante violação indevida de mecanismo de segurança, deixando de tutelar situação em que o dispositivo da vítima não detém qualquer tipo de mecanismo de segurança, ou mesmo situações em que se dê acesso limitado ao delinquente. Ademais, o que o bem jurídico tutelado não é os dados informáticos em si, mas sim a privacidade[21].

O maior problema reside, entretanto, na opção do legislador em incluir elemento subjetivo específico ao tipo penal, ao exigir que a conduta deva possuir a finalidade de obter, adulterar ou destruir dados e informações, ou instalar vulnerabilidades para obter vantagem ilícita.

Veja que se o delinquente invade dispositivo informático, mesmo com a violação de mecanismo de segurança, e instala vulnerabilidade nele, todavia, as vulnerabilidades não são utilizadas com a finalidade de obter vantagem ilícita, não há que se falar em conduta criminosa. O mesmo ocorre se o sujeito invade dispositivo informático, tem acesso aos dados constantes nele, mas não os obtém para si, adultera ou não os destrói.

Percebeu-se que modo de atuação dos delinquentes, diversas vezes viola sistemas se aproveitando de falhas lógicas de programação (*bugs*), ou com o uso de engenharia social, que consiste na indução de vítimas a introduzirem códigos maliciosos em seus sistemas, que uma vez instalados permitem livre acesso sem a necessidade de qualquer violação de sistema de segurança[22]. Por isso o dispositivo

[20] 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: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 22 nov. 2022

[21] CAVALCANTE, Márcio André Lopes. Primeiros comentários à Lei 12.737/2012, que tipifica a invasão de dispositivo informático. **Dizer o Direito**, 2023. Disponível em: <https://www.dizerodireito.com.br/2012/12/primeiros-comentarios-lei-127372012-que.html>. Acesso em: 22 nov. 2022.

[22] Sydow, Spencer Toth. **Crimes informáticos e suas vítimas**. 2ª edição. São Paulo: Editora Saraiva, 2015. p. 42.

sofreu alteração por meio da Lei nº 14.155/2021, onde foi suprimida a expressão "mediante violação indevida de mecanismo de segurança"[23].

Ocorre que, na prática, a alteração legislativa não gerou qualquer repercussão (ou não deveria gerar). Isso porque ao manter o núcleo do tipo penal o verbo "invadir", necessariamente o indivíduo deve fazer o uso de força, romper algum obstáculo[24], o que se traduz na violação de mecanismo de segurança quando estamos no contexto do mundo informático.

A ideia ganha força quando analisamos as palavras utilizadas pelo legislador ao tipificar a violação de domicílio, que assim prevê

> Art. 150 - Entrar ou permanecer, clandestina ou astuciosamente, ou contra a vontade expressa ou tácita de quem de direito, em casa alheia ou em suas dependências:
>
> Pena - detenção, de um a três meses, ou multa[25].

Neste dispositivo o legislador foi cirúrgico ao utilizar como núcleo do tipo penal "entrar" ou "permanecer", afastando a necessidade de qualquer tipo de uso de força ou rompimento de obstáculo, incriminando a simples conduta de estar dentro da residência contra a vontade do proprietário da casa (ou de quem de direito).

Isso ocorre pelo fato de a propriedade privada ser um bem jurídico já reconhecido pelo legislador. Assim, o vácuo legislativo no que diz respeito ao mundo digital somente será suprido quando do efetivo reconhecimento e compreensão dos bens que o envolvem, com a respectiva tutela do Estado.

Esses são apenas alguns dos problemas identificados na tutela dos crimes cibernéticos no nosso ordenamento jurídico. Não se mostra salutar apontar um a um

[23] BRASIL. **Lei nº 14.155, de 27 de maio de 2021**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Disponível em: <https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Lei/L14155.htm>. Acesso em: 23 nov. 2022.

[24] A primeira definição trazida pelo dicionário Michaeles do termo invadir é: Entrar pela força; penetrar hostilmente em determinado lugar; apoderar-se, conquistar, tomar. Disponível em: <https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/invadir>. Acesso em 22 nov. 2022.

[25] BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 23 nov. 2022.

dos *déficits* identificáveis e suas consequências[26], cuja análise é bastante extensa e desnecessária ao presente estudo. O ponto nevrálgico aqui é demonstrar ao leitor a importância de uma atualização legislativa efetiva que reconheça novos bens jurídicos ainda não tutelados.

4 DELITOS EM ESPÉCIE E O NOSSO ORDENAMENTO

Ainda sobre a problemática trazida envolvendo o *caput* do artigo 154-A do Código Penal, a solução é sobremaneira simples. O legislador já conhece a técnica necessária para tutelar o bem jurídico que pretendia, pois dela já utilizou quando da tipificação do crime de violação de domicílio.

Tamanha a simplicidade da solução que, neste ponto, muito possivelmente o leitor já saiba a resposta da questão colocada. Deveria o legislador substituir o núcleo do tipo penal "invadir" por "entrar, ingressar, acessar" ou qualquer outra palavra disponível na língua portuguesa que não traga consigo a exigência do uso de força ou rompimento de obstáculo.

Isso não quer dizer que a invasão propriamente dita tornar-se-ia conduta atípica, já que a invasão engloba o ingresso não forçado. Nada obstante, evidente que o rompimento de obstáculo ou uso de força é dotado de reprovabilidade superior ao simples ingresso, razão pela qual cabe ao legislador prever pena maior para este tipo de conduta, seja por meio de causa de aumento de pena ou por qualificação do delito.

Mais uma vez o legislador conhece da técnica, mas não consegue visualizar a sua aplicação nos crimes cibernéticos. O crime de furto, por exemplo, se qualifica pela: i) destruição ou rompimento de obstáculo; ii) com abuso de confiança, ou mediante fraude ou destreza[27].

---

[26] Muitas condutas não tipificadas no nosso ordenamento jurídico são tidas, pelo senso comum, como desviadas, injustas, criminosas. A falta de uma tutela específica gera sensação de insegurança e ausência de regras no ambiente virtual, que por sua vez repercutem em diversas esferas sociais, seja na esfera judiciária com a aplicação indevida de analogia para satisfação do sentimento de resposta estatal, seja na própria estrutura da sociedade, com o abalo de regimes de governo, fenômeno global que está colocando em xeque a democracia, que se julgava consolidada, de diversos países.

[27] Artigo 155, §4º, incisos I e II, do Código Penal.
BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 23 nov. 2022.

A simples mudança proposta solucionaria diversas situações que atualmente encontram-se em limbo e, por isso, sujeitas a julgamentos equivocados com aplicação de analogia *in malam partem*[28].

Não apenas a doutrina, mas a própria convenção de Budapeste à qual o Brasil aderiu, traz sugestões de condutas que devem ser tipificadas, sendo que parte delas já são tuteladas, mas devem estar inseridas no contexto de invasão, dentre as quais destacam-se duas, o *dano informático* e a *inserção de código malicioso*.

O *dano informático* consiste na danificação, destruição, deterioração, alteração ou eliminação de dados informáticos. Esta conduta dissociada do contexto de invasão não se subsome ao texto contido no artigo 154-A do Código Penal. Majoritariamente a doutrina entende que a conduta se amoldaria ao crime de dano comum, capitulada no artigo 163 do Código Penal[29].

Ainda assim persiste o vácuo legal, pois a conduta capitulada no artigo 163 do Código Penal exige que o agente atue com dolo de danificar coisa alheia. Dessa forma, caso o dano aos dados informáticos se dê de forma culposa e/ou fora do contexto de invasão, a conduta será atípica.

Para melhor compreensão da problemática, imagine que um agente, sem autorização do proprietário de determinado sistema informático, ingresse nele por meio de engenharia social e passe a ter acesso a todos os dados e, culposamente, exclui todo o banco de dados existente no sistema. Sua conduta será atípica.

A alteração legislativa sugerida linhas acima, acrescentando o dano aos dados informáticos como qualificadora, supriria o vácuo jurídico. Nesta hipótese estaríamos diante de uma conduta preterdolosa, onde há dolo na primeira conduta (ingresso não autorizado), mas culpa no resultado (dano), todavia ambas recebendo a reprimenda adequada.

[28] A analogia, diferentemente da interpretação analógica, não constitui técnica de interpretação, mas sim meio de integração de lacunas legislativas, absolutamente vedada no nosso ordenamento quando feita em prejuízo do réu (*in malan partem*), sob pena de ofensa ao princípio da reserva legal insculpido no artigo 1º do Código Penal. Permitida a integração normativa, contudo, quando utilizada em benefício do acusado.

[29] BERTHOLDI, Juliana. **Crimes cibernéticos**. 1ª edição. Curitiba: Contentus, 2020. p. 25.

Se analisarmos o exemplo anterior, a partir do momento que o agente ingressa no sistema informático sem autorização, o crime já estaria consumado. E se a sua conduta resultasse em dano aos dados, dolosa ou culposamente, a reprimenda seria maior.

Nunca é demais repetir, o legislador já conhece a técnica adequada, porém não consegue aplicá-la aos crimes informáticos. Essa afirmação se dá com base no artigo 129, *caput* e §§ 1º e 2º, do Código Penal, onde o dolo reside na lesão corporal e a culpa nos resultados trazidos, punindo cada conduta de forma adequada.

Já a *inserção de código malicioso* consiste na inserção de programas capazes de enviar comandos ao sistema, que implicam em prejuízo da confidencialidade de dados, perda de disponibilidade ou redução de velocidade, ou mesmo a integridade dos dados[30]. Em síntese, são programas que modificam alteram ou destroem dados de dispositivos alheios.

Importante esclarecer que, em que pese a similaridade com o tipo penal acima trazido (dano informático), as condutas são distintas. Aqui a conduta consiste na inserção de códigos maliciosos capazes de causar prejuízo, não exigindo a produção de qualquer resultado naturalístico, é um crime formal. Já aquela conduta exige, necessariamente, a produção do resultado dano, portanto, é um crime material.

No nosso ordenamento a *inserção de código malicioso* se dissociada do contexto de invasão, ou se inexistente a produção de qualquer resultado naturalístico, é conduta atípica. Diferentemente do que ocorre no restante do mundo, onde países como Japão, Alemanha e Itália já preveem norma específica para incriminar a conduta[31].

Por fim, há de se analisar o "*furto" de identidade virtual*, que, segundo Sydow "é a apropriação das características e identificações pessoais de outrem para

[30] Sydow, Spencer Toth. **Crimes informáticos e suas vítimas**. 2ª Edição. São Paulo: Editora Saraiva, 2015. p. 42.
[31] Sydow, Spencer Toth. **Crimes informáticos e suas vítimas**. 2ª Edição. São Paulo: Editora Saraiva, 2015. p. 44-45.

fazer-se passar por este, sem que, contudo, tenha recebido autorização para tanto"[32], além de esclarecer o que é a identidade virtual:

> O uso da rede gera preferências, gera um histórico de locais mais visitados, cria interface personalizada, habitualidade na comunicação com amigos ou conhecidos pelo meio virtual etc. Por isso, é possível dizer que uma pessoa tem uma identidade própria no ciberespaço, a partir de seu acesso, e que essa identidade social pode ser de grande valia para sua profissão e seus relacionamentos. A identidade virtual, então, termina por ser pessoal, mas trata de um conceito de alguém frente a seus núcleos de interesse[33].

A conduta não encontra tipificação em nossa legislação. Em que pese a conduta receber a denominação de "furto", a nomenclatura não parece ser a mais adequada, já que dados informáticos não são passíveis de serem furtados, ao menos não pelo texto atual previsto no artigo 155 do Código Penal.

Isso se dá porque o crime de furto previsto no nosso código possui como núcleo o verbo "subtrair", de modo que a consumação somente se dará quando o bem jurídico (coisa alheia móvel) é retirado da esfera da posse e disponibilidade da vítima, ingressando na livre disponibilidade do agente, de forma mansa, tranquila e desvigiada. É similar ao entendimento que se aplica ao crime de roubo, sumulado pelo Superior Tribunal de Justiça[34], que dispensa a posse mansa, tranquila e desvigiada.

Com efeito, a identidade virtual é constituída por dados informáticos, que por sua vez são compostos por *bits* (meras representações de linguagens interpretadas pelo sistema), sendo impassíveis de serem subtraídos, mas tão somente replicados[35].

Assim, embora o agente possa deter a posse da coisa alheia móvel (dados informáticos), tratam-se de dados duplicados. Não houve a subtração da vítima ou a inversão de posse.

---

[32] Sydow, Spencer Toth. **Crimes informáticos e suas vítimas**. 2ª Edição. São Paulo: Editora Saraiva, 2015. p. 43

[33] Sydow, Spencer Toth. **Crimes informáticos e suas vítimas**. 2ª Edição. São Paulo: Editora Saraiva, 2015. p. 43

[34] Súmula nº 582: Consuma-se o crime de roubo com a inversão da posse do bem mediante emprego de violência ou grave ameaça, ainda que por breve tempo e em seguida à perseguição imediata ao agente e recuperação da coisa roubada, sendo prescindível a posse mansa e pacífica ou desvigiada.

[35] Sydow, Spencer Toth. **Crimes informáticos e suas vítimas**. 2ª Edição. São Paulo: Editora Saraiva, 2015. p. 43

No bojo dos autos do processo 0291040-55.2012.8.21.7000, que tramitou perante o Tribunal de Justiça do Rio Grande do Sul, discutiu-se a possibilidade de furto de dados informáticos. Naquela oportunidade, uma coordenadora de recursos humanos de determinada empresa tinha acesso a diversos arquivos sensíveis.

Surgiu oportunidade à funcionária em outra empresa, razão pela qual solicitou o seu desligamento. Todavia, no seu penúltimo dia de trabalho, com o uso de dispositivo compatível com a entrada USB, copiou os arquivos aos quais tinha acesso sem autorização. Por essa razão o Ministério Público gaúcho a denunciou pela suposta prática do crime capitulado no artigo 155, §4º, inciso II, do Código Penal (furto qualificado pelo abuso de confiança).

Em primeira instância foi condenada. Todavia, ao julgar o recurso de apelação interposto pela defesa, o tribunal reformou a sentença, absolvendo a acusada por atipicidade da conduta imputada, já que ela não teria subtraído os dados informáticos, mas sim os copiado. A conduta, pois, não se amolda ao tipo imputado, conforme constou no acórdão: "a denunciada tão somente copiou dados e arquivos informáticos para si, em momento algum vindo a tirá-los da esfera de disponibilidade da ofendida"[36].

Veja que nesse caso também não há que se falar em cometimento da conduta prevista no artigo 154-A do Código Penal, mesmo que consideremos a reforma legislativa de 2021, já que a funcionária não invadiu nenhum sistema, mas apenas o acessou e copiou os dados que lhe eram acessíveis, sem uso de força ou rompimento de obstáculo.

Com a análise do caso encerra-se no presente estudo, sendo certo que a doutrina já prevê diversos outros crimes cibernéticos tipificados ou não no nosso ordenamento, mas a análise de todos merece estudo dedicado exclusivamente ao tema, não cabendo fazê-lo aqui.

[36] BRASIL. Tribunal de Justiça do Rio Grande do Sul (7. Câmara Criminal). Apelação. **APC nº 70049844483**. Tanto a narrativa contida na denúncia como os substratos probatórios colacionados aos autos revelam que a ré copiou, para si, possivelmente infringindo contrato firmado perante sua empregadora, arquivos e documentos informáticos gravados em disco rígido de computador - conduta atípica e que não se subsume àquela abstratamente prevista no artigo 155 do CP [...]. Relatora: Des. Naele Ochoa Piazzeta. Porto Alegre, 29 abril 2014. Disponível em: <https://www.tjrs.jus.br/buscas/jurisprudencia/exibe_html.php>. Acesso em: 04 mar. 2023.

Aqui, suficientes as análises já feitas, que permitem ao leitor a compreensão da existência de um vácuo legislativo no nosso ordenamento, que decorre da falta de compreensão do legislador da existência de bens jurídicos trazidos com a revolução digital, especialmente os dados e sistemas informáticos.

5 CONCLUSÃO

O ser humano está em constante evolução e, com isso, novas necessidades vão surgindo ao longo do tempo. Disso decorre a necessidade de evolução legislativa para tutela dos valores importantes à existência e coexistência da sociedade no momento histórico cultural que se encontrar, necessidades essas que, no direito penal, se traduzem na tutela dos bens jurídicos.

Recentemente, especialmente no século XXI, a sociedade vem experimentando uma evolução tecnológica exponencial, gerando impactos jamais vistos na história da humanidade. O legislador não é capaz, ao menos por ora, de acompanhar a velocidade da evolução tecnológica, deixando situações no ambiente virtual em absoluto vácuo legislativo.

O nosso país avançou na legislação para tutela do mundo digital, especialmente com a edição da Lei nº 12.737/2012 e com a aderência ao tratado firmado na Convenção de Budapeste. Entretanto o avanço não é de todo expressivo se comparados a ordenamentos jurídicos mundo afora, que possuem legislação bem mais avançada sobre o tema.

O legislador parece ainda estar apegado aos bens jurídicos "tradicionais", razão pela qual diversas condutas que não repercutem no mundo real acabam por se tornarem condutas atípicas, em que pese o senso comum as tenha como condutas injustas e criminosas. Em razão desse sentimento, a sociedade anseia por resposta estatal, de modo que os julgadores, inconscientemente, para atender aos anseios populares, acabam por realizar analogia *in malam partem*.

Somente quando o legislador passar a reconhecer os novos bens jurídicos existentes, como dados e sistemas informáticos, é que nosso ordenamento será capaz de proteger os valores que a sociedade digital julga dignos da tutela do direito criminal.

Por ora, resta aos operadores do direito a vigilância constante para evitar abusos e desrespeitos a direitos e garantias fundamentais, bem como conscientizar o legislador da importância de reconhecer os novos bens jurídicos trazidos pela era digital.

REFERÊNCIAS

BARROSO, Luís Roberto. **Sem data venia**: um olhar sobre o Brasil e o mundo. Rio de Janeiro: História Real, 2020.

BERTHOLDI, Juliana. **Crimes cibernéticos**. 1ª edição. Curitiba: Contentus, 2020.

BRASIL. Tribunal de Justiça do Rio Grande do Sul (7. Câmara Criminal). Apelação. **APC nº 70049844483**. Tanto a narrativa contida na denúncia como os substratos probatórios colacionados aos autos revelam que a ré copiou, para si, possivelmente infringindo contrato firmado perante sua empregadora, arquivos e documentos informáticos gravados em disco rígido de computador - conduta atípica e que não se subsume àquela abstratamente prevista no artigo 155 do CP [...]. Relatora: Des. Naele Ochoa Piazzeta. Porto Alegre, 29 abril 2014. Disponível em: <https://www.tjrs.jus.br/buscas/jurisprudencia/exibe_html.php>. Acesso em: 04 mar. 2023.

BRASIL. **Decreto Legislativo n. 37, de 2021**. Aprova o texto da Convenção sobre o Crime Cibernético, celebrada em Budapeste, em 23 de novembro de 2001. Disponível em: <https://legis.senado.leg.br/norma/35289207/publicacao/35300588>. Acesso em: 22 nov. 2022.

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 23 nov. 2022.

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: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 22 nov. 2022.

BRASIL. **Lei nº 14.155, de 27 de maio de 2021**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Disponível em: <https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Lei/L14155.htm>. Acesso em: 23 nov. 2022.

CAVALCANTE, Márcio André Lopes. Primeiros comentários à Lei 12.737/2012, que tipifica a invasão de dispositivo informático. **Dizer o Direito**, 2023. Disponível em: <https://www.dizerodireito.com.br/2012/12/primeiros-comentarios-lei-127372012-que.html>. Acesso em: 22 nov. 2022.

FERRAJOLI, Luigi. **Direito e Razão:** Teoria do Garantismo. 4ª. ed. rev. São Paulo: Editora Revista dos Tribunais, 2014.

GRECO, Luís. **Modernização do direito penal, bens jurídicos coletivos e crimes de perigo abstrato.** Rio de Janeiro: Lumen Juris, 2011.

Michaelis: **Dicionário Brasileiro da Língua Portuguesa**. Editora Melhoramentos. 2022. Disponível em: <https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/invadir>. Acesso em: 22 nov. 2022.

PRADO, Luiz Regis. **Curso de direito penal brasileiro**. 13ª ed. rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2014.

Sydow, Spencer Toth. **Crimes informáticos e suas vítimas.** 2ª edição. São Paulo: Editora Saraiva, 2015.

THE world's most valuable resource is no longer oil, but data. **The Economist**, 2017. Disponível em: <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>. Acesso em 21 nov. 2022.

TOLEDO, Francisco de Assis. **Princípios Básicos de Direito Penal.** 5ª edição. São Paulo: Saraiva. 1994.

ZAFFARONI, Eugenio Raúl; PIERANGELI, José Henrique. **Manual de Direito Penal Brasileiro:** Parte Geral. 10ª ed. rev. atual. São Paulo: Revista dos Tribunais, 2013.