

NOVOS HORIZONTES NA RESPONSABILIDADE PENAL DAS PESSOAS JURÍDICAS PELA PRÁTICA DE CRIMES CIBERNÉTICOS

NEW HORIZONS ON CRIMINAL LIABILITY OF LEGAL ENTITIES ON CYBERCRIMES

Rafael de Oliveira Costa

Professor Visitante na Universidade da Califórnia-Berkeley. Doutor e Mestre em Direito pela Faculdade de Direito da UFMG. Promotor de Justiça no Estado de São Paulo. Professor na Escola Superior do Ministério Público, na Universidade Anhanguera e em cursos preparatórios para concursos.

Bruno Starcke Buzetti

Mestrando em Ciências Jurídicas ("Master of Science in Legal Studies") pela Ambra University (Orlando/FL, EUA). Especialista em Direito Público pelo Centro Universitário Leonardo da Vinci (Indaial/SC, Brasil). Pós-Graduado em Direito Penal e Processual Penal pela Universidade Gama Filho - UGF (Rio de Janeiro/RJ, Brasil). Analista Jurídico do Ministério Público do Estado de São Paulo.

RESUMO

A partir do aumento de incidência de crimes cibernéticos, os aplicadores do direito passaram a se questionar acerca da adequada regulamentação legal da matéria. Isso resultou numa forte guinada para a análise da responsabilidade penal da pessoa jurídica. Nesse contexto, o presente trabalho tem como objetivo apresentar propostas para que o Brasil seja capaz de cumprir o compromisso assumido, interna e internacionalmente, de assegurar que as pessoas jurídicas sejam responsabilizadas penalmente pela prática de crimes cibernéticos, atentando para os requisitos de criminalização, as penas cabíveis, as medidas cautelares e o ressarcimento das vítimas. Ao final, a pesquisa conclui pela necessidade de fixação de um novo marco legal sobre os crimes cibernéticos.

Palavras-chave: Crimes Cibernéticos; Responsabilidade Penal da Pessoa Jurídica; Convenção de Budapeste sobre o Crime Cibernético.

ABSTRACT

In light of the rising incidence of cybercrimes, legal scholars have begun to question the adequacy of current legal frameworks. This has led to a significant shift towards analyzing the criminal liability of legal entities. In this context, this study aims to present

proposals for Brazil to fulfill its internal and international commitments to ensure that legal entities are held criminally liable for cybercrimes. The study focuses on the requirements for criminalization, penalties, preventive measures, and victim compensation. Ultimately, the research concludes that a new legal framework for cybercrimes is necessary.

Keywords: Cybercrimes; Criminal Liability of Legal Entities; Budapest Convention on Cybercrime.

1. INTRODUÇÃO

De acordo com o *Internet Crime Report 2021* do FBI (*Federal Bureau of Investigation*), no ano de 2021, os Estados Unidos da América passaram por um aumento sem precedentes de ataques cibernéticos e atividade cibernética maliciosa. Apenas naquele ano, o *Internet Crime Center* (IC3) do FBI recebeu 847.376 reclamações, o que representa um aumento de 7%, em relação ao ano anterior, com potenciais perdas excedendo a quantia de 6,9 bilhões de dólares (USA, 2021, p. 3). No ano seguinte, houve ainda um acréscimo substancial nesse número, ultrapassando a valor de 10,2 bilhões de dólares – *vide Internet Crime Report 2022*. (USA, 2022, p. 3)

Dentre os incidentes mais reportados estão: *ransomware* (um tipo de *software* malicioso projetado para bloquear o acesso a um sistema de computador até que um “resgate” em dinheiro - normalmente em criptomoedas - seja pago), *business e-mail compromise schemes* (golpes visando empresas que trabalham com fornecedores e/ou empresas estrangeiras que realizam regularmente pagamentos por transferência eletrônica), o uso criminoso de criptoativos (*bitcoin, litecoin, potcoin, etc.*), além das famigeradas práticas conhecidas como *phishing/vishing/smishing/pharming* (uso de e-mail não solicitado, mensagens de texto, chamadas telefônicas e *sites* falsos, supostamente de uma empresa legítima, solicitando dados pessoais, financeiros ou de *login*, para aplicação de golpes) (USA, 2021, p. 8). Isso sem falar no aumento substancial da prática de crimes comuns, como extorsão, estelionato, calúnia, difamação, injúria e racismo, em ambiente cibernético (USA, 2022, p. 11-16).

O Brasil está entre os nove países com mais vítimas de cibercrimes reportados no mundo, no ano de 2022, são eles: 1º. Estado Unidos da América (479.181 vítimas); 2º. Reino Unido (284.291 vítimas); 3º. Canadá (5.517 vítimas); 4º. Índia (2.550 vítimas); 5º.

Austrália (2.489 vítimas); 6º. França (2.061 vítimas); 7º. África do Sul (1.929 vítimas); 8º. Alemanha (1.494 vítimas); e 9º. Brasil (1.181 vítimas) (USA, 2022, p. 19).

Os crimes cibernéticos não respeitam fronteiras e adotam técnicas cada vez mais complexas, o que dificulta sobremaneira as atividades de fiscalização, prevenção e repressão, cujo sucesso carece de uma intensa rede de cooperação internacional, com compartilhamento de informação e tecnologia, além de uma legislação anticrimes cibernéticos uniforme e eficaz.

Nesse sentido, o Conselho da Europa aprovou, no dia 23 de novembro de 2001, na cidade de Budapeste, Hungria, a Convenção sobre o Crime Cibernético, que entrou em vigor no dia 1º de julho 2004, e conta com a adesão também de países de fora do bloco europeu, como Estados Unidos, Chile, Argentina, Costa Rica, República Dominicana e, enfim, Brasil, que ratificou a Convenção, por meio do Decreto Legislativo nº 37, no dia 21 de dezembro de 2021 (BRASIL, 2021), e internalizou-a em seu ordenamento jurídico, no dia 12 de abril de 2023, pelo Decreto nº 11.491. (BRASIL, 2023)

Reconhecendo “a necessidade de um sistema de cooperação internacional imediato e eficiente, que considere devidamente as necessidades específicas da luta contra o crime cibernético” (BRASIL, 2023), a Convenção de Budapeste previu medidas a serem adotadas a nível nacional pelos Estados Partes, no âmbito do Direito Penal Material e do Direito Processual Penal, bem como de Cooperação Internacional.

Dentre as medidas a serem adotadas a nível nacional, no âmbito do Direito Penal Material, a Convenção prevê, em seu artigo 12, a responsabilização penal das pessoas jurídicas¹.

No escólio do saudoso jurista Eládio Lecey, “a complexidade dos interesses em jogo na estrutura das pessoas jurídicas pode levar à irresponsabilidade organizada dos indivíduos” (2002, p. 45). Aliás, a “diluição da responsabilidade não raro é buscada

¹ *In verbis*: “Cada Parte adotará medidas legislativas e outras providências necessárias para assegurar que pessoas jurídicas possam ser consideradas penalmente responsáveis por crimes tipificados de acordo com esta Convenção, quando cometidos em seu benefício por uma pessoa física em posição de direção, que aja individualmente ou como integrante de um órgão da própria pessoa jurídica, com base: a. no poder de representação da pessoa jurídica; b. na autoridade de tomar decisões em nome da pessoa jurídica; c. na autoridade de exercer controle interno na pessoa jurídica.” (BRASIL, 2023)

deliberadamente, com a utilização de mecanismos colegiados de decisão” (2002, p. 45). O combate eficaz à criminalidade cibernética exige, portanto, que a responsabilidade penal alcance as pessoas jurídicas e não se mantenha restrita às pessoas físicas.

A questão da responsabilização penal das pessoas jurídicas, todavia, não é isenta de polêmica. Alguns países, como os Estados Unidos², o Reino Unido³, a França⁴ e Portugal⁵, há um bom tempo a admitem. Entretanto, outros, como a Alemanha, não a aceitam.

No Brasil, a jurisprudência dos tribunais superiores evoluiu, no sentido de admitir a possibilidade de se responsabilizar penalmente pessoas jurídicas por delitos ambientais; contudo, no tocante aos crimes cibernéticos, a discussão continua aberta.

Seria, então, o Brasil capaz de cumprir o compromisso assumido, interna e internacionalmente, de assegurar que as pessoas jurídicas sejam responsabilizadas penalmente pela prática de crimes cibernéticos?

Para responder à questão posta, analisar-se-á a temática em cinco etapas: (1) conceito de crime cibernético; (2) constitucionalidade da responsabilidade penal da pessoa jurídica no contexto dos crimes cibernéticos; (3) requisitos de criminalização; (4) penas cabíveis; (5) medidas cautelares e ressarcimento das vítimas. Ao final, apresentar-se-á um esboço de como a matéria poderia ser legalmente regulamentada no Brasil.

2. CONCEITO DE CRIME CIBERNÉTICO

O primeiro desafio a ser superado é o de desenvolver um conceito adequado de crime cibernético, uma vez que tanto o ordenamento jurídico brasileiro, quanto a

² Ver: USA. New York Central & Hudson River Railroad Co. v. United States, 212 U.S. 481. U.S. Supreme Court. Washington/DC: Justia U.S. Supreme Court. Disponível em: <https://supreme.justia.com/cases/federal/us/212/481/>. Acesso em: 3 de julho de 2024.

³ Ver: UK. The Queen against The Birmingham and Gloucester Railway Company. English Reports Citation: 114 E.R. 21, 1º de jan. de 1842. Disponível em: <https://vlex.co.uk/vid/the-queen-against-the-803443733>. Acesso em: 3 de julho de 2024.

⁴ Ver: artigo 121-2 do Código Penal francês. Disponível em <https://irp.cdn-website.com/f6e36b8e/files/uploaded/CP%20franc%C3%AAs%20%28em%20espanhol%29.pdf>. Acessado em 14 de janeiro de 2024.

⁵ Ver: Lei nº 109, de 15 de setembro de 2009 (Lei do Cybercrime). Disponível em <https://diariodarepublica.pt/dr/detalhe/lei/109-2009-489693>. Acessado em 14 de janeiro de 2024.

Convenção de Budapeste, são silentes a respeito. Os especialistas na área ainda abordam a temática sob enfoques pontualmente distintos e adotam nomenclaturas bastante diversas, tais como: “crime virtual”, “e-crime”, “crime digital”, “crime on-line”, “tecnocrime” e “crime na rede” (Phillips et. al., 2022, p. 3). No Brasil, destacam-se ainda os termos “delito informático”⁶ e “delito telemático”⁷. Não bastasse, a Convenção de Budapeste, em seu preâmbulo, utiliza os termos “crime cibernético”, “crime informático” e “crime eletrônico” indistintamente.

Historicamente, o termo “cibernética” (*cybernetics*) foi cunhado pelo matemático Norbet Wiener, no ano de 1948, para designar o estudo científico do controle e da comunicação nos animais e nas máquinas, sob a ideia fundamental de que certas funções de controle e de processamento de informações semelhantes em máquinas e seres vivos são equivalentes e redutíveis aos mesmos modelos e mesmas leis matemáticas (Kim, 2004, p. 200). Anos mais tarde, a partir da década de 1980, o termo “cibernético” (*cyber*) passou a ser utilizado como sinônimo de algo relacionado a computadores e à internet (Phillips et. al., 2022, 381), notadamente à relação entre humanos e as tecnologias da informação (Schimitt, 2013, p. 258).

Nesse contexto, surge o termo “ciberespaço” (“espaço cibernético”), cuja paternidade é atribuída ao romancista Willian Gibson, que, em sua visionária obra de ficção científica intitulada *Neuromancer*, publicada no ano de 1984⁸, o descreve como: “Uma alucinação consensual vivida diariamente por bilhões (...). Uma representação gráfica dos dados abstraídos dos bancos de dados de cada computador no sistema humano” (Gibson, 1984, p. 51). O romance influenciou usuários e criadores de redes de computador, consagrando o termo também no mundo concreto, não ficcional.

⁶ O professor Spencer Toth Sydow, no livro intitulado *Curso de Direito Penal Informático*, definiu o delito informático como “a conduta típica, antijurídica e culpável cometida através de recursos informáticos contra bens jurídicos comuns e/ou cometida em face de bem jurídico informático, atingindo ou buscando atingir a esfera da segurança informática em seus elementos confidencialidade, integridade e disponibilidade.” (2022, p. 272)

⁷ O professor Augusto Eduardo de Souza Rossini, na obra *Informática, telemática e direito penal*, classifica o delito telemático como espécie do delito informático, salientando que aquele deve ser praticado necessariamente em ambiente de rede, enquanto este pode ser executado tanto em ambiente de rede quanto fora dele. (2004, p. 110)

⁸ Mais precisamente, o termo “ciberespaço” foi concebido pelo autor no ano de 1982, em uma publicação da revista *Omni*. Entretanto, o termo viria a ganhar popularidade dois anos mais tarde, com a publicação de *Neuromancer*. (BUSSELL, 2013)

O filósofo e sociólogo francês Pierre Lévy, em sua obra *Cibercultura*, define ciberespaço como o “espaço de comunicação aberto pela interconexão mundial dos computadores e das memórias dos computadores” (1999, p. 92), estas entendidas como “suportes de gravação e leitura automática de informações” (1999, p. 34), salientando que o ciberespaço é *povoado* por seres humanos, informações, materiais (*hardware*) e programas (*software*), que “interpretam dados, agem sobre informações, transformam outros programas, fazem funcionar computadores e redes, acionam máquinas físicas, viajam, reproduzem-se etc.” (1999, p. 41).

Mais recentemente, o Centro Nacional de Cibersegurança de Portugal publicou o que entende por ciberespaço, definindo-o como um “ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação” (CNCS, 2022).

Em verdade, não há um conceito fechado acerca do que vem a ser o ciberespaço, notadamente em razão da constante evolução tecnológica e cultural que lhe é inerente. Contudo, é possível afirmar que ele está inserido em um amplo e complexo contexto, composto por dados (*data*), dispositivos e sistemas informáticos, redes de dispositivos interconectados e, mais importante, seres humanos, cuja tutela jurídica não pode ser negligenciada.

Inerente a esse contexto há o conceito de “cibersegurança” (“segurança cibernética”), designando o conjunto de medidas e ações de “prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade⁹, integridade¹⁰ e disponibilidade¹¹ da informação, das redes digitais e dos sistemas de informação no ciberespaço, e das pessoas que nele interagem” (CNCS, 2022). O termo “crime cibernético”, enfim, surge em um contexto extrajurídico, para designar condutas contrárias à segurança cibernética desejada, bem como a prática

⁹ Confidencialidade é a “propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada a pessoa, a sistema, a órgão ou a entidade não autorizados nem credenciados.” (SYDOW, 2022, p. 817)

¹⁰ Integridade é a “qualidade da informação não modificada em seu conteúdo, forma, quanto à origem, trânsito e destino.” (SYDOW, 2022, p. 827)

¹¹ Disponibilidade é a “propriedade pela qual se assegura que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados.” (SYDOW, 2022, p. 821)

de crimes comuns mediante o uso de recursos cibernéticos, inclusive nas hipóteses de utilização de inteligência artificial.

Assim, “Convencidos da necessidade de buscar prioritariamente uma política criminal comum destinada à proteção da sociedade contra o crime cibernético” (Brasil, 2023), os Estados membros do Conselho da Europa e demais Partes elaboraram a Convenção de Budapeste, com o fim de “impedir ações conduzidas contra a confidencialidade, a integridade e a disponibilidade de sistemas informáticos¹², redes e dados de computador¹³, bem como para impedir o abuso de tais sistemas, redes e dados” (Brasil, 2023).

Como exposto anteriormente, a Convenção de Budapeste não trouxe um conceito de crime cibernético, preferindo definir alguns de seus elementos e listar condutas cibernéticas entendidas como criminosas (sem a pretensão de exauri-las). Entretanto, ao fazê-lo, ela acabou por fixar parâmetros relevantes.

Em primeiro lugar, seu artigo 1º define o que entende por sistema informático (ou sistema de computador)¹⁴ e dados informáticos (ou dados de computador)¹⁵, termos que irão ocupar o centro de todas as figuras a serem tipificadas como crime cibernético, na forma da Convenção. Sistema informático (ou sistema de computador) é conceituado como “qualquer dispositivo isolado ou conjunto de dispositivos interconectados ou relacionados, que assegure, isoladamente ou em conjunto, pela execução de um programa, o tratamento (ou processamento) automatizado de dados” (Coe, 2001b, p. 3)¹⁶,

¹² A depender da versão (a Convenção possui duas versões originais, uma no idioma inglês e outra no francês), este termo pode aparecer como “sistemas informáticos” ou “sistemas de computador”. A versão oficial em inglês utiliza o termo *computer systems* (“sistemas de computador”). Já a versão francesa utiliza o termo *systèmes informatiques* (“sistemas informáticos”). A tradução de Portugal, por exemplo, tem por base a versão francesa e utiliza o termo “sistemas informáticos” ao longo de todo o texto da Convenção. Curiosamente, a tradução brasileira mistura as duas fontes. No preâmbulo, como visto, utiliza o termo “sistemas informáticos” (da fonte francesa). No restante do texto, contudo, utiliza o termo “sistemas de computador” (da fonte em inglês). Imperioso que se compreenda, portanto, que ambos os termos, no contexto da Convenção de Budapeste, designam a mesma ideia.

¹³ A depender da versão, este termo pode aparecer como “dados informáticos” ou “dados de computador”. A versão oficial em idioma inglês utiliza o termo *computer data* (“dados de computador”), enquanto a versão em idioma francês utiliza o termo *données informatiques* (“dados informáticos”). A tradução brasileira, nesse caso, optou exclusivamente pela fonte em idioma inglês, razão por que utiliza o termo “dados de computador”. Frise-se, mais uma vez, que, no contexto da Convenção, ambos os termos designam a mesma ideia.

¹⁴ Ver nota 12.

¹⁵ Ver nota 13.

¹⁶ Como visto nas notas 12 e 13, a Convenção de Budapeste possui duas versões originais, uma em idioma inglês e outra em francês, sendo que a versão em inglês utiliza os termos “sistema de computador”, “dados de computador” e “processamento automático de dados”, enquanto a versão em francês utiliza, para as

estes entendidos como “qualquer representação de fatos, de informações ou de conceitos sob uma forma suscetível de tratamento (ou processamento) num sistema informático (ou de computador), incluindo um programa apto a fazer um sistema informático (ou de computador) executar uma função” (Coe, 2001b, p. 3)¹⁷.

Portanto, o conceito de sistema informático abrange desde um único dispositivo isolado, capaz de assegurar, pela execução de um programa, o tratamento¹⁸ automatizado de dados, até o mais complexo conjunto de dispositivos interconectados, como é o caso da rede mundial de computadores (ou internet). Aliás, no ano de 2023, o Conselho da Europa publicou o *Relatório explicativo à Convenção sobre o Cibercrime*, enfatizando que o sistema informático “é um equipamento composto por *hardware* e *software* desenvolvido para o tratamento automático de dados” (Coe, 2023, p. 45), podendo incluir “dispositivos de entrada, saída e armazenamento” (Coe, 2023, p. 45) e “funcionar independentemente ou estar ligado em rede com outros dispositivos semelhantes” (Coe, 2023, p. 45).

A abrangência do conceito de sistema informático está diretamente relacionada com a extensão do âmbito de incidência dos crimes cibernéticos. A título de exemplo, de acordo com o artigo 2º, primeira parte, da Convenção, caracteriza crime cibernético “o acesso doloso e não autorizado à totalidade de um sistema informático ou a parte dele” (Coe, 2001b, p. 3). Em outras palavras, o acesso doloso e não autorizado a um único dispositivo (que seja capaz de assegurar, pela execução de um programa, o tratamento automatizado de dados) já configura crime cibernético. Não é necessário, portanto, que haja um conjunto de dispositivos interconectados em rede (apesar de isso também ser possível) para que se caracterize o crime cibernético. O mesmo raciocínio é perfeitamente aplicável às demais figuras previstas na Convenção, uma vez que possuem como elemento central o sistema informático. Em síntese, os crimes cibernéticos não se restringem a infrações penais praticadas na internet ou mesmo em redes menores; ao contrário, eles abrangem todo espectro de infrações penais praticadas por meio de

mesmas ideias, os termos “sistema informático”, “dados informáticos” e “tratamento automatizado de dados”, respectivamente. Optamos, assim, por dar preferência aos termos da versão em francês (mencionando os termos da versão em inglês entre parênteses), porque são mais condizentes com aqueles utilizados pela legislação brasileira.

¹⁷ Ver nota 16.

¹⁸ Em uma análise sistemática da Convenção de Budapeste, é possível concluir que o termo “tratamento” é empregado de forma ampla, para designar tanto o processamento, quanto a transmissão e o armazenamento de dados.

sistemas informáticos (dispositivos físicos (*hardware*), conectados ou não em rede, capazes de assegurar, pela execução de um programa (*software*), o tratamento automatizado de dados, como computadores de mesa (*desktop*), notebooks, smartphones, tablets, drives externos, pen-drives etc.).

Ademais, o crime cibernético (apesar do termo “crime”) tem natureza de infração penal, abrangendo crimes e contravenções penais. É o que se depreende da versão original da Convenção, redigida em francês¹⁹, que, ao longo de todos os artigos da seção sobre direito penal material, utiliza o termo “infração penal” (*infraction pénale*) ao invés de “crime” (Coe, 2001b, pp. 3-7). Aliás, como dito anteriormente, a expressão “crime cibernético” é fruto de um contexto originalmente extrajurídico, não havendo qualquer indício de que o termo “crime” tenha sido empregado com o intuito de excluir as contravenções penais de seu âmbito de incidência.

Pode-se, enfim, conceituar o crime cibernético, à luz da Convenção de Budapeste, como *qualquer infração penal praticada por meio de sistema informático, conectado ou não em rede, ou contra a segurança cibernética, notadamente com afronta à confidencialidade, integridade e disponibilidade de sistemas, redes e/ou dados informáticos*. Trata-se, portanto, de conceito compatível com os tipos penais congêneres previstos na legislação brasileira.

Com efeito, o crime de intimidação sistemática virtual (*cyberbullying*), previsto no artigo 146-A, parágrafo único, do Código Penal, consiste na intimidação sistemática “realizada por meio de rede de computadores, de rede social, de aplicativos, de jogos online ou por qualquer outro meio ou ambiente digital, ou transmitida em tempo real” (Brasil, 1940). Trata-se, portanto, de infração penal praticada por meio de sistema informático.

O crime de invasão de dispositivo informático, previsto no artigo 154-A do Código Penal, consiste em “Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou

¹⁹ Sempre que há conflito significativo entre as versões originais (em inglês e francês) e a tradução brasileira, optamos por privilegiar as versões originais, uma vez que são essas que efetivamente vinculam os signatários, inclusive o Brasil. No caso, entendemos mais pertinente a versão original em francês, uma vez que os termos jurídicos empregados são mais próximos aos adotados no Brasil. De qualquer sorte, o termo *criminal offences*, do original em inglês, é amplo a ponto de abranger o que adotamos como contravenção penal no Brasil.

informações sem autorização expressa ou tácita do usuário do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita”. Trata-se, dessa forma, de infração penal praticada contra a segurança cibernética, com afronta à confidencialidade, integridade e disponibilidade de sistemas, redes e/ou dados informáticos.

O crime de furto mediante fraude, previsto no artigo 155, §4º-B, do Código Penal, “cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo” é infração penal praticada por meio de sistema informático.

O crime de fraude eletrônica, previsto no artigo 171, § 2º-A, do Código Penal, “cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo” também é infração penal praticada por meio de sistema informático.

Como último exemplo, a contravenção penal de jogo de azar pela internet, prevista no artigo 50, § 2º, da Lei das Contravenções Penais, trata-se igualmente de infração penal praticada por meio de sistema informático.

Finalmente, imperioso observar que a Convenção de Budapeste (em seu artigo 6º) equipara a crime cibernético condutas antecedentes de possuir ou, de qualquer forma, disponibilizar os meios (dispositivo, programa informático (ou de computador), senha, código de acesso ou dados similares) para a consecução dos crimes cibernéticos listados. Aliás, o Código Penal também o faz, de forma semelhante, em relação ao crime de invasão de dispositivo informático (em seu artigo 154-A, § 1º).

Assim, incorporando-se ao conceito em tela as condutas antecedentes supracitadas, temos como crime cibernético *qualquer infração penal praticada por meio de sistema informático, conectado ou não em rede; ou contra a segurança cibernética, notadamente com afronta à confidencialidade, integridade e disponibilidade de sistemas, redes e/ou dados informáticos; ou mediante a posse ou disponibilização dos meios para tais fins.*

3. CONSTITUCIONALIDADE DA RESPONSABILIDADE PENAL DA PESSOA JURÍDICA NO CONTEXTO DOS CRIMES CIBERNÉTICOS

Compreendido o amplo contexto dos crimes cibernéticos, passemos à análise da responsabilidade penal das pessoas jurídicas que, nesse contexto, praticam infrações penais, iniciando-se pela análise de sua compatibilidade com o sistema constitucional vigente no Brasil.

Seguindo o adágio *societas delinquere non potest*, parcela da doutrina resiste à responsabilização penal da pessoa jurídica. Nesse sentido, Jescheck sustenta que:

[...] as pessoas jurídicas e as associações sem personalidade somente podem atuar através de seus órgãos, razão pela qual elas próprias não podem ser punidas. Frente a elas carece, ademais, de sentido a desaprovação ético-social inerente à pena, visto que a reprovação de culpabilidade somente pode ser formulada a pessoas individualmente responsáveis, e não perante membros de uma sociedade que não participaram do fato nem perante a uma massa patrimonial. (1993, p. 300)

Para os defensores desta corrente, a capacidade de ação e a culpabilidade exigem a presença de uma vontade, que não existiria no ente moral. (Conde; Arán, 2010, p. 631)

De outro modo, as Cortes inglesas reconhecem, desde o século XIX, a possibilidade de responsabilização criminal das pessoas jurídicas.²⁰

Nos Estados Unidos, a Suprema Corte já decidiu que:

Embora o direito deva ter em conta os direitos de todos, e os das empresas não menos do que os dos indivíduos, ele não pode fechar os seus olhos para o fato de que a grande maioria das atividades econômicas nos tempos modernos é conduzida por empresas, de que particularmente todo o comércio entre os Estados está inteiramente em suas mãos, e de que conceder a elas imunidade de qualquer punição, em decorrência da velha e explodida doutrina de que uma empresa não pode delinquir, iria tornar indisponíveis os únicos meios de efetivamente regular a matéria e de corrigir os abusos praticados. (tradução livre) (USA, 1909)

²⁰ Ver: UK. The Queen against The Birmingham and Gloucester Railway Company. English Reports Citation: 114 E.R. 21, 1º de jan. de 1842. Disponível em <https://vlex.co.uk/vid/the-queen-against-the-803443733>. Acesso em: 3 de julho de 2024.

Aliás, nas palavras do professor Fernando Antônio Nogueira Galvão da Rocha, “é inegável que a tendência atual do Direito mundial é no sentido de admitir a utilização do Direito Penal contra a pessoa jurídica, nos crimes socialmente mais importantes.” (2023, p. 5)

O tema da responsabilidade penal da pessoa jurídica, no Direito brasileiro, ganhou relevância com o advento da Constituição Federal de 1988, que prevê expressamente, em seu artigo 225, § 3º, que as condutas e atividades lesivas ao meio ambiente sujeitarão os infratores, sejam eles pessoas físicas ou jurídicas, a sanções penais. Ademais, a mesma Constituição, em seu artigo 173, § 5º, elencou como hipóteses passíveis de responsabilização da pessoa jurídica a prática de atos contra a ordem econômica e financeira e contra a economia popular. (Brasil, 1988)²¹

Entretanto, foi com a Lei nº 9.605, de 12 de fevereiro de 1998, sobre sanções penais e administrativas derivadas de condutas e atividades lesivas ao meio ambiente, que a responsabilidade penal das pessoas jurídicas foi efetivamente regulamentada, notadamente nos artigos 3º, 21, 22, 23 e 24.

Ironicamente, parte da doutrina brasileira defendeu a inconstitucionalidade (e até mesmo a incoerência) da responsabilidade penal da pessoa jurídica, sob os seguintes argumentos: (1) as pessoas jurídicas não possuem capacidade para a prática de ações de relevância penal; (2) elas não são culpáveis; (3) também não podem sofrer sanções penais; e (4) há ofensa ao princípio constitucional que preceitua que nenhuma pena passará da pessoa do condenado.

Esses argumentos, todavia, foram superados pela jurisprudência brasileira, notadamente a partir do julgamento do Recurso Especial nº 564.960/SC (*leading case*),

²¹ Sob essa perspectiva, as professoras Ana Maria Lumi Kamimura Murata e Paula Ritzmann Torres advogam a constitucionalidade da responsabilidade penal da pessoa jurídica no contexto dos crimes cibernéticos, especificamente quando estes atingem aqueles bens jurídicos listados expressamente nos artigos 173, § 5º, e 225, § 3º, da Constituição Federal, ou seja, a ordem financeira e econômica, a economia popular e o meio ambiente. *In verbis*: “há previsão na Constituição de 1988 da responsabilidade penal da pessoa jurídica. O art. 173, § 5º, da CR, prevê a responsabilidade da pessoa jurídica, ‘sujeitando-as às punições compatíveis com sua natureza, nos atos praticados contra a ordem econômica e financeira e contra a economia popular’. Já no 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’. Expressamente, o texto constitucional enumera bens jurídicos a possibilitar a responsabilização penal do ente coletivo. Como o que qualifica os delitos como cibernéticos não é o bem jurídico, é possível vislumbrar condutas que se enquadram nas hipóteses listadas, para essa forma de responsabilidade constante do decreto.” (Murata; Torres, 2023, p. 15)

no dia 13 de junho de 2005, sob os seguintes fundamentos: (1) “Se a pessoa jurídica tem existência própria no ordenamento jurídico brasileiro e pratica atos no meio social através da atuação de seus administradores, poderá vir a praticar condutas típicas e, portanto, ser passível de responsabilização penal”; (2) “A culpabilidade, no conceito moderno, é a responsabilidade social, e a culpabilidade da pessoa jurídica, neste contexto, limita-se à vontade do seu administrador ao agir em seu nome e proveito”; (3) “A Lei Ambiental previu para as pessoas jurídicas penas autônomas de multas, de prestação de serviços à comunidade, restritivas de direitos, liquidação forçada e desconsideração da pessoa jurídica, todas adaptadas à sua natureza jurídica”; e (4) “Não há ofensa ao princípio constitucional de que ‘nenhuma pena passará da pessoa do condenado...’, pois é incontroversa a existência de duas pessoas distintas: uma física – que de qualquer forma contribui para a prática do delito – e uma jurídica, cada a qual recebendo a punição de forma individualizada, decorrente de sua atividade lesiva” (Brasil, 2005).

O Supremo Tribunal Federal foi além ao reconhecer a constitucionalidade da responsabilidade penal da pessoa jurídica e superar a “teoria da dupla imputação” (até então dominante na jurisprudência do Superior Tribunal de Justiça), assentando, no Recurso Extraordinário nº 548.181/PR (*leading case*), julgado no dia 6 de agosto de 2013, que o “art. 225, § 3º, da Constituição Federal não condiciona a responsabilização penal da pessoa jurídica por crimes ambientais à simultânea persecução penal da pessoa física em tese responsável no âmbito da empresa” (BRASIL, 2013, p. 1), ou seja, que a “norma constitucional não impõe a necessária dupla imputação” (Brasil, 2013, p. 1).

Não há dúvida, portanto, que a jurisprudência brasileira entende constitucional a responsabilidade penal da pessoa jurídica no contexto dos crimes ambientais. Entretanto, o mesmo raciocínio seria extensível aos demais crimes, notadamente aos crimes cibernéticos? Em outras palavras, a previsão constitucional de que as condutas e atividades consideradas lesivas ao meio ambiente sujeitarão as pessoas jurídicas a sanções penais (artigo 225, § 3º) deve ser interpretada como uma restrição constitucional (“reserva de Constituição”), com o fim de restringir a responsabilidade penal das pessoas jurídicas apenas a crimes ambientais; ou, em sentido oposto, deve ser entendida como um mandado de criminalização da pessoa jurídica em relação a condutas e atividades lesivas ao meio ambiente, deixando ao legislador infraconstitucional a liberdade de definir os demais casos de responsabilidade penal das pessoas jurídicas?

A lógica diz que a resposta só pode ser sim, ou seja, que o mesmo raciocínio é extensível aos demais crimes, notadamente aos crimes cibernéticos, e que a previsão constitucional supracitada deve ser interpretada como um mandado de criminalização da pessoa jurídica em relação a condutas e atividades lesivas ao meio ambiente, deixando ao legislador infraconstitucional a liberdade de definir os demais casos de responsabilidade penal das pessoas jurídicas. Não por outra razão, a então Ministra do Supremo Tribunal Federal Rosa Weber, relatora do Recurso Extraordinário supracitado, ao analisar a questão da responsabilização penal da pessoa jurídica, asseverou expressamente que “não há reserva de Constituição para a criminalização de condutas, nem para a definição de quem possa ser sujeito ativo da prática de crimes” (Brasil, 2013, p. 36), cabendo ao legislador “o juízo de conveniência e oportunidade quanto à consagração do instituto” (Brasil, 2013, p. 36).

Com efeito, quando a Constituição Federal fixa os limites constitucionais à aplicação do Direito Penal e Processual Penal, notadamente em seu artigo 5º, incisos XXXVIII a LXVIII, ela não fixa qualquer limite à responsabilização penal das pessoas jurídicas. Muito pelo contrário, como visto, o artigo 225, § 3º, da Constituição Federal, claramente exorta o legislador infraconstitucional a responsabilizar penalmente as pessoas jurídicas por condutas e atividades consideradas lesivas ao meio ambiente, sem fazer qualquer referência que pudesse ser entendida como restrição à responsabilização penal das pessoas jurídicas pela prática de outros crimes.

Não por outra razão, os professores Guilherme José Purvin de Figueiredo e Solange Teles da Silva, há mais de 25 anos, já afirmavam que “A responsabilidade penal da pessoa jurídica é possível, está plenamente amparada pela Constituição da República Federativa do Brasil e constitui um avanço inegável na evolução do Direito Penal.” (Figueiredo; Silva, 1998, p. 57).

Importante ainda destacar que o Supremo Tribunal Federal, analisando a questão relativa à responsabilidade das pessoas jurídicas, de modo geral, fez questão de asseverar expressamente que as “organizações corporativas complexas da atualidade se caracterizam pela descentralização e distribuição de atribuições e responsabilidades, sendo inerentes, a esta realidade, as dificuldades para imputar o fato ilícito a uma pessoa concreta” (Brasil, 2013, p. 1) e que em “não raras oportunidades, as responsabilidades

internas pelo fato estarão diluídas ou parcializadas de tal modo que não permitirão a imputação de responsabilidade penal individual” (Brasil, 2013, p. 2).

Essas observações, frise-se, são extremamente pertinentes à realidade dos crimes cibernéticos, que, como destacado na introdução deste artigo, estão em franca expansão, não respeitam fronteiras e são a cada dia mais elaborados, de modo a dificultar sobremaneira as atividades de fiscalização, prevenção e repressão. Não por outra razão, a Convenção de Budapeste sobre o Crime Cibernético exorta os Estados Partes a adotarem medidas legislativas e outras que se revelem necessárias para assegurar que as pessoas jurídicas possam ser consideradas responsáveis por infrações cibernéticas.

Nesse ponto, o professor Fernando Antônio Nogueira Galvão da Rocha, observa que o “debate doutrinário que inicialmente centrou atenções sobre a possibilidade de responsabilização penal das pessoas jurídicas evoluiu para enfrentar a questão relativa a como realizar adequadamente tal responsabilização.” (2023, p. 5)

Com efeito, os novos riscos na sociedade pós-moderna acarretam uma crise no Direito Penal. Essa crise leva a uma ruptura no paradigma vigente, promovendo novas reflexões e novos rumos no combate aos delitos, tornando-se indispensável uma leitura constitucional do Direito Penal. Assim, ainda que o Direito Penal clássico não tenha estabelecido os critérios de responsabilização da pessoa jurídica, isso não pode implicar no esvaziamento de enunciados constitucionais supracitados. Assim, com o intuito de impedir que a pessoa jurídica obtenha vantagens advindas da prática de condutas típicas e fomentar que os órgãos de direção atuem de modo a afastar a prática de delitos, a adequada exegese dos enunciados constitucionais só pode ser aquela que confere à Constituição a máxima força normativa e efetividade.

Conclui-se, inexoravelmente, que o instituto da responsabilidade penal da pessoa jurídica²², na forma como preconizada pelo artigo 12 da Convenção de Budapeste sobre o Crime Cibernético, além de constitucional, é essencial no combate ao crescente avanço da criminalidade cibernética no Brasil e no mundo.²³

²² Para maior aprofundamento na temática da responsabilidade penal das pessoas jurídicas, ver: ROCHA, Fernando Antônio Nogueira Galvão da. *Responsabilidade penal das pessoas jurídicas*. 4ª ed. Belo Horizonte/MG: Editora D'Plácido, 2017.

²³ A importância do instituto, aliás, passou a ser ainda mais acentuada no Brasil com o advento da Emenda Constitucional nº 115, de 10 de fevereiro de 2022, que ampliou o rol de direitos e deveres individuais, ao

4. REQUISITOS DE CRIMINALIZAÇÃO

Ultrapassada a etapa de análise da constitucionalidade da responsabilidade penal da pessoa jurídica no contexto dos crimes cibernéticos, imperioso analisar os requisitos de criminalização, ou seja, os requisitos que devem ser implementados para que a pessoa jurídica possa ser concretamente responsabilizada pela sua prática.

Em primeiro lugar, a responsabilidade penal da pessoa jurídica nos cibercrimes deve ser regulamentada por lei federal. Com efeito, nos termos do artigo 5º, inciso XXXIX, da Constituição Federal “não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal”. Ademais, por força do artigo 22, inciso I, da Constituição da República Federativa do Brasil, compete privativamente à União legislar sobre direito penal.

Frise-se que a única lei brasileira que prevê a responsabilidade penal da pessoa jurídica é a Lei nº 9.605, de 12 de fevereiro de 1998, que, como visto anteriormente, dispõe sobre crimes contra o meio ambiente. Essa, aliás, é a razão de a jurisprudência brasileira ter consolidado a constitucionalidade da responsabilidade penal da pessoa jurídica no âmbito dos crimes ambientais, sem mencionar expressamente crimes de outras espécies.

A regulamentação da matéria, todavia, não precisa ser prolixa, com a previsão de novos tipos penais, especificamente aplicáveis às pessoas jurídicas, desprezando-se os tipos já existentes e em vigor no Direito Penal brasileiro. Na essência, basta que haja lei federal atribuindo responsabilidade penal e penas adequadas às pessoas jurídicas, de forma geral e abstrata, pela prática de infrações penais já existentes e daquelas que virão a existir, desde que enquadráveis nos parâmetros fixados pela própria lei regulamentadora. Aliás, esse foi o caminho escolhido pelo legislador ao regulamentar a responsabilidade penal das pessoas jurídicas, no âmbito da Lei nº 9.605/98, quando, no

acrescentar o inciso LXXIX ao artigo 5º da Constituição Federal, para tornar expresso o direito fundamental à proteção de dados pessoais em meios digitais, *in verbis*: “é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.” (BRASIL, 2022)

artigo 3º, atribuiu responsabilidade penal a elas e, nos artigos 21 a 24, fixou-lhes as penas aplicáveis.

A título de exemplo, para que se atribua responsabilidade penal às pessoas jurídicas pela prática de crimes cibernéticos, poder-se-á dispor, em um único artigo de lei, o seguinte: *As pessoas jurídicas serão responsabilizadas penalmente pela prática de crime cibernético – infração penal executada por meio de sistema informático, conectado ou não em rede; ou contra a segurança cibernética, notadamente com afronta à confidencialidade, integridade e disponibilidade de sistemas, redes e/ou dados informáticos; ou mediante a posse ou disponibilização dos meios para tais fins.*

Com efeito, os parâmetros fixados na redação supracitada são suficientes para atribuir responsabilidade penal às pessoas jurídicas pelos crimes cibernéticos já existentes em nossa legislação penal (cf. item 2) e quaisquer outros que venham a surgir posteriormente no contexto da criminalidade cibernética.

Ademais, a Convenção de Budapeste sobre o Crime Cibernético traz requisitos específicos à responsabilização penal das pessoas jurídicas no contexto dos crimes cibernéticos, dentre os quais pode-se destacar: (1) a infração penal deve ser cometida (por ação ou omissão) em benefício da pessoa jurídica, por pessoa física, agindo quer individualmente, quer como membro de um órgão da pessoa jurídica que exerça no seu seio uma posição de direção, com poder de representação, autoridade para tomar decisões em nome dela ou autoridade para exercer controle no seio da pessoa jurídica; (2) essa responsabilidade deve ser determinada sem prejuízo da responsabilidade criminal das pessoas físicas que cometeram a infração. (Brasil, 2023)

Dessa forma, acrescentando-se os requisitos supracitados, a atribuição de responsabilidade penal às pessoas jurídicas, em um único artigo de lei, poderá ser concretizada, nos seguintes termos: *As pessoas jurídicas serão responsabilizadas penalmente pela prática, por ação ou omissão, de crime cibernético – infração penal executada por meio de sistema informático, conectado ou não em rede; ou contra a segurança cibernética, notadamente com afronta à confidencialidade, integridade e disponibilidade de sistemas, redes e/ou dados informáticos; ou mediante a posse ou disponibilização dos meios para tais fins –, sem prejuízo da responsabilidade penal das pessoas físicas que cometeram a infração, e desde que cometida em benefício da pessoa*

jurídica, por pessoa física, agindo quer individualmente, quer como membro de um órgão da pessoa jurídica que exerça no seu seio uma posição de direção, com poder de representação, autoridade para tomar decisões em nome dela ou autoridade para exercer controle no seio da pessoa jurídica.

5. PENAS CABÍVEIS

Uma vez atribuída responsabilidade penal às pessoas jurídicas, resta a fixação de penas adequadas no contexto dos crimes cibernéticos.

A visão tradicional que enxergava a pena privativa de liberdade como central no sistema penal é fática e logicamente incompatível com a ideia de sancionamento penal das pessoas jurídicas. Entretanto, cuida-se de visão há muito tempo ultrapassada, notadamente com a consagração, já no século passado, das penas alternativas às privativas de liberdade no Direito Penal brasileiro. Aliás, não por outra razão, o Ministro do Superior Tribunal de Justiça Gilson Dipp, relator do Recurso Especial nº 564.960/SC, assevera que a “insuscetibilidade de imposição de penas privativas de liberdade às pessoas jurídicas é um argumento pouco aceitável contrário à sua responsabilização penal” (Brasil, 2005), acrescenta que o “ordenamento penal brasileiro prevê outras sanções penais para os entes morais” (Brasil, 2005) e destaca que a “Lei Ambiental, com efeito, previu para as pessoas jurídicas penas autônomas de multas, de prestação de serviços à comunidade, restritivas de direitos, liquidação forçada e desconsideração da pessoa jurídica.” (Brasil, 2005)

O Ministro está se referindo exatamente à Lei nº 9.605/98, que, em seus artigos 21 a 24, fixou penas adequadas às pessoas jurídicas, no contexto dos crimes ambientais, quais sejam:

- 1) Multa.
- 2) Restritivas de direitos:
 - a) Suspensão parcial ou total das atividades: quando estas não estiverem obedecendo às disposições legais ou regulamentares, relativas à proteção do meio ambiente.

b) Interdição temporária de estabelecimento, obra ou atividade: quando o estabelecimento, obra ou atividade estiver funcionando sem a devida autorização, ou em desacordo com a concedida, ou com violação de disposição legal ou regulamentar.

c) Proibição de contratar com o Poder Público, bem como dele obter subsídios, subvenções ou doações: por até 10 anos.

3) Prestação de serviços à comunidade:

a) Custeio de programas e de projetos ambientais.

b) Execução de obras de recuperação de áreas degradadas.

c) Manutenção de espaços públicos.

d) Contribuições a entidades ambientais ou culturais públicas.

4) Liquidação forçada: a pessoa jurídica constituída ou utilizada, preponderantemente, com o fim de permitir, facilitar ou ocultar a prática de crime ambiental, terá decretada sua liquidação forçada, seu patrimônio será considerado instrumento do crime e como tal perdido em favor do Fundo Penitenciário Nacional. (BRASIL, 1998)

Esse modelo, há décadas consagrado pelo Direito Penal brasileiro e reconhecido como válido pela jurisprudência nacional, pode ser utilizado como base para a fixação das penas cabíveis às pessoas jurídicas, no contexto dos cibercrimes, com as devidas adaptações.

A Lei nº 9.605/98 não prevê parâmetros específicos para o cálculo da pena de multa às pessoas jurídicas. Entretanto, a Lei nº 12.965/2014 (Marco Civil da Internet) fixa parâmetros, em seu artigo 12 (Brasil, 2014), para a aplicação de multa a pessoas jurídicas em caso de infração às normas de proteção aos registros, aos dados e às comunicações privadas, que podem ser igualmente úteis no contexto dos crimes cibernéticos, são eles:

1) valor de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos;

2) considerando-se a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção.

Pode-se, ainda, acrescentar os parâmetros previstos no artigo 52, § 1º, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais) (Brasil, 2018), quais sejam:

- 1) gravidade e natureza das infrações e dos direitos pessoais afetados;
- 2) boa-fé do infrator;
- 3) vantagem auferida ou pretendida pelo infrator;
- 4) condição econômica do infrator;
- 5) reincidência;
- 6) grau do dano;
- 7) cooperação do infrator;
- 8) adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano;
- 9) adoção de política de boas práticas e governança;
- 10) pronta adoção de medidas corretivas;
- 11) proporcionalidade entre a gravidade da falta e a intensidade da sanção.

Quanto às restritivas de direitos, é possível adaptá-las, nos seguintes termos:

- 1) Suspensão parcial ou total das atividades, quando estas estiverem relacionadas com a prática de crime cibernético.
- 2) Interdição temporária de estabelecimento, quando este for utilizado para a prática de crime cibernético.
- 3) Proibição de contratar com o Poder Público, bem como dele obter subsídios, subvenções ou doações, por até 10 anos.

A Lei nº 9.605/98 também não traz parâmetros específicos para a quantificação do prazo de suspensão parcial das atividades, de interdição temporária de estabelecimento, nem de proibição de contratar com o Poder Público, bem como dele obter subsídios, subvenções ou doações.

Contudo, é plenamente viável, razoável e adequada a aplicação da lógica estabelecida pelo artigo 55 do Código Penal (Brasil, 1940) para aplicação das penas restritivas de direitos previstas na citada Lei Penal, desde que realizadas as adaptações pertinentes. Em outras palavras, o prazo das penas restritivas de direitos seria calculado utilizando-se os mesmos critérios de aplicação de pena consagrados pelo Código Penal, nos artigos 59 a 76 (Brasil, 1940), para pessoas físicas, adotando como base as mesmas penas fixadas em abstrato nos tipos penais imputados à pessoa jurídica. Ou seja, a pena restritiva de direitos aplicada à pessoa jurídica teria a mesma duração da pena privativa

de liberdade eventualmente fixada à pessoa física, quando da prática da mesma infração penal.

No tocante às penas de prestação de serviços à comunidade, poder-se-ia cogitar as seguintes:

1) Custeio de programas e projetos de tecnologia da informação, proteção de registros, dados pessoais e comunicações privadas, bem como contra cibercrimes e ataques cibernéticos em geral: adotando-se os mesmos parâmetros de cálculo do *quantum debeat* indicados na análise da pena de multa.

2) Execução de programas e projetos de tecnologia da informação, proteção de registros, dados pessoais e comunicações privadas, bem como contra cibercrimes e ataques cibernéticos em geral: utilizando-se os mesmos parâmetros de quantificação indicados na análise das penas restritivas de direitos.

Finalmente, como sanção mais gravosa, nos casos extremos em que a pessoa jurídica é constituída ou utilizada, preponderantemente, com o fim de permitir, facilitar ou ocultar a prática de crime cibernético, pertinente a aplicação da pena de Liquidação Forçada, a fim de considerar o patrimônio jurídico da pessoa jurídica instrumento do crime e, como tal, perdido em favor do Poder Público.

Frise-se que o modelo desenvolvido neste artigo, com base nas Leis nº 9.605/1998, 12.965/2014 e 13.709/2018, tem congruência com aquele sugerido aos membros da União Europeia, por meio da Diretiva do Parlamento Europeu e do Conselho de 12 de agosto de 2013, relativa a ataques contra os sistemas de informação, que em seu artigo 11, igualmente propõe como sanções aplicáveis às pessoas jurídicas: (1) multa; (2) exclusão do direito a benefícios ou auxílios públicos; (3) proibição temporária ou permanente de exercer atividades comerciais; (4) liquidação; e (5) encerramento temporário ou definitivo dos estabelecimentos utilizados para a prática da infração. (UE, 2013, p. 13)

6. MEDIDAS CAUTELARES E RESSARCIMENTO DAS VÍTIMAS

Imperioso destacar que os crimes cibernéticos são dinâmicos e podem rapidamente gerar danos superlativos a uma grande quantidade de vítimas, caso não existam mecanismos legais que viabilizem uma contra ação rápida das autoridades competentes. Indispensável, portanto, que a lei regulamentadora também traga a previsão de cautelares específicas para a garantia da ordem pública, da ordem econômica, da conveniência da instrução criminal e, até mesmo, para assegurar a aplicação da lei penal.

Adotando como base o Título IX do Código de Processo Penal, notadamente os artigos 282, 311 e 312 (Brasil, 1941), em cotejo com o artigo 22 da Lei nº 9.605/98 (Brasil, 1998) e com o artigo 139, inciso IV, do Código de Processo Civil (Brasil, 2015), é possível disciplinar a aplicação de cautelares às pessoas jurídicas, no contexto dos crimes cibernéticos, nos seguintes termos: *Em qualquer fase da investigação criminal ou do processo penal, caberão medidas cautelares decretadas judicialmente, de ofício ou a requerimento do Ministério Público, do querelante, do assistente de acusação, ou por representação da autoridade policial, como garantia da ordem pública, da ordem econômica, por conveniência da instrução criminal ou para assegurar a aplicação da lei penal, quando houver prova da existência do crime e indícios suficientes de autoria, desde adequadas à gravidade do crime e às circunstâncias do fato.*

Ademais, como espécies de cautelares adequadas às pessoas jurídicas, é possível elencar: (1) suspensão parcial de atividades; (2) interdição temporária de estabelecimento; (3) proibição de contratar com o poder público, bem como dele obter subsídios, subvenções ou doações; e (4) outras medidas indutivas, coercitivas, mandamentais ou sub-rogatórias necessárias; pelo tempo que durar o risco à ordem pública, à ordem econômica, à conveniência da instrução criminal e à aplicação da lei penal.

Finalmente, é importante que a lei, a exemplo do artigo 387, inciso IV, do Código de Processo Penal (BRASIL, 1941), permita que a sentença penal já fixe um valor mínimo para a reparação dos danos causados pela infração, considerando os prejuízos sofridos pelas vítimas.

7. ESBOÇO DE LEI REGULAMENTADORA

Com base em tudo o que foi analisado, e encampando as propostas apresentadas pelo professor Fernando Antônio Nogueira Galvão da Rocha na Comissão de Constituição e Justiça e de Cidadania da Câmara dos Deputados, no ano de 2021²⁴, é possível regulamentar a responsabilidade penal da pessoa jurídica em relação a crimes cibernéticos, com cominação de penas adequadas, fixação de cautelares eficientes e previsão de ressarcimento de danos às vítimas, nos seguintes termos:

Art. 1º. A pessoa jurídica será responsabilizada penalmente pela prática, por ação ou omissão, de crime cibernético.

Parágrafo único. Crime cibernético é qualquer infração penal praticada por meio de sistema informático, conectado ou não em rede; ou contra a segurança cibernética, notadamente com afronta à confidencialidade, integridade e disponibilidade de sistemas, redes e/ou dados informáticos; ou mediante a posse ou disponibilização dos meios para tais fins.

Art. 2º. A atividade da pessoa jurídica é penalmente relevante quando violar dever que lhe é diretamente dirigido e a decisão institucional que a determinar for motivada pelo interesse ou benefício da entidade.

§ 1º. Para que a pessoa jurídica seja responsabilizada penalmente, a infração penal deverá ser praticada em benefício dela, por pessoa física, agindo quer individualmente, quer como membro de um órgão da pessoa jurídica que exerça no seu seio uma posição de direção, com poder de representação, autoridade para tomar decisões em nome dela ou autoridade para exercer controle no seio da pessoa jurídica.

§ 2º. A responsabilidade das pessoas jurídicas é independente da responsabilidade das pessoas físicas.

Art. 3º. Atribui-se à pessoa jurídica o crime:

I – doloso, quando a decisão institucional determinar a realização de atividade que viole a norma incriminadora ou aceitar a ocorrência sua de sua violação; e II – culposo, quando a violação da norma incriminadora decorrer do defeito de organização da entidade.

Art. 4º. A pessoa jurídica é imputável desde a sua constituição.

Parágrafo único. Extinta a pessoa jurídica posteriormente ao fato criminoso, com a finalidade de evitar ou mitigar os efeitos da aplicação da lei penal, o juiz poderá determinar que as penas sejam aplicadas à pessoa jurídica que a suceder.

Art. 5º O desconhecimento institucional sobre a regulamentação da atividade é inescusável. O erro sobre a ilicitude da atividade, se inevitável, exclui a culpabilidade; se evitável, o juiz poderá diminuir a pena de um a dois terços.

Parágrafo único. Considera-se evitável o erro se a pessoa jurídica decide por realizar a atividade sem a compreensão de sua ilicitude, quando lhe era possível, nas circunstâncias, ter ou atingir essa compreensão.

Art. 6º A pessoa jurídica que, de qualquer modo, concorre para o crime de outra pessoa jurídica incide nas penas a este cominadas, na medida de sua própria culpabilidade.

Parágrafo único. Se a participação pessoa jurídica for de menor importância, o juiz poderá diminuir a pena de um a dois terços.

Art. 7º. As penas aplicáveis isolada, cumulativa ou alternativamente às pessoas jurídicas são:

I – multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição

²⁴ Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-permanentes/ccjc/apresentacoes-em-eventos/apresentacoes-de-convidados-em-eventos-de-2021/audiencia-publica-da-subcomissao-para-assuntos-penais-1/documentos-ap-subcomissao-assuntos-penais/17082021-apresentacao_-fernando-galvao. Acesso em: 3 de julho de 2024.

econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;

II – restritivas de direitos;

III – prestação de serviços à comunidade;

IV – liquidação forçada.

Art. 8º. As penas restritivas de direitos da pessoa jurídica são:

I – suspensão parcial ou total de atividades: quando estas estiverem relacionadas com a prática de crime cibernético.

II – interdição temporária de estabelecimento: quando este for utilizado para a prática de crime cibernético.

III – proibição de contratar com o Poder Público, bem como dele obter subsídios, subvenções ou doações, por até 10 anos.

Art. 9º. A prestação de serviços à comunidade pela pessoa jurídica consistirá em:

I – custeio de programas e projetos de tecnologia da informação, proteção de registros, dados pessoais e comunicações privadas, bem como contra cibercrimes e ataques cibernéticos em geral;

II – execução de programas e projetos de tecnologia da informação, proteção de registros, dados pessoais e comunicações privadas, bem como contra cibercrimes e ataques cibernéticos em geral.

Art. 10. As penas de natureza pecuniária serão calculadas de acordo com os seguintes parâmetros e critérios:

I – gravidade e natureza das infrações e dos direitos pessoais afetados;

II – boa-fé do infrator;

III – vantagem auferida ou pretendida pelo infrator;

IV – condição econômica do infrator;

V – reincidência;

VI – grau de dano;

VII – cooperação do infrator;

VIII – adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano;

IX – adoção de política de boas práticas e governança;

X – pronta adoção de medidas corretivas;

IX – proporcionalidade entre a gravidade da falta e a intensidade da sanção.

Art. 11. As penas restritivas de direitos e a de execução de programas e projetos serão calculadas tendo como base a pena privativa de liberdade prevista em abstrato no(s) crime(s) imputado(s) à pessoa jurídica, devendo-se aplicar os mesmos critérios de aplicação da pena previstos no Capítulo III, da Parte Geral, do Código Penal.

Art. 12. A pessoa jurídica constituída ou utilizada, preponderantemente, com o fim de permitir, facilitar ou ocultar a prática de cibercrime, na forma do art. 1º, terá decretada sua liquidação forçada, seu patrimônio será considerado instrumento do crime e como tal perdido em favor do Fundo Penitenciário Nacional.

Art. 13. Em qualquer fase da investigação criminal ou do processo penal, caberão, por determinação judicial, de ofício ou a requerimento do Ministério Público, do querelante, do assistente de acusação, ou por representação da autoridade policial, como garantia da ordem pública, da ordem econômica, por conveniência da instrução criminal ou para assegurar a aplicação da lei penal, quando houver indícios suficientes da existência do crime cibernético e de sua autoria, desde que adequada(s) à gravidade do crime e às circunstâncias do fato, as seguintes medidas cautelares:

I – suspensão parcial de atividade;

II – interdição temporária de estabelecimento;

III – proibição de contratar com o Poder Público, bem como dele obter subsídios, subvenções ou doações;

IV - outras medidas indutivas, coercitivas, mandamentais ou sub-rogatórias necessárias.

Parágrafo único. As cautelares poderão ser aplicadas isolada, cumulativa ou alternativamente e serão mantidas pelo tempo que durar o risco à ordem

pública, à ordem econômica, à conveniência da instrução criminal e à aplicação da lei penal.

Art. 14. O órgão judicial, ao proferir sentença condenatória, fixará valor mínimo para reparação dos danos causados pela infração, considerando os prejuízos sofridos pela(s) vítima(s).

CONCLUSÃO

Crime cibernético é a infração penal praticada por meio de sistema informático, conectado ou não em rede; ou contra a segurança cibernética, notadamente com afronta à confidencialidade, integridade e disponibilidade de sistemas, redes e/ou dados informáticos; ou mediante a posse ou disponibilização dos meios para tais fins.

A criminalidade cibernética está em franca expansão, não respeita fronteiras e está a cada dia mais elaborada, o que dificulta sobremaneira as atividades de fiscalização, prevenção e repressão, cujo sucesso carece de uma intensa rede de cooperação internacional, com compartilhamento de informação e tecnologia, além de uma legislação anticrimes cibernéticos uniforme e eficaz, com o mínimo de brechas possíveis, pois estas certamente serão identificadas e utilizadas pelos cibercriminosos em favor deles, perpetuando, dessa forma, a atividade criminosa em tela.

Ciente desse risco, o Conselho da Europa aprovou, no dia 23 de novembro de 2001, na cidade de Budapeste, Hungria, a Convenção sobre o Cibercrime, que entrou em vigor no dia 1º de julho 2004, e conta com a adesão também de países de fora do bloco europeu, como Estados Unidos, Chile, Argentina, Costa Rica, República Dominicana e, enfim, Brasil, que ratificou a Convenção, por meio do Decreto Legislativo nº 37, no dia 21 de dezembro de 2021 (BRASIL, 2021), e internalizou-a em seu ordenamento jurídico, no dia 12 de abril de 2023, pelo Decreto nº 11.491. (BRASIL, 2023)

Dentre as medidas a serem adotadas a nível nacional, no âmbito do Direito Penal Material, a Convenção prevê, em seu artigo 12, a responsabilização penal das pessoas jurídicas.

O Brasil é capaz de cumprir o compromisso assumido em âmbito interno e internacional, no sentido de assegurar que as pessoas jurídicas sejam responsabilizadas penalmente pela prática de infrações cibernéticas, não havendo óbice constitucional para tanto.

Todavia, a matéria carece de regulamentação, que deve ser feita por lei federal, na forma dos artigos 5º, inciso XXXIX, e 22, inciso I, ambos da Constituição Federal.

Ademais, a lei federal regulamentadora deverá atribuir responsabilidade penal e fixar penas adequadas às pessoas jurídicas, de forma geral e abstrata, pela prática de crimes cibernéticos.

Imperioso destacar, ainda, que os crimes cibernéticos são dinâmicos e podem rapidamente gerar danos a uma grande quantidade de vítimas, caso não existam mecanismos legais que viabilizem uma contra ação rápida das autoridades competentes. Indispensável, portanto, que a lei regulamentadora também traga a previsão de cautelares específicas para a garantia da ordem pública, da ordem econômica, da conveniência da instrução criminal e, até mesmo, para assegurar a aplicação da lei penal.

Ademais, é importante que a lei, a exemplo do artigo 387, inciso IV, do Código de Processo Penal, permita que a sentença penal já fixe um valor mínimo para a reparação dos danos causados pela infração, considerando os prejuízos sofridos pelas vítimas.

Finalmente, embora o presente trabalho não pretenda esgotar a temática, buscase suscitar discussões e lançar luzes sobre a regulamentação da responsabilidade penal da pessoa jurídica pela prática de crimes cibernéticos, atentando para a cominação de penas adequadas, fixação de cautelares eficientes e previsão de ressarcimento de danos às vítimas.

REFERÊNCIAS

BRASIL. Decreto nº 11.491, de 12 de abril de 2023. Promulga a Convenção sobre Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001. Brasília/DF: Planalto, 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/Ato2023-2026/2023/Decreto/D11491.htm. Acesso em: 14 de janeiro de 2024.

BRASIL. Emenda Constitucional n 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoas entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília/DF: Planalto, 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#art1. Acesso em: 14 de janeiro de 2024.

BRASIL. Decreto Legislativo nº 37, de 2021. Aprova o texto da Convenção sobre Crime Cibernético, celebrada em Budapeste, em 23 de novembro de 2001. Brasília/DF: Planalto, 2021. Disponível em: <https://www.in.gov.br/en/web/dou/-/decreto-legislativo-368859089>. Acesso em: 14 de janeiro de 2024.

BRASIL. *Congresso ratifica acordo internacional sobre crimes cibernéticos*. Senado Federal (Agência Câmara de Notícias). Brasília/DF: Senado Federal, 2021. Disponível em: <https://www12.senado.leg.br/noticias/materias/2021/12/23/congresso-ratifica-acordo-internacional-sobre-crimes-ciberneticos>. Acesso em: dia 14 de janeiro de 2024.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília/DF: Planalto, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 14 de janeiro de 2024.

BRASIL. Recurso Extraordinário nº 548.181/PR. Supremo Tribunal Federal. Brasília/DF: Portal STF, 2013. Disponível em: <https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=7087018>. Acesso em: 16 de janeiro de 2024.

BRASIL. Recurso Especial nº 564.960/SC (2003/0107368-4). Superior Tribunal de Justiça. Brasília/DF: STJ, 2005. Disponível em: <https://processo.stj.jus.br/SCON/jurisprudencia/toc.jsp?livre=%28RESP.clas.+e+%40num%3D%22564960%22%29+ou+%28RESP+adj+%22564960%22%29.suce>. Acesso em: 14 de janeiro de 2024.

BRASIL. Lei nº 9.605, de 12 de fevereiro de 1998. Dispõe sobre as sanções penais e administrativas derivadas de condutas e atividades lesivas ao meio ambiente, e dá outras providências. Brasília/DF: Planalto, 1998. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/19605.htm. Acesso em: 14 de janeiro de 2024.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília/DF: Planalto, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 14 de janeiro de 2024.

BUSSELL, Jennifer. Cyberspace. Encyclopedia Britannica, 2023. Disponível em: <https://www.britannica.com/topic/cyberspace>. Acesso em: 31 de janeiro de 2024.

CNCS. Glossário. Centro Nacional de Cibersegurança – Portugal. Lisboa, 2022. Disponível em: <https://www.cncs.gov.pt/pt/glossario/#linhasobservacao>. Acesso em: 31 de janeiro de 2024.

COE. Convention on Cybercrime. Estrasburgo/GE: Concil of Europe Portal, 2001a. Disponível em: <https://rm.coe.int/1680081561>. Acesso no dia 14 de janeiro de 2024.

COE. Convention sur la cybercriminalité. Estrasburgo/GE: Concil of Europe Portal, 2001b. Disponível em: <https://rm.coe.int/168008156d>. Acesso em: 14 de janeiro de 2024.

CONDE, Francisco Muñoz; ARÁN, Mercedes García. *Derecho Penal: Parte General*. 3ª ed. Valencia: Tirant lo Blanch, 2010, p. 631.

FERREIRA, Ivete Senise. *A criminalidade informática*. Direito & Internet: Aspectos Jurídicos Relevantes. São Paulo: Edipro, 2001.

FIGUEIREDO, Guilherme José Purvin de; SILVA, Solange Teles da. Responsabilidade Penal das Pessoas Jurídicas de Direito Público na Lei nº 9.605/98. *Revista de Direito da Procuradoria Geral*. Rio de Janeiro/RJ: Coordenadoria de Pesquisa e Publicações Científicas do CEJUR, 1998. Disponível em: <https://pge.rj.gov.br/comum/code/MostrarArquivo.php?C=MTkxOA%2C%2C>. Acesso em: 14 de janeiro de 2024.

GONTIJO, Cynthia Rúbia Braga, et. al. *Ciberespaço: que território é esse?* Educ. Tecnol., Belo Horizonte, v. 12, n. 3, pp. 34-38, set./dez., 2007.

GIBSON, William. *Neuromancer*. Tradução de Abdoule Sam Byd e Lumir Nahodil. São Paulo/SP: Ace Books, 2003.

JAISHANKAR, Karuppannan. Space transition theory of cybercrimes. In: Schmallager, F., & Pittaro, M. (Eds.), *Crimes of the internet*. Upper Saddle River/NJ: Prentice Hall, 2008, pp. 283-301. Disponível em: <https://www.jaishankar.org/theory.html#:~:text=The%20postulates%20of%20the%20theory,to%20their%20status%20and%20position>. Acesso em: 3 de julho de 2024.

JESCHECK, Hans-Heinrich. *Tratado de Derecho Penal*. Tradução da 4ª ed. Tradução de José Luis Manzanares Samaniego. Granada: Comares, 1993, p. 300.

JUNGBLUT, Airton Luiz. A heterogenia do mundo on-line: algumas reflexões sobre a virtualização, comunicação mediada por computadores e ciberespaço. In: *Horizontes Antropológicos*. Porto Alegre, ano 10, n. 21, jan./jun., 2004, pp. 97-121.

JÚNIOR, Mário José Lopes Guimarães. O ciberespaço como cenário para as ciências sociais. *Ilha Revista de Antropologia*. Florianópolis/SC, v. 2, n. 1, p. 139-154, 2000. Disponível em: <https://periodicos.ufsc.br/index.php/ilha/article/view/14652>. Acesso em: 3 de julho de 2024.

KIM, Joon Ho. Cibernética, ciborgues e ciberespaço: notas sobre as origens da cibernética e sua reinvenção cultural. In: *Horizontes Antropológicos*. Porto Alegre, ano 10, n. 21, pp. 199-219, jan./jun., 2004.

LÉVY, Pierre. *Cibercultura*. Tradução de Carlos Irineu da Costa. São Paulo: Editora 34, 2000.

MORAIS NETO, Arnaldo Sobrinho de Moraes. *Cybercrime e cooperação penal internacional: um enfoque à luz da Convenção de Budapeste*. Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Ciências Jurídicas da Universidade Federal da Paraíba – UFPB Centro de Tecnologia, João Pessoa/PA, 2009. Disponível em: <http://www.ct.ufpb.br/pos/contents/pdf/bibliovirtual/dissertacoes-2009/arnaldo->

[sobrinho-cibercrime-e-cooperacao-penal-internacional.pdf](#). Acesso em: 30 de janeiro de 2024.

MURATA, Ana Maria Lumi Kamimura; TORRES, Paula Ritzmann. Convenção de Budapeste sobre os crimes cibernéticos foi promulgada, e agora? *Boletim IBCCRIM*. Paulo/SP: IBCCRIM, ano 31, nº 368, junho, 2023. ISSN 1676-3661. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/575/108. Acesso em: 3 de julho de 2024.

PHILLIPS, Kirsty; DAVIDSON, Julia C.; FARR, Ruby R.; BURKHARDT, Christine; CANEPPELE, Stefano; AIKEN, Mary P. Conceptualizing cybercrime: definitions, typologies and taxonomies. *Forensic Sciences*, 2022, pp. 379-398. Disponível em <https://doi.org/10.3390/forensicsci2020028>. Acesso em: 3 de julho de 2024.

ROCHA, Fernando Antônio Nogueira Galvão da. *Estudos sobre responsabilidade penal de pessoas jurídicas*. Belo Horizonte/MG: Editora Dialética, 2023. ISBN 978-65-252-9698-2.

ROCHA, Fernando Antônio Nogueira Galvão da. *Teoria do crime da pessoa jurídica*. Proposta para a Câmara – Código Penal. Comissão de Constituição e Justiça e de Cidadania da Câmara dos Deputados. Brasília/DF: Portal da Câmara, 2021. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-permanentes/ccjc/apresentacoes-em-eventos/apresentacoes-de-convidados-em-eventos-de-2021/audiencia-publica-da-subcomissao-para-assuntos-penais-1/documentos-ap-subcomissao-assuntos-penais/17082021-apresentacao_-fernando-galvao. Acesso em: 3 de julho de 2024.

ROCHA, Fernando Antônio Nogueira Galvão da. *Responsabilidade Penal da Pessoa Jurídica*. 4ª. ed. Belo Horizonte/MG: Editora D'Plácido, 2017.

ROSSINI, Augusto Eduardo de Souza. *Informática, telemática e direito penal*. São Paulo/SP: Memória Jurídica, 2004.

SCHMITT, Michael N. *Tallinn manual on the international law applicable to cyber warfare: prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence*. Cambridge: Cambridge University Press, 2013. Disponível em: <https://www.onlinelibrary.iihl.org/wp-content/uploads/2021/05/2017-Tallinn-Manual-2.0.pdf>. Acesso no dia 31 de janeiro de 2024.

SYDOW, Spencer Toth. *Curso de Direito Penal Informático: Partes Geral e Especial*. 3ª ed. São Paulo/SP: Juspodivm, 2022.

UE. Diretiva 2013/40/UE do Parlamento Europeu e do Conselho de 12 de agosto de 2013: relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho. *Jornal da União Europeia*. Bruxelas, 2013. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32013L0040>. Acesso em: 3 de julho de 2024.

UK. The Queen against The Birmingham and Gloucester Railway Company. English Reports Citation: 114 E.R. 21, 1º de jan. de 1842. Disponível em: <https://vlex.co.uk/vid/the-queen-against-the-803443733>. Acesso em: 3 de julho de 2024.

USA. *Internet Crime Report 2022*. Washington/DC: Department of Justice – Federal Bureau of Investigation, 2022. Disponível em: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf. Acesso em: 3 de julho de 2024.

USA. *Internet Crime Report 2021*. Washington/DC: Department of Justice – Federal Bureau of Investigation, 2021. Disponível em: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf. Acesso em: 3 de julho de 2024.

USA. New York Central & Hudson River Railroad Co. v. United States, 212 U.S. 481. U.S. Supreme Court. Washington/DC: Justia U.S. Supreme Court, 1909. Disponível em: <https://supreme.justia.com/cases/federal/us/212/481/>. Acesso em: 3 de julho de 2024.

USA. Security and Privacy Controls for Information Systems and Organizations. *NIST (National Institute of Standards and Technology)*. Washington/DC: U.S. Department of Commerce, rev. 5, 2020. Disponível em: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>. Acesso em: 3 de julho de 2024.