VIII ENCONTRO VIRTUAL DO CONPEDI

DIREITO PENAL, PROCESSO PENAL E CONSTITUIÇÃO IV

Copyright © 2025 Conselho Nacional de Pesquisa e Pós-Graduação em Direito

Todos os direitos reservados e protegidos. Nenhuma parte destes anais poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

Diretoria – CONPEDI
Presidente - Profa. Dra. Samyra Haydêe Dal Farra Naspolini - FMU – São Paulo
Diretor Executivo - Prof. Dr. Orides Mezzaroba - UFSC – Santa Catarina
Vice-presidente Norte - Prof. Dr. Jean Carlos Dias - Cesupa – Pará
Vice-presidente Centro-Oeste - Prof. Dr. José Querino Tavares Neto - UFG – Goiás
Vice-presidente Sul - Prof. Dr. Leonel Severo Rocha - Unisinos – Rio Grande do Sul
Vice-presidente Sudeste - Profa. Dra. Rosângela Lunardelli Cavallazzi - UFRJ/PUCRio – Rio de Janeiro
Vice-presidente Nordeste - Prof. Dr. Raymundo Juliano Feitosa - UNICAP - Pernambuco

Representante Discente: Prof. Dr. Abner da Silva Jaques - UPM/UNIGRAN - Mato Grosso do Sul

Conselho Fiscal:
Prof. Dr. José Filomeno de Moraes Filho - UFMA - Maranhão
Prof. Dr. Caio Augusto Souza Lara - SKEMA/ESDHC/UFMG - Minas Gerais
Prof. Dr. Valter Moura do Carmo - UFERSA - Rio Grande do Norte
Prof. Dr. Fernando Passos – UNIARA - São Paulo
Prof. Dr. Edinilson Donisete Machado - UNIVEM/UENP - São Paulo
Secretarias
Relações Institucionais:
Prof. Dra. Claudia Maria Barbosa - PUCPR - Paraná
Prof. Dr. Heron José de Santana Gordilho - UFBA - Bahia
Profa. Dra. Daniela Marques de Moraes - UNB - Distrito Federal
Comunicação:
Prof. Dr. Robison Tramontina - UNOESC - Santa Catarina
Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali - Rio Grande do Sul
Prof. Dr. Lucas Gonçalves da Silva - UFS - Sergipe
Relações Internacionais para o Continente Americano:
Prof. Dr. Jerônimo Siqueira Tybusch - UFSM - Rio Grande do sul
Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA - Maranhão
Prof. Dr. Felipe Chiarello de Souza Pinto - UPM – São Paulo
Relações Internacionais para os demais Continentes:
Profa. Dra. Gina Vidal Marcilio Pompeu - UNIFOR - Ceará
Profa. Dra. Sandra Regina Martini - UNIRITTER / UFRGS - Rio Grande do Sul
Profa. Dra. Maria Claudia da Silva Antunes de Souza - UNIVALI – Santa Catarina
Educação Jurídica
Profa. Dra. Viviane Coêlho de Séllos Knoerr - Unicuritiba - PR
Prof. Dr. Rubens Beçak - USP - SP
Profa. Dra. Livia Gaigher Bosio Campello – UFMS – MS
Eventos:
Prof. Dr. Yuri Nathan da Costa Lannes - FDF - São Paulo
Profa. Dra. Norma Sueli Padilha - UFSC - Santa Catarina
Prof. Dr. Juraci Mourão Lopes Filho - UNICHRISTUS - Ceará

Comissão Especial
Prof. Dr. João Marcelo de Lima Assafim - UFRJ - RJ
Profa. Dra. Maria Creusa De Araújo Borges - UFPB - PB
Prof. Dr. Antônio Carlos Diniz Murta - Fumec - MG
Prof. Dr. Rogério Borba - UNIFACVEST - SC

D597

Direito penal, processo penal e constituição IV [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Carolina Angelo Montoli; Luiz Gustavo Gonçalves Ribeiro; Matheus Felipe De Castro. – Florianópolis: CONPEDI, 2025.

Inclui bibliografia
ISBN: 978-65-5274-169-1
Modo de acesso: www.conpedi.org.br em publicações
Tema: Direito Governança e Políticas de Inclusão

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito penal. 3. Processo penal. VIII Encontro Virtual do CONPEDI (2; 2025; Florianópolis, Brasil).

CDU: 34

CONPEDI

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

VIII ENCONTRO VIRTUAL DO CONPEDI

DIREITO PENAL, PROCESSO PENAL E CONSTITUIÇÃO IV

Apresentação

Em uma tarde de Sábado, no início do inverno brasileiro, o Grupo de Trabalho Direito Penal, Processo Penal e Constituição IV reuniu-se com o escopo de debater temas modernos e interdisciplinares das Ciências Penais, que resultou na confirmação de que o Conpedi é, há algum tempo, uma associação que contempla grandes profissionais, docentes e acadêmicos do direito. Com grande capacidade crítica, os estudiosos de ecléticos temas do universo do direito e do processo penal, corroboraram o sucesso dos eventos remotos do Conselho Nacional de Pesquisa e Pós-Graduação em Direito. Diversas Instituições, de norte a sul do país, estiveram representadas nos debates, culminando com um livro, de consulta imprescindível, que é composto dos seguintes artigos/capítulos, ora apresentados por título, autoria e síntese:

No primeiro artigo, intitulado "METAVERSO E CRIMINALIDADE: FRONTEIRAS DA RESPONSABILIZAÇÃO PENAL NO ESPAÇO DIGITAL", os autores Cristian Kiefer Da Silva e Rafaela Cristina Alves Lisboa investigam as complexas fronteiras da responsabilização penal no contexto do metaverso, ambiente virtual imersivo que inaugura novas formas de interação social, econômica e comportamental. A pesquisa explora as dificuldades na persecução penal, incluindo a tipificação de condutas, a coleta de provas digitais e a determinação de jurisdição em espaços virtualizados. Além disso, examina os impactos desses crimes na proteção de direitos fundamentais, como privacidade, liberdade de expressão e propriedade. Destaca-se que a natureza peculiar do Metaverso requer uma adaptação profunda dos instrumentos penais, de modo a estabelecer um sistema sancionador proporcional que, sem abdicar da necessária eficácia repressiva, assegure plenamente o respeito aos direitos e garantias fundamentais, delineando, assim, os contornos de uma

ambientais. O estudo destaca que a impunidade, definida como a falta de investigação, acusação, julgamento e condenação dos responsáveis por violações dos direitos protegidos, fomenta a reincidência e a desproteção das vítimas e seus familiares. Destaca-se, como objetivo, a urgência de combater a impunidade e fortalecer a proteção ambiental na Amazônia Legal, através de uma abordagem integrada que envolva a responsabilização dos criminosos, o fortalecimento das instituições e o desenvolvimento sustentável das comunidades locais.

O terceiro trabalho que compõe o livro é intitulado “A ATUAÇÃO JURISDICIONAL E PROCESSUAL DO PODER PÚBLICO NA GARANTIA DOS DIREITOS DA MULHER PRESIDIÁRIA” e tem como autores Tammara Drummond Mendes, Roberto Apolinário de Castro e Renata Apolinário de Castro Lima. A pesquisa explora a análise das situações prisionais e estatísticas com base de dados em relação ao encarceramento de mulheres no Brasil. Também é abordada a situação de mulheres na situação especial de prisão em tempos de gravidez e a violação de seus direitos enquanto pessoa do sexo feminino. Explora-se formas de garantir o cumprimento dos direitos e interesses das detentas reclusas no sistema prisional brasileiro em conformidade com a Lei de Execuções Penais, buscando-se medidas eficazes de ressocialização das mesmas e a não violação ou o mínimo cerceamento possível de seus direitos fundamentais.

No trabalho intitulado “A APLICAÇÃO DO PRINCÍPIO DA PROPORCIONALIDADE NA ADMISSIBILIDADE DE PROVAS ILÍCITAS NO PROCESSO PENAL BRASILEIRO: UMA ANÁLISE CRÍTICA”, o autor Jônatas Peixoto Lopes analisa a problemática da admissibilidade excepcional de provas ilícitas no processo penal brasileiro, com enfoque na aplicação do princípio da proporcionalidade como critério de ponderação entre direitos fundamentais conflitantes. A Constituição Federal de 1988, em seu artigo 5º, LVI, estabelece expressamente a inadmissibilidade das provas obtidas por meios ilícitos. Contudo, a interpretação sistemática do texto constitucional e o reconhecimento de que nenhum direito fundamental é absoluto têm fomentado intenso debate doutrinário e jurisprudencial sobre

O trabalho seguinte, intitulado “TEORIA DA LATITUDE E LONGITUDE DO DIREITO PENAL”, tem como autor Liciomar Fernandes da Silva, o mesmo que introduz e desenvolve a teoria a partir de uma análise crítica das práticas policiais, especialmente no contexto do Brasil. A teoria aborda a realidade de agentes de segurança pública no que se refere à alteração de locais e horários dos fatos para simular realidades distintas daquelas efetivamente ocorridas, impactando diretamente na persecução penal e na formação da verdade processual. Com base em revisão doutrinária e análise empírica, evidencia-se que tais práticas violam direitos fundamentais e comprometem o devido processo legal, o contraditório e a ampla defesa. O trabalho destaca a necessidade da utilização obrigatória de tecnologias como o GPS e câmeras corporais para garantir maior transparência e controle da atividade policial. A teoria se distingue de conceitos como o flagrante preparado e os frutos da árvore envenenada, enfocando a alteração espacial e temporal como elemento central da fraude processual. O trabalho revela que a falta de controle e a cultura punitivista institucionalizada favorecem a perpetuação de práticas ilícitas e o enfraquecimento do Estado de Direito. Propõe-se uma reorientação institucional em favor da legalidade, da proteção dos direitos fundamentais e da reconstrução da confiança pública nas instituições jurídicas.

O sexto artigo, intitulado “TEORIA DA PROVA: PROVAS ILÍCITAS”, da autora Ana Luzia Barbosa Fernandes Braúna, revela que a teoria da prova, para além de fomentar o debate sobre a busca da verdade com o fim de realização da justiça, e a forma como a prova afeta as decisões judiciais em processos criminais, revela também uma opção de política criminal ao estabelecer fatores necessários que limitam e condicionam a busca da verdade. Os limites impostos à produção e apreciação da prova são salvaguarda de direitos fundamentais, e sua violação implica na obtenção de provas proibidas, ou provas ilícitas, imprestáveis à instrução processual. A teoria das provas ilícitas, entretanto, comporta flexibilizações com fundamento na teoria da ponderação. Estabelece-se, então, um debate acerca dos institutos jurídico-penais, a partir da compreensão e distinção do modelo acusatório, para avaliação da eficiência, eficácia e efetividade dos postulados que constituem a Teoria a prova, perquirindo-se se há conformação institucional das soluções jurídicas

trabalho problematiza se o Conselho de Sentença é efetivamente representativo quanto à realidade socioeconômico-cultural do Brasil, e tem como objetivo geral analisar se o processo de seleção e composição do corpo de jurados brasileiro é representativo e se a implementação de elementos do júri estadunidense pode aprimorar o sistema brasileiro. A pesquisa, ao ser concluída, demonstrou que o Conselho de Sentença brasileiro não reflete a diversidade socioeconômico-cultural do país e que a implementação dos elementos estadunidenses venire e voir dire, pode contribuir para a representatividade do corpo de jurados brasileiro.

O oitavo artigo, intitulado "O SEQUESTRO DA DIGNIDADE E O HUMANISMO DE RESISTÊNCIA: A BASE NORMATIVA PARA O CÔMPUTO EM DOBRO DA PENA PRIVATIVA DE LIBERDADE EM CONDIÇÕES ULTRAJANTES", dos autores Maicke Oliveira Santos, Tatiany Nascimento Chagas e Carlos Augusto Alcântara Machado, tem como objetivo analisar se o cômputo em dobro da pena privativa de liberdade em condições degradantes possui base normativa ou principiológica que consubstancie sua aplicabilidade como resposta possível frente ao Estado de Coisas Inconstitucional (ECI) no sistema prisional brasileiro, o qual, em 2015, foi reconhecido pelo Supremo Tribunal Federal (STF) na Arguição de Descumprimento de Preceito Fundamental (ADPF) n.º 347. Ou seja, parte do problema se a ausência de lei formal tratando sobre a temática é fundamento válido para obstar a medida compensatória no país. Ademais, almeja verificar se a decisão que declarou o ECI é uma resposta da Corte Constitucional Brasileira a um Estado sem compromisso com o respeito à dignidade, resistindo, humanamente, contra os excessos cometidos no sistema carcerário, correlacionando, assim, as nomenclaturas "sequestro da dignidade" e "humanismo de resistência".

O nono artigo, que tem por título "A INTEGRIDADE DA VERDADE POR TRÁS DAS DECISÕES DO TRIBUNAL DE JUSTIÇA DO PARANÁ: A JURISPRUDÊNCIA SOBRE A QUEBRA DA CADEIA DE CUSTÓDIA NO ANO DE 2023", dos autores João Vitor Jahjah e Bruna Azevedo de Castro, externa que o processo penal, para além de instrumento

pesquisa analisa a integridade das provas que consubstanciam as decisões do Tribunal de Justiça do Paraná pela fundamentação sobre a cadeia de custódia, buscando aferir a fiabilidade dos vestígios pelos quais se reconstrói o fato imputado ao réu.

O texto “PRESUNÇÃO DE INOCÊNCIA E O PROCESSO ADMINISTRATIVO DISCIPLINAR NA LEI DE EXECUÇÃO PENAL: UMA ANÁLISE CRÍTICA”, escrito por Lucas Pereira Carvalho De Brito Mello e Elisa Girotti Celmer, analisa a presunção de inocência no contexto do Processo Administrativo Disciplinar (PAD) no âmbito da Lei de Execução Penal (LEP). A presunção de inocência é princípio expresso no texto da Constituição Federal de 1988 e enfrenta desafios particulares quando aplicada aos processos administrativos disciplinares no sistema prisional. A distinção clássica entre esferas administrativa e penal se mostra distorcida e insuficiente, na medida em que as sanções impostas no âmbito disciplinar afetam diretamente o status libertatis do apenado. Neste trabalho, busca-se compreender a interseção entre a presunção de inocência e o Processo Administrativo Disciplinar (PAD), explorando suas nuances, desafios e implicações no contexto da execução penal. A lógica de “pune-se agora, revê-se depois” em caso de absolvição no processo penal superveniente compromete o ideal de justiça e o próprio propósito do processo penal como instrumento de contenção do arbítrio estatal.

Em “O PAPEL DOS CARTÓRIOS NO COMBATE À LAVAGEM DE DINHEIRO”, a autora Elina Magnan Barbosa revela que, para o combate e prevenção à lavagem de dinheiro, em virtude da alta complexidade do delito, foi necessária, além das recomendações de Convenções internacionais voltadas aos seus países-signatários, a criação de uma força tarefa internacional – FATF-GAFI. Esta, por sua vez, vislumbrou a necessidade da implementação de recomendações voltadas não só a atividades financeiras, mas, também, a empresas e profissões não financeiras designadas, dentre elas a dos tabeliães/notários e registradores. Concluiu-se que, apesar do relevante papel dos cartórios no combate ao branqueamento de divisas, existe ainda certa relutância quanto ao envio de comunicações referentes a atividades suspeitas à Unidade de Inteligência Financeira, em razão do princípio da confiança e do

com transtornos mentais. A problemática se refere à regulação da Política Antimanicomial pelo Conselho Nacional de Justiça. A regulação se faz necessária para cumprimento da Convenção Internacional dos Direitos das Pessoas com Deficiência e a Lei n. 10.216/2001, bem como pela necessidade de redirecionamento do modelo assistencial em saúde mental. Os resultados esperados são referentes à necessidade de regulação pelo Estado Brasileiro das cláusulas da Convenção Internacional dos Direitos das Pessoas com Deficiência e decorrentes da Lei n. 10.216/200, visando modificar, alterando ou revogando normas que constituam discriminação contra pessoas com deficiência.

Na pesquisa intitulada “ENTRE O GUETO E A CELA: A CRIMINALIZAÇÃO DA POBREZA”, Eneida Orbage De Britto Taquary, Aimeê Giovana Heffel e Maria Luisa Monteiro de Paula Melo analisam como a desigualdade socioeconômica, em sua forma de pobreza, e a marginalização histórica influenciam diretamente o aumento da criminalidade, fazendo um paralelo entre os criminalistas Roxin, Zaffaroni, Vera Malaguti e Gunther Jakobs. O artigo critica a seletividade penal, frequentemente com enfoque punitivo na pobreza, e sua contribuição para a perpetuação dos ciclos de criminalidade, além de defender uma atuação estatal assertiva e com políticas públicas de inclusão e reinserção do agente na sociedade. O problema se refere a seletividade sistêmica utilizada como critério para a punir a pobreza, mais do que o ato criminoso propriamente dito, e como esta se estrutura como critério determinante para a existência de uma sociedade com um exacerbado número carcerário. A hipótese decorre das estratégias estatais para se combater a criminalidade, não apenas punindo o indivíduo, mas compreendendo suas raízes sociais e oferecendo-lhes oportunidades para sair da marginalidade. Como resultado esperado, busca-se compreender que a criminalidade não é um fenômeno isolado, mas sim um reflexo do sistema e da marginalização de determinados grupos sociais. Evidenciando ainda que o aspecto punitivo apenas como resposta estatal é ineficaz, devendo se estabelecer uma resposta mais assertiva e voltada para políticas públicas.

Em “CONTROVÉRSIAS SOBRE A COMPROVAÇÃO DO CRIME DE EMBRIAGUEZ

necessidade de lavratura do Termo de Constatação de Embriaguez para comprovar o crime previsto no art. 306, do Código de Trânsito Nacional, pelos agentes públicos; a distinção entre a prova produzida pela lavratura do Termo de Constatação de Embriaguez e a prova testemunhal e ainda a aceitabilidade do Termo de Constatação de Embriaguez pelos Tribunais Brasileiros como prova cabal do crime. O resultado esperado se restringe a verificar que o Termo de Constatação de Embriaguez é suficiente para comprovar o crime previsto no art. 306, do Código de Trânsito Nacional.

Na pesquisa denominada "OS IMPACTOS DA DECISÃO DAS AÇÕES DIRETAS DE INCONSTITUCIONALIDADE (ADI'S 6298, 6299, 6300 E 6305) PARA A IMPARCIALIDADE DO JUIZ DE GARANTIAS", Laura Massud Machado, Rafaella Santana Dias Simões e Diego Fajardo Maranha Leao De Souza revelam que a decisão do Supremo Tribunal Federal nas ADI's 6298, 6299, 6300 e 6305 trouxe modificações significativas para o juiz de garantias. O objetivo do estudo foi analisar os impactos dessa decisão para a imparcialidade do instituto, uma vez mudada a redação legal do artigo 3º-C do Código de Processo Penal, por meio de alteração na Lei 13.964/19, que substituiu a palavra "recebimento" por "oferecimento", estabelecendo a partir dela que a competência do juiz de garantias cessa com o oferecimento da denúncia. O trabalho avalia os efeitos causados na imparcialidade processual por conta dessa decisão, conceituando o juiz de garantias, trazendo análises da sua aplicação tanto no âmbito nacional quanto internacional e os reflexos jurídicos da atuação Plenária em matéria legislativa, a fim de questionar se a imparcialidade processual do juiz de garantias foi afetada negativamente. Ao final, conclui-se ter sido prejudicada a eficácia do objetivo de imparcialidade do instituto do Juiz de Garantias, por conta do cenário de insegurança jurídica gerado a partir da intervenção judicial.

Por fim, em "DECRETO 11.491/2023, RESPONSABILIDADE PENAL DA PESSOA JURÍDICA POR CRIMES CIBERNÉTICOS E COMPLIANCE", os autores Mateus Eduardo Siqueira Nunes Bertoncini e Glaucio Antônio Pereira Filho expõem que o estudo tem como foco o Decreto 11.491/2023, que promulgou a Convenção de Budapeste no

identificação da matriz de risco específico da seara cibernética. Ao fim, propõe-se formas concretas de aprimoramento dos programas de integridade empresarial, à luz do aludido marco normativo internacional.

Observa-se, portanto, que se tratam de trabalhos ecléticos e atuais e que, por certo, se lidos e compreendidos, oferecerão uma grande contribuição para o avanço das práticas e políticas necessárias para o aperfeiçoamento das ciências criminais no Brasil.

Por fim, nós, organizadores do livro, convidamos todos para uma leitura aprazível e crítica de todos os textos.

Inverno de 2024.

Professora Doutora Carolina Angelo Montoli, Fundação João Pinheiro – Escola de Governo. Email: carolinamontolli@gmail.com

Professor Doutor Matheus Felipe De Castro, Universidade Federal de Santa Catarina. Email: matheusfelipedecastro@gmail.com

Professor Doutor Luiz Gustavo Gonçalves Ribeiro, Centro Universitário Dom Helder. Email: lgribeirobh@gmail.com

DECRETO 11.491/2023, RESPONSABILIDADE PENAL DA PESSOA JURÍDICA POR CRIMES CIBERNÉTICOS E COMPLIANCE

DECREE 11.491/2023, CRIMINAL LIABILITY OF LEGAL ENTITIES FOR CYBERCRIMES AND COMPLIANCE

Mateus Eduardo Siqueira Nunes Bertoncini [1]
Glaucio Antonio Pereira Filho [2]

Resumo

O presente estudo tem como foco o Decreto 11.491/2023, que promulgou a Convenção de Budapeste no ordenamento jurídico brasileiro, prevendo expressamente a responsabilidade penal da pessoa jurídica na seara da "cibercriminalidade". Assim, será possível averiguar em que medida os sistemas de compliance empresariais poderão se adaptar à este novo regramento. Através do método hipotético-dedutivo, com análises primordialmente doutrinárias, a pesquisa perpassa pela análise dos crimes cibernéticos e suas espécies. Ainda, aborda a estrutura da Convenção, com ênfase na previsão de responsabilidade penal das pessoas jurídicas (objetiva, por falha organizacional ou de supervisão), porém carente de legislação penal específica, bem como nos instrumentos transnacionais de repressão e prevenção a ilícitos informáticos. Ademais, expõe os sistemas de compliance nesta seara, seus elementos e pressupostos, tal qual a identificação da matriz de risco específico da seara cibernética. Ao fim, propõe-se formas concretas de aprimoramento dos programas de integridade empresarial, à luz do aludido marco normativo internacional.

Palavras-chave: Convenção de budapeste, Decreto 11.491/2023, Crimes cibernéticos, Responsabilidade penal da pessoa jurídica, Compliance

Abstract/Resumen/Résumé

This study focuses on Decree 11,491/2023, which enacted the Budapest Convention into the Brazilian legal system, expressly providing for the criminal liability of legal entities in the area of "cybercrime". Thus, it will be possible to determine to what extent corporate compliance systems can adapt to this new regulation. Using the hypothetical-deductive

compliance systems in this area, their elements and assumptions, such as the identification of the specific risk matrix of the cyber area. Finally, concrete ways of improving corporate integrity programs are proposed, in light of the aforementioned international regulatory framework.

Keywords/Palabras-claves/Mots-clés: Budapest convention, Decree 11,491/2023, Cybercrimes, Criminal liability of legal entities, Compliance

1 INTRODUÇÃO

A internet e os *softwares* permeiam quase todas as esferas da vida cotidiana, mormente empresarial. Do lazer à gestão financeira das pessoas naturais e jurídicas, o uso de computadores, "smatphones" e outros periféricos, conectados à rede mundial de computadores, é maciço e ininterrupto.

A humanidade passa pela chamada "quarta revolução industrial" (Schwab, 2016), acelerada pelo uso da inteligência artificial (Siqueira, Lara, 2020, p. 302). Por isso, a segurança cibernética tornou-se uma prioridade global.

Segundo Robert Spadinger (2018), a Internet é onipresente, tanto na vida individual, como forma de entretenimento ou comunicação, quanto nas corporações e serviços públicos governamentais. E nos próximos anos veremos a contínua expansão da Internet e de seus serviços associados em todos os setores. Conclui o autor que o mundo se transforma cada vez mais em uma grande rede, maior, mais conectada, disponível em qualquer lugar e aparelho, permitindo uma infinidade de atividades pessoais e profissionais.

Nesse contexto, a Convenção de Budapeste sobre Crimes Cibernéticos, adotada pelo Conselho da Europa em 2001, destaca-se como um marco normativo crucial. Com a promulgação do Decreto 11.491/2023, que formaliza a adesão concreta do Brasil a Convenção, incorporando-a a nosso sistema normativo, surgem novos instrumentos jurídicos a serem observados pelos sistemas empresariais de integridade (compliance), em face dos ilícitos aludidos.

Assim, o objetivo precípuo do presente trabalho é averiguar em que medida a aludida Convenção pode causar impacto sobre os sistemas de compliance, na seara da *cibercriminalidade*. Será possível vislumbrar possibilidades de adequação dos programas de integridade, conferindo maior eficiência na gestão dos riscos inerentes à atuação digital.

Para tanto, serão analisados os crimes cibernéticos e suas espécies. Ainda, de relevo perquerir as origens da Convenção, bem como a estrutura do Decreto 11.491/2023, enfatizando-se seus instrumentos de prevenção e repressão, mormente transnacionais.

Aquilatando a relevância do tema, frise-se que neste Diploma inseriu-se a previsão de responsabilidade penal das pessoas jurídicas pelos crimes cibernéticos, inclusive mediante subsunção objetiva ou advinda de falha organizacional (bem como de ausência/deficiência de supervisão do agente criminoso). Há que se enfrentar tal tema, que levanta controvérsias doutrinárias e encontra avançadas normas em ordenamentos jurídicos de outros países.

Disto, considerando a adesão do Brasil à necessária responsabilização penal das pessoas jurídicas (ao menos quanto aos crimes cibernéticos), inevitável o aprimoramento dos programas de integridade, para que acompanhem a sofisticação deste tipo de delinquência. Nesta senda, se se faz relevante identificar os elementos e pressupostos dos sistemas de compliance, para que se especifique suas nuances na gestão de riscos informáticos.

Ao cabo, será possível apontar, concretamente, possibilidades de adequação dos controles internos de conformidade corporativos ao disposto na Convenção de Budapeste.

Para tanto, far-se-á abordagem doutrinária acerca dos temas, empregando-se o método hipotético-dedutivo.

2 CRIMES CIBERNÉTICOS

Os crimes cibernéticos são condutas tipificadas penalmente, em que o computador seja utilizado como instrumento de sua perpetração ou consistir em seu objeto material (ROQUE, 2007).

Nos crimes informáticos impróprios, os meios digitais são usados como instrumento delitivo. O fim de proteção da norma não é a inviolabilidade da informação automatizada de dados, mas bens jurídicos diversos e, corriqueiramente, tradicionais (Guaragni, Rios, 2019). O exemplo típico é o estelionato por meio virtual, com criação de *websites* falsos visando angariar doações.

Já nos crimes próprios, a informática (segurança dos sistemas, titularidade das informações, integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado (Jesus, Milagre, 2016). Cite-se os delitos tipificados nos arts. 313-A e 313-B do Código Penal (inserção de dados falsos em sistema de informações e modificação ou alteração não autorizada de sistema de informações).

A difusão destas condutas em escala mundial é alarmante, com considerável potencial danoso. Há diversos exemplos dos danos globais causados por tais condutas no ambiente virtual: caso “Ashley Madison” com vazamento de milhares de dados sigilosos de usuários (Jacob, 2024), extorsão virtual da empresa JBS por ataque *hacker* (G1, 2021), uso indevido de dados pessoais de milhões de pessoas para fins eleitorais, pela empresa Cambridge Analytica, em diversos países (BBC, 2018), etc.

Dentre os crimes informáticos mais cometidos cotidianamente, destaca-se: plágio (art. 184 do Código Penal), invasão de dispositivo e furto de dados (arts. 154-A), furto qualificado

por dispositivo eletrônico ou informático (155, §4º-B do Código Penal), delitos contra a honra (calúnia, injúria e difamação), apologia e incitação ao crime (arts. 287 e 286 do Código Penal), pornografia infantil (art. 240 do Estatuto da Criança e do Adolescente), racismo (Lei 7.716/89), divulgação de cena de estupro, ou estupro de vulnerável, de cena de sexo ou de pornografia (art. 218-C do Código Penal), criação de perfil "fake" para obter vantagem ou causar dano (art. 307 do Código Penal), dentre outros (Assis, 2019).

Reafirme-se ainda que a inteligência artificial agrava consideravelmente a repercussão e alcance de tais ilícitos (reprodução em larga escala de "phishing", "ransonware", ataques DDos, etc) (MPMT, 2023).

Neste sentido, Karina Farias (2022) alerta que as técnicas de inteligência artificial potencializam e ampliam a ocorrência de fraudes penais e irregularidades civis no tratamento de dados, especialmente com o uso de robôs para captar dados e criar perfis de consumo e uso de redes sociais. Observa que o aumento dos crimes cibernéticos tem tido consequências devastadoras para pessoas e empresas, tanto pelo vazamento de dados sensíveis quanto pela vulnerabilização de serviços essenciais, além do impacto econômico e da violação de direitos fundamentais. Menciona também a implementação de "ransomware", que impede o acesso a arquivos e exige pagamento para liberar os dados, afetando pessoas e empresas e comprometendo informações e sigilo industrial. Além disso, aponta a ocorrência de "spoofing" e "phishing", esquemas que induzem usuários a páginas falsas para fornecer dados sensíveis, e o surgimento de predadores virtuais que visam crianças e adolescentes, quebrando sua privacidade e segurança.

Enfim, é evidente a relevância do tema, sendo necessário o implemento de instrumentos de prevenção e combate eficazes, mundialmente interligados, eis que tais delitos não respeitam fronteiras (UNODC, 2024).

3 CONVENÇÃO DE BUDAPESTE - DECRETO 11.491/2023

Os delitos informáticos mereceram especial atenção do Conselho da Europa, através da criação de um comitê para elaboração de um instrumento internacional normativo sobre tais crimes, em constante mutação e evolução (Council of Europe, 2021).

Assim criou-se a Convenção sobre o Crime Cibernético, aberta para adesão em 2001, em Budapeste. Após décadas de vigor no ordenamento internacional, foi ratificada por diversos

países, membros e não membros do Conselho da Europa. O Brasil a ratificou em 2022 e a promulgou internamente com o Decreto 11.491/2023 (Murata, Torres, 2023, p. 13).

A Convenção de Budapeste é composta por um preâmbulo e quatro capítulos principais, que abordam diversos aspectos do cibercrime e as medidas necessárias para combatê-lo.

Destaca-se o artigo 2, contendo obrigação dos países signatários de criminalizar o acesso ilegal a sistemas de computadores[1].

No Capítulo II são descritas medidas legislativas e outras que os países devem adotar para criminalizar certas condutas e fornecer ferramentas eficazes de investigação.

Já no Capítulo III se elencou os Procedimentos Processuais e Medidas de Cooperação, cruciais para a eficácia da Convenção, pois estabelece procedimentos processuais e medidas de cooperação internacional, fundamentais para a luta contra o cibercrime.

Estabeleceu-se medidas para assegurar a preservação rápida de dados armazenados, permitindo que as autoridades competentes solicitem a preservação de dados críticos para investigações (art. 16). Tratou-se da produção de dados armazenados, viabilizando às autoridades competentes ordenar a produção de dados de assinantes e dados de tráfego armazenados por um provedor de serviços (art. 18). Ainda, previu-se a assistência mútua entre os países signatários, facilitando a troca de informações e a cooperação em investigações e processos judiciais (art. 23).

O Decreto 11.491/2023 incorpora a Convenção de Budapeste ao ordenamento brasileiro, contendo tais dispositivos. Destarte, fornece às autoridades instrumentos de cooperação em investigações e processos judiciais relacionados ao cibercrime, facilitando a troca de informações e a assistência mútua entre os países signatários.

Destaque-se a implementação de medidas para assegurar a preservação rápida de dados e a produção de provas, bem como a facilitação da assistência mútua transnacional, incluindo a troca de informações, a realização de buscas e apreensões, e a obtenção de provas em outros países.

Tem-se ainda a previsão de procedimentos simplificados para a extradição de indivíduos acusados de crimes cibernéticos, conforme as leis nacionais e os tratados internacionais aplicáveis.

[1] No Brasil, como se viu, tem-se a criminalização do crime cibernético próprio constante no art. 154-A do Código Penal, inserido pela Lei 14.155/2021 (invasão de dispositivo informático), bem como dos crimes previstos nos arts. 313-A e 313-B do mesmo Diploma (inserção de dados falsos e modificação/alteração não autorizada de sistema de informações.

Do ponto de vista empresarial-corporativo, destaca-se a previsão de responsabilidade penal da pessoa jurídica em crimes cibernéticos, a ser implementada definitivamente no ordenamento brasileiro (como parte aderente ao ato normativo internacional).

4 RESPONSABILIDADE PENAL DA PESSOA JURÍDICA

Cuida-se de tema ainda polêmico, que, inicialmente, sofreu aguda resistência doutrinária, mas, que, gradativamente vem se dissipando em muitos países, o que parece recomendável, haja vista a compatibilidade da responsabilidade penal da pessoa jurídica com os delitos praticados no ambiente cibernético.

4.1 Resistência da doutrina clássica do direito penal

Pessoas jurídicas nada mais são que entes fictícios, agrupamentos de homens que, reunidos para um fim, cuja realização procuram, mostram ter vida própria, distinta da dos indivíduos que os compõem (Bevilácqua, 1929, p. 58).

Por mais que o Brasil tenha aderido à Convenção de Budapeste, que traz expressa obrigatoriedade de responsabilização penal da pessoa jurídica por crimes cibernéticos, a doutrina clássica do direito penal brasileiro não admite tal ideia, ao considerar, como lecionava João Mestieri (1990), que não pode ser sujeito ativo por ser incapaz de ação e, ainda, de culpabilidade.

Nesse sentido, René Ariel Dotti (1995) afirmava que, no sistema jurídico brasileiro, a responsabilidade penal é atribuída exclusivamente a pessoas físicas, pois crimes e contravenções não podem ser praticados por pessoas jurídicas, sendo a imputabilidade jurídico-penal inerente aos seres humanos.

Por força da teoria finalista, adotada pelo sistema penal brasileiro[2], a espinha dorsal da ação final é a vontade, consciente do fim, reitora do acontecer causal (Welzel, 2001), atribuível ao ser humano. Portanto, os conceitos clássicos dogmáticos não seriam compatíveis com a ideia de responsabilização criminal do ente fictício.

No entanto, diversos Estados optaram pela tipificação penal de condutas atribuíveis às pessoas jurídicas.

[2] Artigo 18, I e II do Código Penal Brasileiro.

4.2 Ordenamentos estrangeiros e opção política pela responsabilização penal da pessoa jurídica

Em outros ordenamentos, optou-se pela responsabilização penal das pessoas jurídicas. Paulo César Busato (2019) expõe que a responsabilidade penal das pessoas jurídicas era negada, tradicionalmente, com base em três argumentos: falta de capacidade de ação, de culpabilidade e de sofrer penas. Aduz que essas máximas foram sendo enfraquecidas nas últimas décadas, e o impulso para a mudança veio de instâncias políticas, com argumentos de maior eficácia e pragmatismo, que se impuseram sobre considerações teóricas. A decisão político-criminal de responsabilizar pessoas jurídicas se estendeu dos países anglo-saxões aos sistemas continentais.

Para o autor, essa tendência se inverteu por duas razões principais: a necessidade de punir delitos socioeconômicos e financeiros (criminalidade de colarinho branco) e a urgência de novas vias de luta contra a criminalidade organizada. Também houve a guinada por razões de legalidade, devido aos problemas com delitos especiais cometidos no âmbito de sociedades ou por seus representantes, eis que mais de 80% dos delitos socioeconômicos são cometidos através de empresas.

Destarte, a necessidade de combater a criminalidade organizada, de larga escala, mormente com impacto socioeconômico, fez com que diversos ordenamentos jurídicos buscassem a tipificação penal de condutas imputáveis a pessoas jurídicas (através das quais os danos aos bens jurídicos penalmente tutelados são exponenciais). Alguns exemplos são notórios:

"The Bribery Act" de 2010, do direito britânico, trouxe imputação específica para a falha de organização empresarial que facilita a ocorrência de crimes (Reino Unido, 2010). O Código Penal francês contempla a responsabilização penal das "personnes morales" em seus artigos 121-2 e 121-3, à exceção do Estado, face a atos a si atribuíveis, por seus órgãos ou representantes, sem exclusão da responsabilidade das pessoas físicas sobre os mesmos fatos (FRANÇA, 1994).

Já o Código Penal espanhol (Espanha, 1995), no artigo 31 bis, prevê que "las personas jurídicas serán penalmente responsables":

> a) De los delitos cometidos en nombre o por cuenta de las mismas, y en su beneficio directo o indirecto, por sus representantes legales o por aquellos que actuando individualmente o como integrantes de un órgano de la persona jurídica, están autorizados para tomar decisiones en nombre de la persona jurídica u ostentan facultades de organización y control dentro de la misma.
> b) De los delitos cometidos, en el ejercicio de actividades sociales y por cuenta y en beneficio directo o indirecto de las mismas, por quienes, estando sometidos a la autoridad de las personas físicas mencionadas en el párrafo anterior, han podido

> realizar los hechos por haberse incumplido gravemente por aquéllos los deberes de supervisión, vigilancia y control de su actividad atendidas las concretas circunstancias del caso.

Na sequência, o Diploma espanhol contempla como excludente de responsabilidade das pessoas jurídicas (ou atenuante) a adoção, com eficácia, de modelos de organização e gestão com medidas de vigilância e controle idôneas para prevenção de delitos, e que tenham supervisão de seus sistemas de prevenção e controle mediante órgão autônomo (art. 31 bis, 2). Em verdade, confere grande relevância penal aos sistemas de compliance comprovadamente eficazes e independentes.

O Código Penal português (Portugal, 1995) também prevê como exceção a responsabilidade das "pessoas coletivas e entidades equiparadas", com exceção do Estado, limitando a imputabilidade a alguns tipos penais, quando cometidos: a) em nome da pessoa jurídica "ou por sua conta e no seu interesse direto ou indireto por pessoas que nelas ocupem uma posição de liderança"; ou "b) por quem aja em seu nome ou por sua conta e no seu interesse direto ou indireto, sob a autoridade das pessoas referidas na alínea anterior, em virtude de uma violação dos deveres de vigilância ou controlo que lhes incumbem" (artigo 11º).

Ademais, há previsão de responsabilidade concomitante (pessoas jurídica e física) e até mesmo independente ("a responsabilidade das pessoas colectivas (...) não exclui a responsabilidade individual dos respectivos agentes nem depende da responsabilização destes" – art. 11º, 7). O Diploma português prevê até mesmo a continuidade da responsabilização penal em caso de cisão e fusão, que deve ser "herdada" pelas pessoas que advierem destas operações (art. 11º, 7).

Enfim, como se viu, os ordenamentos jurídicos vêm optando (opção política), pela reprimenda penal às pessoas jurídicas, pautados na necessidade de expansão do direito penal, advinda da aparição de novos riscos sociais, da crescente insegurança e descrédito de outras instâncias de proteção (Sánchez, 2013).

A despeito de toda a dogmática penal clássica, a responsabilização dos "entes fictícios" na seara criminal se difundiu nos mais variados ordenamentos, inclusive no brasileiro. Neste, inclusive, explicitou-se a opção política ainda mais quando da adesão à Convenção de Budapeste.

4.3 Responsabilidade penal da pessoa jurídica por crimes cibernéticos

O Artigo 12 do Decreto 11.491/2023 (que promulga a Convenção sobre o Crime Cibernético no ordenamento brasileiro) estabelece que o país aderente adotará medidas (inclusive legislativas) para assegurar que pessoas jurídicas possam ser consideradas penalmente responsáveis por crimes tipificados na Convenção, quando cometidos em seus benefícios por pessoa física em posição de direção (individualmente ou como membro de órgão da organização), com base no poder de representação, na autoridade para tomar decisões ou autoridade para exercer controle interno da pessoa jurídica. Além disso, prevê que a pessoa jurídica possa ser responsabilizada quando a falta de supervisão ou controle tenha possibilitado o cometimento de um crime previsto na Convenção, por uma pessoa natural agindo sob autoridade dessa pessoa jurídica e em benefício dela.

Ou seja, estabeleceu-se pressupostos para a responsabilização penal das pessoas jurídicas: que os crimes estejam tipificados na Convenção de Budapeste, que tenham sido cometidos por representante/preposto com poder de direção, com autoridade ou com prerrogativa de controle interno da corporação, em prol desta. Ademais, tem-se a previsão de responsabilização por falta de supervisão ou controle, isto é, por omissão. Assim, além da forma dolosa comissiva, previu-se que a hipótese omissiva (ou a indolência na supervisão) igualmente trará reprimenda penal a empresa, quando o detentor do poder de direção ou controle falhar na supervisão ou fiscalização, viabilizando o ilícito.

Repare-se que os ordenamentos estrangeiros acima aludidos contemplam tais hipóteses. Neste ponto, concebe-se a responsabilização penal derivada do déficit organizacional, delineada por Leandro Sarcedo (2014), sob a premissa da culpabilidade própria da pessoa jurídica, como agrupamento que age coletivamente, não sendo a mera soma das culpabilidades individuais. Por este viés, a culpabilidade coletiva não exclui nem depende da responsabilidade individual das pessoas físicas. A reprovabilidade social do agir coletivo decorre de sua organização insuficiente para cumprir suas obrigações. Trata-se da ideia de defeito de organização, ou culpa organizacional, por não adotar medidas razoáveis e indispensáveis para impedir o delito.

Para aludido autor, mesmo os modelos de *heterorresponsabilidade*, que embora partam da transferência para a pessoa jurídica da responsabilidade de um ato praticado por um representante seu e em seu interesse ou proveito, ainda assim têm necessariamente que agregar à imputação a culpabilidade própria do ente coletivo, consistente em sua insuficiente organização para evitar a ocorrência de um fato daquela espécie. Da mesma forma, a partir desta concepção, nos modelos de *autorresponsabilidade*, faz-se possível a imputação de um

fato delituoso a um ente coletivo, mesmo quando não é possível imputá-lo a uma pessoa física determinada, desde que demonstrada a insuficiente organização corporativa no sentido de prevenir ou evitar a ocorrência com aquelas peculiaridades.

A despeito das discussões doutrinárias sobre esta possibilidade de imputação penal, é nítido que a Convenção de Budapeste traz, expressamente, a obrigatoriedade dos países signatários contemplarem, em seus ordenamentos, a responsabilização penal, cível e administrativa da pessoa jurídica por falha de supervisão ou controle, especificamente quando do cometimento de crimes cibernéticos por qualquer pessoa natural sob seu jugo ou em benefício da corporação (tratando-se de hipóteses não cumulativas – isto é, basta a ocorrência de uma das condições).

Esta concepção advém do conceito de "direito penal do risco" (ou ainda, da "sociedade de risco"), bem explanado pela autora portuguesa Carolina Uchôa (2019). Para a autora, o direito penal tem sido a primeira opção para conter crimes corporativos, argumentando-se que sua forte censura social cumpriria fins de prevenção geral e especial. Sanções apenas a pessoas físicas, ou vias cíveis e administrativas, não seriam suficientes. A criminologia ensina que a agrupação de pessoas facilita e incita autores físicos a cometer delitos em benefício do grupo, daí a ideia de sancionar não só os autores materiais, mas toda a agrupação. As novas formas de criminalidade (delitos de negócio) trazem dificuldades que demandam nova aborgadem. Vaticina a autora que as respostas dos grandes sistemas penais (*common law* e Europa continental) se aproximam, admitindo um direito penal moderno, que abarca as corporações.

De todo modo, a eficácia plena de tal norma dependerá de inserção, no ordenamento brasileiro, de Lei Penal que tipifique os ilícitos penais imputáveis a pessoa jurídica e estabeleça as respectivas penas (considerando o disposto no art. 5º, XXXIX da Carta Magna – "não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal"). Ou seja, o Congresso Nacional deverá legislar sobre o tema (art. 22, I da Constituição Federal), sob pena de descrédito do país (internamente e internacionalmente).

No momento, a pessoa jurídica é sujeita a reprimenda penal apenas na seara ambiental (art. 225, §3º da Constituição Federal e art. 3º da lei 9.605/98).

Certamente, parâmetros serão estabelecidos pelo legislador e jurisprudência, mormente quanto à eventual responsabilidade objetiva da corporação e a concomitância de responsabilidade da pessoa natural, exsurgindo possibilidade de absolvição desta e, quiçá, responsabilização objetiva da pessoa jurídica.

Novamente, mesmo ante a complexa e divergente dogmática penal sobre o tema (Sarcedo, 2014), o certo é que as corporações devem se preocupar com a prevenção dos ilícitos cibernéticos, evitando danos, prejuízos e responsabilização (senão ainda penal – que em breve deverá ser estipulada normativamente - certamente de ordem administrativa e cível, por Diplomas diversos já em vigor: Código de Defesa do Consumidor, Lei Geral de Proteção de Dados, etc).

E um dos meios eficazes de prevenção é, justamente, o compliance.

5 SISTEMAS DE COMPLIANCE

Sobre os sistemas de conformidade (ou integridade) corporativos, Sérgio Moro (2019) esclarece que, após grandes escândalos de corrupção nos EUA, as leis americanas influenciaram cenários internacionais. As práticas de compliance foram disseminadas por multinacionais como instrumento de prevenção e monitoramento de desvios de conduta de funcionários, fornecedores e prestadores de serviços. No Brasil, o movimento pelo compliance iniciou-se após 2016, ainda incipiente. O aculturamento por compliance é gradual e perene, não se limitando a estruturas, códigos de conduta, canais de denúncia e políticas internas. É um incessante orientar, direcionar, guiar e educar profissionais sobre integridade.

O Decreto 11.129/2022, regulamentando a Lei 12.846/2013 ("Lei Anticorrupção"), buscou conceituar e estabelecer parâmetros para os "programas de integridade":

> Art. 56. Para fins do disposto neste Decreto, programa de integridade consiste, no âmbito de uma pessoa jurídica, no conjunto de mecanismos e procedimentos internos de integridade, auditoria e incentivo à denúncia de irregularidades e na aplicação efetiva de códigos de ética e de conduta, políticas e diretrizes, com objetivo de:
> I - prevenir, detectar e sanar desvios, fraudes, irregularidades e atos ilícitos praticados contra a administração pública, nacional ou estrangeira; e
> II - fomentar e manter uma cultura de integridade no ambiente organizacional.
> Parágrafo único. O programa de integridade deve ser estruturado, aplicado e atualizado de acordo com as características e os riscos atuais das atividades de cada pessoa jurídica, a qual, por sua vez, deve garantir o constante aprimoramento e a adaptação do referido programa, visando garantir sua efetividade.

Portanto, no âmbito corporativo, os sistemas de compliance se estabeleceram como essenciais para a boa governança e gerenciamento de riscos.

Tem-se como elementos essenciais de tais programas, segundo Saccani e Oliver (2018): *análise de riscos* (detectar condutas irregulares e eficácias das medidas de controle); *código de conduta e políticas da empresa* (normas de conduta, gerais e específicas); *controles, capacitação e difusão* (formação dos colaboradores); *mecanismos de detecção e sanção*

(investigações internas, canais de denúncia, sanções disciplinares); *institucionalização* (funções, órgão e competências) e *documentação* (formalização para prova, circulares e outros).

O objetivo, portanto, é a prevenção, detecção e gestão de riscos de descumprimentos de normas (internas e públicas), visando incutir na corporação uma cultura ética para o crescimento sustentável. Fábio Guaragni (2020) ressalta este objetivo precípuo, definindo compliance como um conjunto de medidas de prevenção de riscos empresariais. Para ser eficaz, as normativas devem ser cumpridas por todos na organização. O compliance busca aderência ética individual e coletiva, necessitando de um sistema de identificação, correção e prevenção de desvios. A criação e aplicação de um programa de compliance deve ser institucionalizada por medidas de controle, como código de conduta, sanções disciplinares, canais de denúncia e investigações internas.

Com efeito, o pressuposto de todo sistema de compliance é a avaliação de riscos de conformidade (conforme estabelece o parágrafo único do art. 56 do Decreto 11.129/2022). Ou seja, primeiramente há que se definir quais são as ameaças financeiras, organizacionais e de reputação de dada corporação em determinado contexto local e legal (Saccani, Oliver, 2018). Trata-se do *risk assessment* (análise de risco), conceituado por Batisti e Kempfer (2016), fundamental (e o primeiro passo) para inaugurar um programa robusto de compliance, que leva em conta as circunstâncias individuais da companhia, pontualmente os riscos prováveis relacionados às atividades que a mesma desenvolve, desencadeando o mapeamento e a sistematização de uma matriz de riscos.

A matriz de riscos nada mais é que um mapeamento das exposições específicas da corporação a determinados tipos de inconformidades, afetas às mais variadas áreas de atuação (ambiental, econômica, relação coma gentes públicos *etc.*).

Considerando a intensa digitalização das atividades empresariais, é de extremo relevo a matriz de risco afeta, justamente, aos cibercrimes, para se definir códigos de conduta voltados ao tema, controles internos, formação dos colaboradores, mecanismos de detecção e sanção sobre estes ilícitos e a institucionalização dos meios de prevenção e combate.

5.1 Compliance no âmbito dos crimes cibernéticos

Devido a escala global da criminalidade cibernética, o compliance nesta seara tornou-se essencial à atividade empresarial. Especificamente quanto à globalização e a necessária integridade empresarial, destaca Mateus Bertoncini (2018) que a globalização trouxe uma

visível mudança no mundo corporativo, ao pressionar as empresas, para se manter ativas no mercado, a ter de instituir novas técnicas e ferramentas para a minimização de riscos originados por suas ações (sistemas de gestão de riscos). No passado as empresas somente avaliavam o risco sob o ponto de vista da perda econômica. Nos dias de hoje aproxima-se cada vez mais da eventual responsabilidade jurídica dos administradores ou da própria empresa, seja pelo abuso de poder dos administradores, seja pela incidência de fraudes internas com lesão a terceiros ou pela responsabilidade social. Destaca o autor que o compliance é o novo modelo desta gestão e traduz a boa governança corporativa.

De fato, os sistemas de integridade ganham especial relevo na prevenção dos crimes cibernéticos, não só pelo potencial danoso desta espécie de criminalidade (agravada com a previsão de responsabilidade penal das corporações), mas também para inserção as empresas no mercado mundial. O compliance é, cada vez mais, uma exigência para inserção no mercado (Oliva, Silva, 2018, p. 2709).

Estabelecendo-se os riscos inerentes a atividade digital de determinada empresa ("matriz de risco" específica), faz-se possível criar sistemas de segurança cibernética, implantando-se regras e controles, políticas internas, critérios, ritos gerenciais e procedimentos adequados às possíveis inconformidades cibernéticas (vazamento de informações, fraudes, uso indevido dos programas operacionais, potenciais lesões a consumidores e fornecedores por inconsistências cibernéticas, etc).

Como exemplo, é possível o emprego de softwares aptos a identificar anomalias, usos indevidos dos terminais da empresa, fugas dos padrões estabelecidos nos códigos de conduta, gerando alertas e instaurando procedimentos de controle.

Evidentemente, como parte de um sistema de compliance, tais controles devem ser frequente e incessantemente revistos, atualizados e retroalimentados (Saccani, Oliver, 2018).

Neste sentido, a corporação com atuação no Brasil deve se atentar para o contexto legal vigente sobre o tema, como premissa para a adequação do programa de integridade cibernético: Lei "Carolina Dickman" (12.737/2012), Decreto que regulamenta o comércio eletrônico (7.962/2013), Marco Civil da Internet (Lei 12.965/2014); Decreto sobre governança no compartilhamento de dados no âmbito da administração pública e Cadastro Base do Cidadão (Dec. 10.046/2019) e, ainda, a Lei Geral de Proteção de Dados (Lei 13.709/2018).

Como se viu, outras normas tratam indiretamente do tema, como o próprio Código Penal, eis que diversos crimes cibernéticos impróprios encontram tipificação neste Diploma e

em outros de natureza penal (estelionato qualificado por fraude eletrônica, crimes contra a honra, pornografia infantil, racismo, crimes contra o consumidor, etc).

Assim, a prevenção e controle sobre o cometimento de tais ilícitos, eventualmente imputáveis a pessoa jurídica, por seus prepostos ou mesmo terceiros contratados, é de suma importância para evitar e reprimir a responsabilização cível, administrativa e, mormente com o advento do Decreto 11.491/2023, penal (dada a previsão de imputação objetiva ou, ao menos, advinda do déficit organizacional – ou falha na supervisão).

Enfim, as empresas poderão adequar seus sistemas de compliance também às novas previsões da Convenção de Budapeste, finalmente incorporadas ao nosso ordenamento.

5.2 Instrumentos do Decreto 11.491/2023 e possibilidades de adaptação e aprimoramento dos sistemas de compliance

Como se viu, a globalização e o avanço da tecnologia intensificaram a necessidade de cooperação internacional no combate aos crimes cibernéticos.

Órgãos como a Organização Internacional de Polícia Criminal (Interpol, 2024), o Escritório das Nações Unidas sobre Drogas e Crime (UNODC, 2024) e outros, desempenham um papel crucial nessa cooperação, atuando na troca de informações, na investigação de crimes transnacionais e na coordenação de ações entre diferentes países.

Francisco Rezek (2018), aclara a importância da atuação coordenada das autoridades integradas de diversos países. Observa que Estados se dividem por fronteiras, jurisdições são limitadas, e a "comunidade" internacional tem um longo caminho até atingir a integração que a Internet proporcionou. As características da Internet (descentralização, distribuição por diversos territórios) impõem desafios para investigar, julgar e punir crimes. As provas podem estar a milhares de quilômetros de onde os efeitos foram sentidos ou o julgamento deve ocorrer. Na rede, qualquer um pode ofertar serviços lícitos ou ilícitos a qualquer pessoa no mundo. Grandes empresas distribuem sua estrutura em países específicos, submetendo-se a uma única jurisdição. Conclui o autor que, enquanto reconhecermos a necessidade de adaptação mas não lutarmos por novas mentalidades, o aparato estatal de repressão estará sempre perdendo. Se a mudança social clama por submissão do Direito a novas *ratios* sociais, ela também deve trazer mudanças no próprio homem que aplica a Lei.

Assim, a Convenção sobre Crimes Cibernéticos de Budapeste estabelece um marco legal crucial para a cooperação internacional nessa área, estabelecendo a previsão dos países

signatários, por exemplo, cooperarem em medidas cautelares investigativas (busca e apreensão, ordens de exibição, obtenção de dados em tempo real, interceptações, etc – arts. 18 a 21 e 29 a 35 do Decreto 11.491/2023).

De relevo também a previsão de contato 24h, diariamente, entre as autoridades centrais de cada país para fins de cooperação em investigações ou procedimentos relacionados a crimes cibernéticos (art. 35).

Disto, os sistemas de compliance podem se readequar a estes novos *standarts*, criando junto ao "compliance officer" diretrizes e procedimentos para célere cooperação com as autoridades, inclusive transnacionais, no fornecimento de informações e consecução e diligências (mormente que toquem de algum modo a corporação, obviamente no seu interesse).

Com isto, a pessoa jurídica passa a demonstrar compromisso com a segurança cibernética e a transparência, não apenas fortalecendo sua imagem, mas também a prevenção de ilícitos nesta seara e, consequentemente, evitando responsabilização (ou ao menos amenizando).

Para tanto, a adequação e aprimoramento do programa de conformidade pode passar pela criação de órgãos ou comitês específicos para tratar de questões relacionadas à cibersegurança, focado na matriz de risco em tela no âmbito internacional (obviamente, para empresas multinacionais). Há ainda a possibilidade de inclusão de metas de cibersegurança nos planos estratégicos da empresa, implementado o compromisso da alta administração com a segurança da informação.

Ainda, as empresas podem prever em seus Códigos de Conduta o necessário investimento em soluções de segurança de última geração, como firewalls, sistemas de detecção de intrusão e ferramentas de análise de ameaças, que podem, inclusive, moldar canais de cooperação direta com autoridades públicas transnacionais (no fornecimento de informações e cooperação em diligências, com comunicações instantâneas às autoridades centrais dos países – previstas no art. 27 do Decreto 11.491/2023).

Ademais, as corporações podem prever métodos de "preservação expedita de dados armazenados em computador", tal qual previsto no art. 16 do Decreto 11.491/2023, contando com a tecnologia disponível.

De relevo também a possibilidade de treinamentos regulares dos colaboradores nesta seara, com simulações de ataques cibernéticos, normas de conduta para tratamento de vazamentos de dados (ou mesmo invasão de dispositivos), visando identificar, continuamente, as vulnerabilidades da empresa e testar a eficácia dos planos de resposta a incidentes. Neste

viés, pode-se elaborar planos de respostas a incidentes, com previsão de ágil cooperação com as autoridades transnacionais (arts. 27 e 29, 2, "a" da Convenção, dentre outros) e locais, incumbidas de prevenir e reprimir estes delitos.

Enfim, inúmeras são as possibilidades de adequação dos sistemas de compliance às disposições da Convenção recém promulgada, visando maior eficiência e amplitude dos controles corporativos.

CONCLUSÃO

A adesão do Brasil à Convenção de Budapeste representa um marco importante na luta contra os crimes cibernéticos, delitos estes que se espraiam em ritmo exponencial, com sofisticação.

A previsão de responsabilização penal das pessoas jurídicas por esses delitos exige ainda mais que as empresas adotem medidas de compliance robustas (preparando-se para os tipos penais "corporativos" a serem elaborados pelo legislador). Os programas de integridade corporativa devem ser adaptados para identificar e mitigar os riscos cibernéticos, promovendo uma cultura de segurança da informação e garantindo a cooperação com as autoridades.

A implementação de medidas como a análise de riscos, a criação de códigos de conduta específicos para a área de tecnologia da informação, a realização de treinamentos e a definição de protocolos de resposta a incidentes são essenciais para que as empresas possam se adequar à nova realidade, e em especial às disposições do Decreto 11.491/2023.

Com as adequações internas à nova norma, observando seus instrumentos de prevenção e repressão transnacionais, as corporações ganham em eficácia na proteção de seus ativos. Ainda, previnem-se quanto a eventuais sanções penais, sobre o corpo diretivo ou mesmo sobre a própria empresa (advinda de vindoura legislação que tipifique condutas das pessoas jurídicas).

Em última análise, incorporar os conceitos e instrumentos da Convenção em foco aos programas de integridade, representa para as corporações um importante passo para a efetiva implementação de condutas éticas e cautas no manejo da informática.

REFERÊNCIAS

ASSIS, Rebeka. **Crimes Virtuais: descubra quais são os 7 mais cometidos!**. Jusbrasil. 2019. Disponível em: https://www.jusbrasil.com.br/artigos/crimes-virtuais-descubra-quais-sao-os-7-mais-cometidos/784440112. Acesso em: 27 jul. 2024.

BBC News Brasil. **Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades**. 2018. Disponível em https://www.bbc.com/portuguese/internacional-43461751. Acesso em: 20 jul. 2024.

BERTONCINI, Mateus Eduardo Siqueira Nunes; CAMPOS DE ARAUJO, Alexandra Barbosa. Competition Compliance: Controlling and Combating Illicit Practices in the Economic Market. **ESG Studies Review**, São Paulo (SP), v. 1, n. ssue, p. e01605, 2018. DOI: 10.37497/esg.v1issue.1605. Disponível em: https://esglawreview.org/convergencias/article/view/1605. Acesso em: 27 ago. 2024.

BEVILÁCQUA, Clóvis. **Teoria Geral do Direito Civil**, 2ª edição, Rio de Janeiro: Livraria Francisco Alves, 1929

BRASIL. **Código Penal**. Disponível em https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 30 jul. 2024.

BRASIL. **Constituição da República Federativa do Brasil**. Disponível emhttps://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 30 jul. 2024.

BRASIL. **Decreto 7.962/2013**. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d7962.htm. Acesso em: 30 jul. 2024.

BRASIL. **Decreto 10.046/2019**. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d10046.htm. Acesso em: 30 jul. 2024.

BRASIL. **Decreto 11.129/2022**. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/decreto/d11129.htm. Acesso em: 30 jul. 2024.

BRASIL. **Decreto 11.491/2023**. Disponível em https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11491.htm. Acesso em: 30 jul. 2024.

BRASIL. **Estatuto da Criança e do Adolescente**. Disponível em https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 30 jul. 2024.

BRASIL. **Lei 7.716/89**. Disponível em https://www.planalto.gov.br/ccivil_03/leis/l7716.htm. Acesso em: 30 jul. 2024.

BRASIL. **Lei 12.737/2012**. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 30 jul. 2024.

BRASIL. **Lei 12.846/2013**. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12846.htm. Acesso em: 30 jul. 2024.

BRASIL. **Lei 12.965/2014**. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 30 jul. 2024.

BRASIL. **Lei 13.709/2018**. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 30 jul. 2024.

BUSATO, Paulo Cesar; CUSSAC, José L. González. O modelo espanhol de responsabilidade penal das pessoas jurídicas do CP de 2010. **Revista dos Tribunais**. 2019. Disponível em: https://site.mppr.mp.br/sites/hotsites/arquivos_restritos/files/migrados/File/Responsabilidade_Penal_de_Pessoa_Juridica_Busato.pdf. Acesso em: 27 ago. 2024.

COUNCIL OF EUROPE. **Convention on cybercrime: Special edition dedicated to the draft-ers of the Convention** (1997-2001). Estrasburgo: Council of Europe, 2021. Disponível em: https://rm.coe.int/special-edition-budapest-convention-en-2022/1680a6992e. Acesso em: 28 jul. 2024

DOTTI, René Ariel. **A incapacidade criminal da pessoa jurídica: uma perspectiva do Direito brasileiro**. Revista Brasileira de Ciências Criminais. São Paulo. Vol. 11. Jul/set 1995

ESPANHA. **Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.** Disponível em: https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444#a31bis. Acesso em 27.ago.2024

FARIAS, Karina da Hora. **Impactos dos crimes cibernéticos e os riscos da inteligência artificial: os pilares do direito na proteção dos dados sensíveis**. (Dissertação) Mestrado em Direito do Programa de Pós-graduação da Universidade Federal da Bahia (UFBA), Salvador - Brasil, 2022. 167 p. Disponível em: https://repositorio.ufba.br/bitstream/ri/36911/1/DISSERTA%c3%87%c3%83O%20DE%20KARINA%20DA%20HORA%20FARIAS.pdf. Acesso em: 30 jul. 2024.

FRANÇA. **Code pénal français.** Disponível em: legifrance.gouv.fr. Acesso em 27.ago.2024

GUARAGNI, Fábio André; RIOS, Rodrigo Sánchez. Novas tendências de combate aos crimes cibernéticos: cooperação internacional e perspectivas na realidade brasileira contemporânea. **Revista de Estudos Criminais**, Porto Alegre, v. 18, n. 73, p. 167-196, 2019.

GUARAGNI, Fábio André; STEIDEL, Evelin. Desvios de personalidade em grupos empresariais e neutralização por compliance: uma tentativa para minimizar o impacto da corrupção no horizonte da criminalidade? **Direito Penal Econômico – Administrativização do direito penal, criminal compliance e outros temas contemporâneos.** Londrina. Ed. Thoth, p. 45-77, 2017.

G1. **JBS diz que pagou US$ 11 milhões em resgate a ataque hacker em operações nos EUA. 2021**. Disponível em https://g1.globo.com/economia/noticia/2021/06/09/jbs-diz-que-pagou-11-milhoes-em-resposta-a-ataque-hacker-em-operacoes-nos-eua.ghtml. Acesso em: 20 jul. 2024.

INTERPOL. **What is INTERPOL?**. Disponível em: https://www.interpol.int/Who-we-are/What-is-INTERPOL. Acesso em: 27 jul. 2024.

JACOB, Sofia. **Caso Ashley Madison: O vazamento de dados que revelou o submundo de vidas privadas**. Jusbrasil. 2024. Disponível em: https://www.jusbrasil.com.br/artigos/caso-ashley-madison-o-vazamento-de-dados-que-revelou-o-submundo-de-vidas-privadas/2513179758. Acesso em: 27 jul. 2024.

JESUS, Damásio de; MILAGRES, José Antônio. **Manual de Crimes Informáticos**. 1ª Edição. ed. São Paulo: Saraiva, 2016.

LUMI KAMIMURA MURATA, D. A. M.; RITZMANN TORRES, M. P. A convenção de Budapeste sobre os crimes cibernéticos foi promulgada, e agora?. **Boletim IBCCRIM**, [S. l.], v. 31, n. 368, 2023. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/575. Acesso em: 30 jul. 2024.

MESTIERI, João; **Teoria Elementar do Direito Criminal – Parte Geral**, Rio de Janeiro: Edição do Autor, 1990.

MIRANDA BATISTI, Beatriz; KEMPFER, Marlene. Parâmetros de compliance por meio da metodologia de análise de risco para a mitigação da responsabilidade objetiva diante da Lei Anticorrupção (12.846/2013) em face de negócios públicos. **Revista Brasileira de Direito Empresarial**. 2016. Disponível em: https://indexlaw.org/index.php/direitoempresarial/article/view/1019/1014. Acesso em: 20 jul. 2024.

MORO, Sérgio Fernando; MARTINS, José Alberto Monteiro; LEONI, Jaqueline Vasconcelos. **A Eficácia do Compliance Público/Privado no Combate à Corrupção**. EALR, V. 10, nº 2, p. 245-260, Mai-Ago, 2019. Disponível em: https://portalrevistas.ucb.br/index.php/EALR/issue/view/565. Acesso em: 25 jul. 2024

MPMT. **IA, deepfake e hacktivismo: a tempestade perfeita para 2024**. 2023. Disponível em: https://mpmt.mp.br/portalcao/news/1217/132101/ia-deepfake-e-hacktivismo-a-tempestade-perfeita-para-2024/36. Acesso em: 27 jul. 2024.

OLIVA, Milena Donato; SILVA, Rodrigo da Guia. Origem e evolução histórica do compliance no direito brasileiro. In: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (coord.). **Compliance: perspectivas e desafios dos programas de conformidade**. Belo Horizonte: Fórum, 2018. p. 29-51.

REINO UNIDO. **Bribery Act 2010.** Disponível em https://www.legislation.gov.uk/ukpga/2010/23/contents. Acesso em: 27 ago. 2024.

REZEK, José Francisco; GUIDI, Guilherme Berti de Campos. Crimes na internet e cooperação internacional em matéria penal entre Brasil e Estados Unidos. **Revista brasileira de políticas públicas** [recurso eletrônico], v. 8, n. 1, p. 276-288 2018. Disponível em: https://www.publicacoes.uniceub.br/RBPP/article/view/5130/3713. Acesso em: 20 jul. 2024.

ROQUE, Sérgio Marcos. **Criminalidade Informática: crimes e criminosos do computador**. 1ª ed. São Paulo: ADPESP Cultural, 2007.

Saccani, Raúl R. e Oliver, Gustavo L. Definiendo Compliance y los Programas de Integridad. In: Saccani, Raúl R. e Oliver, Gustavo L. (org) **Tratado de compliance**: Tomo I. 1. Ed. Buenos Aires: La Ley, 2018, p. 3-142.

SARCEDO, Leandro. **Compliance e responsabilidade penal da pessoa jurídica: construção de um novo modelo de imputação, baseado na culpabilidade corporativa**. 2015. Tese (Doutorado em Direito Penal) - Faculdade de Direito, University of São Paulo, São Paulo, 2015. doi:10.11606/T.2.2015.tde-07122015-163555. Acesso em: 30 jul. 2024.

SCHWAB, Klaus. **The fourth industrial revolution**. Geneva: World Economic Forum, 2016. Disponível em: https://law.unimelb.edu.au/__data/assets/pdf_file/0005/3385454/Schwab-The_Fourth_Industrial_Revolution_Klaus_S.pdf. Acesso em: 20 jul. 2024.

SILVA SÁNCHEZ, Jesús-María. **A expansão do direito penal: aspectos da política criminal nas sociedades pós-industriais**. Tradução de Luiz Otávio de Oliveira Rocha. 3. ed. rev. e atual. São Paulo: RT, 2013.

SIQUEIRA, Dirceu Pereira; LARA, Fernanda Corrêa Pavesi. Quarta revolução industrial, inteligência artificial e a proteção do homem no direito brasileiro. **Revista Meritum**, Belo Horizonte, vol. 15, n. 4, p. 300-311, 2020. Disponível em: http://revista.fumec.br/index.php/meritum/article/view/8223. Acesso em: 20 jul. 2024.

SPADINGER, Robert. O futuro das telecomunicações e uma análise dos desafios para a inserção do Brasil numa cadeia global. In: KUBOTA, Luis Claudio et al. **Tecnologias da Informação e comunicação: competência, políticas e tendências**. Brasília: Ipea, 2018

UCHÔA, Carolina de Novaes. **A gestão responsiva do risco penal empresarial - a responsabilidade penal da empresa e os programas de compliance em um ambiente integrado e comunicativo**. 2019. Dissertação (Mestrado em Direito) - Faculdade de Direito da Universidade de Coimbra, Coimbra, 2019. Disponível em: https://estudogeral.uc.pt/handle/10316/90377. Acesso em: 30 jul. 2024.

UNODC. **Crimes cibernéticos**. Disponível em: https://www.unodc.org/lpo-brazil/pt/covid19/cibercriminalidade-e-desinformacao.html#:~:text=Crimes%20cibern%C3%A9ticos&text=Sua%20natureza%20complexa%20de%20crime,como%20o%20da%20Covid%2D19. Acesso em: 27 jul. 2024.

UNODC. **Sobre o UNODC**. Disponível em: https://www.unodc.org/lpo-brazil/pt/sobre-unodc/index.html. Acesso em: 27 jul. 2024.

WELZEL, Hans. **O Novo Sistema Jurídico-Penal**. Trad. Luiz Regis Prado. São Paulo: Revista dos Tribunais, 2001