IV ENCONTRO VIRTUAL DO CONPEDI

DIREITO PENAL, PROCESSO PENAL E CONSTITUIÇÃO II

LUIZ GUSTAVO GONÇALVES RIBEIRO

MAIQUEL ÂNGELO DEZORDI WERMUTH

ALCEU DE OLIVEIRA PINTO JUNIOR

D597

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

Coordenadores: Alceu de Oliveira Pinto Junior; Luiz Gustavo Gonçalves Ribeiro; Maiquel Ângelo Dezordi Wermuth – Florianópolis: CONPEDI, 2021.

Inclui bibliografia
ISBN: 978-65-5648-413-6
Modo de acesso: www.conpedi.org.br em publicações
Tema: Constitucionalismo, desenvolvimento, sustentabilidade e smart cities.

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito penal. 3. Processo penal. IV Encontro Virtual do CONPEDI (1: 2021 : Florianópolis, Brasil).

CDU: 34

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

IV ENCONTRO VIRTUAL DO CONPEDI

DIREITO PENAL, PROCESSO PENAL E CONSTITUIÇÃO II

Apresentação

APRESENTAÇÃO

A pandemia do novo coronavírus segue exigindo de todos nós, neste ano de 2021, adaptação. O CONPEDI segue envidando esforços, nesse sentido, para reunir, em ambiente eletrônico, pesquisadores da pós-graduação jurídica de todo o Brasil em suas muitas salas virtuais, nas quais temas de altíssima relevância são amplamente debatidos.

Nesse sentido, temos a honra de apresentar, aqui, aquelas pesquisas que foram apresentadas no âmbito do Grupo de Trabalho "Direito Penal, Processo Penal e Constituição II", na tarde do dia 13 de novembro de 2021.

No artigo intitulado "LICITAÇÕES E CONTRATOS ADMINISTRATIVOS: A LEI 14.133 /2021 E O CRIME DE CONTRATAÇÃO DIRETA ILEGAL PREVISTO NO ART. 337-E DO CÓDIGO PENAL", Davi Pereira Remedio e José Antonio Remedio analisam o artigo 337-E do Código Penal, avaliando a amplitude de sua tipificação e da severidade das sanções cominadas ao delito, o que deverá contribuir para o combate à corrupção e para melhor responsabilização dos infratores participantes direta ou indiretamente das licitações e contratos administrativos.

O texto "ANÁLISE ECONÔMICA DO DIREITO E O CRIME DE MANIPULAÇÃO DO MERCADO DE CAPITAIS", de Marcelo Costenaro Cavali, Alessandra Gomes Faria Baldini e Vanessa Piffer Donatelli da Silva aborda os fundamentos econômicos que justificam a criminalização da manipulação do mercado de capitais.

Bibiana Terra e Bianca Tito, no texto intitulado "DIREITO PENAL DE EMERGÊNCIA E A INOBSERVÂNCIA POR PARTE DO ESTADO AO PRINCÍPIO DA INTERVENÇÃO MÍNIMA: O SIMBOLISMO PENAL E SUAS IMPLICAÇÕES NAS POLÍTICAS CRIMINAIS CONTEMPORÂNEAS DO BRASIL", avaliam o direito penal em seu caráter emergencial, diante da inobservância por parte do Estado ao princípio da intervenção mínima preconizado no texto constitucional de 1988.

Por sua vez, no artigo "DELITOS DE PERIGO ABSTRATO DE BENS JURÍDICOS COLETIVOS: UMA ANÁLISE CRÍTICA A PARTIR DA TEORIA PERSONALISTA DE

WINFRIED HASSEMER", Airto Chaves Junior e Thiago Santos Aguiar de Pádua empreendem uma análise crítica dos delitos de perigo abstrato de bens jurídicos coletivos a partir dos critérios propostos por Winfried Hassemer.

O texto "COMUNICAÇÃO DA PRISÃO EM FLAGRANTE COMO MEIO DE CONTROLE POPULAR DO SERVIÇO DE SEGURANÇA PÚBLICA", de autoria de Bibiana Paschoalino Barbosa e Luiz Fernando Kazmierczak, analisa o caráter de direito fundamental da segurança pública, especificamos os meios de controle dos atos administrativos com enfoque no controle social, trazendo como conclusão que a comunicação da prisão em flagrante é meio efetivo de controle popular consubstanciando a efetivação da publicidade dos atos administrativos.

Ana Flavia De Melo Leite e Gabriel Silva Borges, no texto "A ASSISTÊNCIA DE ADVOGADO AO INDICIADO EM SEDE DE INTERROGATÓRIO POLICIAL E A NOVA LEI DE ABUSO DE AUTORIDADE", discutem a atuação do advogado juntamente ao indiciado preso em flagrante quando de sua oitiva perante a Autoridade Policial no período noturno, diante da edição da Lei 13.869/2019 que criminaliza condutas que tangenciam o procedimento como crimes de abuso de autoridade.

Em "A IMPORTÂNCIA DA APLICAÇÃO DA TEORIA DA IMPUTAÇÃO OBJETIVA NA RESPONSABILIZAÇÃO PENAL DA PESSOA JURÍDICA NOS CRIMES ECONÔMICOS: UMA ANÁLISE DA LEGISLAÇÃO BRASILEIRA E ESPANHOLA", Edith Maria Barbosa Ramos, Roberto Carvalho Veloso e Rayane Duarte Vieira abordam a aplicação da Teoria da Imputação Objetiva no âmbito do Direito Penal Econômico, trazendo apontamentos sobre a importância da Responsabilização Criminal da Pessoa Jurídica para fins de combate à criminalidade contemporânea.

No artigo "GLOBALIZAÇÃO E CRIMINALIDADE TRANSNACIONAL: A VIABILIDADE DA COOPERAÇÃO INTERNACIONAL E MEDIDAS ALTERNATIVAS EXTRAPENAIS", Anna Kleine Neves e Fernanda Borba de Mattos d´Ávila avaliam a viabilidade da cooperação internacional e medidas alternativas extrapenais, empreendendo reflexões sobre a influência e consequências causadas pela Globalização e pela transnacionalidade no Direito Penal, sobre a importância da cooperação jurídica internacional e de medidas alternativas extrapenais na resolução dos possíveis conflitos.

Em seu "ESTUDO COMPARADO DA PRISÃO PREVENTIVA NO BRASIL E DA PRISÃO INVESTIGATÓRIA NA ALEMANHA: O ENCARCERAMENTO DE PESSOAS E NOVAS ALTERNATIVAS EM POLÍTICAS CRIMINAIS", Jessica de Jesus Mota e

Lucia Carolina Raenke Ertel propõem-se a demonstrar como é utilizada a prisão preventiva no Brasil e a prisão investigatória na Alemanha, estudando os principais aspectos das prisões cautelares nos dois países.

O artigo "A POSSIBILIDADE DE SUSPENSÃO DAS MÚLTIPLAS MEDIDAS SANCIONATÓRIAS INSTAURADAS SOB O MESMO CONTEXTO FÁTICO-PROBATÓRIO COMO CAMINHO PARA MINORAR OS RISCOS DO BIS IN IDEM", de autoria de Jean Colbert Dias, Anderson Ferreira e Marcelo de Souza Sampaio, investiga o campo de incidência do Direito Penal e do Direito Administrativo Sancionador, evidenciando-se uma nova vertente do Supremo Tribunal Federal sobre o assunto.

No trabalho intitulado "INQUÉRITO DAS FAKE NEWS: ENTRE O INSTRUMENTALISMO E O GARANTISMO PENAL", os autores João Paulo Avelino Alves De Sousa e Rejane Feitosa de Norões Milfont analisam o inquérito das fake News à luz da teoria do garantismo penal de Luigi Ferrajoli, na vigência da Constituição Federal de 1988.

"CATEGORIAS PROCESSUAIS E DISCUSSÕES ACERCA DO PROCESSO PENAL BRASILEIRO ORIGINÁRIO NO SUPREMO TRIBUNAL FEDERAL: AÇÃO PENAL E A DECISÃO PENAL", de Francisco Geraldo Matos Santos e Renato Ribeiro Martins Cal, é um trabalho que apresenta considerações críticas a respeito de algumas categorias no processo penal cuja competência originária é do STF, tendo em vista a necessidade de compreender se há ou não efetivação do que o texto constitucional pós 1988 realmente se propôs a proteger no que tange ao acusado.

Luiz Gustavo Gonçalves Ribeiro, Silvia Altaf da Rocha Lima Cedrola e Daniel Alberico Resende, no texto "A NOVA FACETA DO DIREITO À INTIMIDADE NO MEIO AMBIENTE DIGITAL: A TIPIFICAÇÃO DO REVENGE PORN", avaliam como as transformações e inovações tecnológicas desencadearam uma necessidade de alteração do ordenamento jurídico pátrio, mais especificamente no Direito Penal, sendo que essa necessidade, ligada ao meio ambiente digital, colide, por vezes, com o direito à intimidade, o que justifica o estudo do chamado revenge-porn, mormente a partir da análise das Leis Federais nº 12.737/2012 e nº 12.965/2014.

No artigo "CIBERCRIME E A NECESSÁRIA REFORMA DA LEGISLAÇÃO PENAL BRASILEIRA", Clarisse Aparecida Da Cunha Viana Cruz, Daniel Brasil de Souza e Pedro José de Campos Garcia avaliam é se a legislação penal brasileira é suficiente para proteger os cidadãos contra os cibercrimes.

O trabalho “MEDIDAS JURÍDICAS PROVISÓRIAS E JUSTIÇA DRAMÁTICA: A CRISE NA COMUNICAÇÃO ENTRE A ATIVIDADE JURÍDICO-PERSECUTÓRIA DO ESTADO E A OPINIÃO PÚBLICA NO CONTEXTO DA SOCIEDADE EM REDE”, de Bruna Barbosa de Góes Nascimento e Henrique Ribeiro Cardoso analisam como a atividade jurídico-persecutória do Estado nos casos que atraem a atenção pública está sendo impactada tanto pelos meios de comunicação em massa quanto pelas redes sociais que expressam em larga medida a opinião pública no contexto da atual sociedade em rede.

Em “A INEFICÁCIA DA POLÍTICA CRIMINAL NO COMBATE AO TRÁFICO DE DROGRAS ENQUANTO OBJETO DE LUCRO DAS ORGANIZAÇÕES CRIMINOSAS”, Cristian Kiefer Da Silva analisa a ineficácia da política criminal no combate ao tráfico de drogas enquanto objeto de lucro das organizações criminosas.

O artigo “MEIO AMBIENTE DIGITAL E A AUTORIA DELITIVA NOS CRIMES CIBERNÉTICOS”, de Júlio César Batista Pereira e Reinaldo Caixeta Machado, aborda como os avanços da informática e da tecnologia têm sido palco diário de ameaças à sociedade de risco, capazes de afetar diversos segmentos que repercutem na seara jurídica e em um ambiente que foge da naturalidade, tradicionalmente tutelado pelo Direito.

No texto “A (IN)COMPATIBILIDADE DO CRIME DE DESACATO COM O DIREITO À LIBERDADE DE EXPRESSÃO NA ÓTICA DO SUPERIOR TRIBUNAL DE JUSTIÇA”, Abner da Silva Jaques, Endra Raielle Cordeiro Gonzales e João Fernando Pieri de Oliveira analisam o debate sobre a descriminalização do delito de desacato no Brasil, partindo das decisões proferidas no âmbito do STJ.

Em “CRIMES PRATICADOS CONTRA A ADMINISTRAÇÃO PÚBLICA E PRINCÍPIO DA INTERVENÇÃO MÍNIMA NA JURISPRUDÊNCIA DO STJ”, Airto Chaves Junior e Thiago Santos Aguiar de Pádua avaliam se os argumentos utilizados pelo Superior Tribunal de Justiça na análise da tipicidade material do fato nos delitos praticados contra a Administração Pública violam o Princípio da Intervenção Mínima.

Thulio Guilherme Silva Nogueira, no texto “O DIREITO À PRESENÇA FÍSICA DO IMPUTADO NOS ACORDOS PENAIS CELEBRADOS EM AMBIENTE VIRTUAL”, questiona a viabilidade constitucional da negociação de acordos penais no ambiente virtual, concluindo que a negociação no âmbito virtual não pode ser impositiva, e deve ser tratada como faculdade da defesa.

Em “A DUPLA INCIDÊNCIA DE SANÇÃO PENAL E ADMINISTRATIVA EM MATÉRIA URBANÍSTICA E O PRINCÍPIO DO NE BIS IN IDEM”, Bruna Azevedo de Castro e Sibila Stahlke Prado se debruçam sobre o tema da regulação jurídica da utilização e aproveitamento do solo e como o Direito intervém sancionando administrativa e criminalmente condutas que implicam lesão ou perigo de lesão ao ordenamento urbano.

O artigo “CONTROVÉRSIAS SOBRE O CONCEITO DE CONTUMÁCIA NO CRIME DE SONEGAÇÃO FISCAL”, de Marcelo Batista Ludolf Gomes, aborda a dificuldade quanto à definição deste novel conceito trazido pelo Supremo Tribunal Federal ao crime de sonegação fiscal.

Por fim, o artigo intitulado “A CONSTITUCIONALIZAÇÃO DO DIREITO PENAL E A LIMITAÇÃO TEMPORAL DAS MEDIDAS DE SEGURANÇA”, de Daniela Carvalho Almeida Da Costa e Gabriela Silva Paixão, abordam a temática da duração máxima da medida de segurança na jurisprudência dos tribunais superiores.

O(a) leitor(a), por certo, perceberá que os textos, além de ecléticos, são críticos quanto à realidade do sistema penal, o que reflete o compromisso dos(as) autores(as) na busca pelo aperfeiçoamento do direito material e processual penal em prol da melhor e maior adequação ao texto constitucional e às demandas da contemporaneidade, dentro de um modelo integrado de Ciências Criminais.

Tenham todos(as) ótima leitura, é o que desejam os organizadores!

Prof. Dr. Alceu de Oliveira Pinto Júnior – UNIVALI

Prof. Dr. Luiz Gustavo Gonçalves Ribeiro – ESDHC

Prof. Dr. Maiquel Ângelo Dezordi Wermuth – UNIJUÍ

CIBERCRIME E A NECESSÁRIA REFORMA DA LEGISLAÇÃO PENAL BRASILEIRA

CYBERCRIME AND THE NECESSARY REFORM OF BRAZILIAN CRIMINAL LEGISLATION

Clarisse Aparecida Da Cunha Viana Cruz
Daniel Brasil de Souza [1]
Pedro José de Campos Garcia [2]

Resumo

Este artigo analisou o cibercrime. Por ser tema recente, o problema discutido é se a legislação penal brasileira é suficiente para proteger os cidadãos contra esse delito. Por conseguinte, há uma breve explanação de sua origem e a classificação dos tipos penais que a englobam. Após, foram expostos os principais ditames legais que tratam do assunto. A metodologia utilizada é a jurídico-teórica e o procedimento dedutivo, juntamente à pesquisa bibliográfica. Por fim, concluiu-se que, diante das incertezas e da exposição que o meio digital coloca seus usuários, a legislação penal vigente é insuficiente na proteção dos cidadãos contra os cibercriminosos.

Palavras-chave: Cibercrime, Código penal brasileiro, Crime virtual, Dispositivos eletrônicos, Internet

Abstract/Resumen/Résumé

This article looked at cybercrime. As it is a recent issue, the issue discussed is whether Brazilian criminal law is sufficient to protect citizens against this crime. Therefore, there is a brief explanation of its origin and the classification of penal types that comprise it. Afterwards, the main legal dictates that deal with the subject were exposed. The methodology used is the legal-theoretical and the deductive procedure, together with the bibliographical research. Finally, it was concluded that, given the uncertainties and exposure that the digital medium places its users, the current criminal legislation is insufficient to protect citizens against cybercriminals.

Keywords/Palabras-claves/Mots-clés: Cybercrime, Brazilian criminal code, Cyber crime, Electronic devices, Internet

[1] Mestrando em Direito Ambiental pela Escola Superior Dom Hélder Câmara. Advogado. ORCID: https://orcid.org/0000-0003-2053-5443. Currículo Lattes: http://lattes.cnpq.br/6863844865812490. E-mail: souzadanielbrasil@hotmail.com

[2] Mestrando em Direito pela Escola Superior Dom Hélder Câmara. Superintendente de Regularização Fundiária da Secretaria de Estado de Agricultura, Pecuária e Abastecimento de Minas Gerais. Currículo Lattes: http://lattes.cnpq.br/3856390702087969. E-mail: pedrojcgarcia19@gmail.com

1 INTRODUÇÃO

Na atualidade, é incontestável o papel que as novas tecnologias de informação e comunicação ocupam na sociedade, tornando-se, através da internet, essenciais para a vida social, cultural, econômica, laboral e política dos cidadãos.

No entanto, essa facilidade de comunicação e de dispersão de dados também cria riscos à segurança pessoal de cada usuário na medida em que há pessoas que utilizam de suposta invisibilidade propiciada nesse espaço para praticarem crimes, sendo essa prática conhecida como cibercrime. Por essa razão, este artigo se justifica, tendo em vista os prejuízos que esses criminosos podem causar por meio de seus ataques aos dispositivos eletrônicos e à internet, sendo extremamente necessário que haja uma ampla discussão social, acadêmica, jurídica e governamental a fim de encontrar meios para limitar essa ação.

Neste contexto, este artigo tem como problemática o estudo dos tipos penais vinculados ao cibercrime e o questionamento: a legislação penal brasileira vigente é suficiente para proteção dos cidadãos contra os cibercrimes?

Para responder essa questão, os objetivos traçados abarcam uma breve evolução histórica do surgimento da internet e do cibercrime, contextualizando-a a realidade nacional dentro desse assunto; a classificação penal do crime cibernético, mencionando os sujeitos envolvidos, tipo penal, espécies de condutas, ação penal cabível e processo investigatório e, por fim, a análise das perspectivas futuras para a legislação penal brasileira quanto à esse tipo penal, como a reforma do Código Penal e o Decreto nº 10.222/20.

Para tanto, foi utilizada a metodologia de pesquisa teórica, baseando-se em doutrinas, legislações, jurisprudências e dados sobre o tema, encontrados em livros, meios eletrônicos, textos acadêmicos e material de curso adquirido com recurso próprio, sendo o marco teórico a obra "Manual de Crimes Informáticos" de Damásio de Jesus (2016).

2 EVOLUÇÃO HISTÓRICA DA INTERNET E DO CIBERCRIME

De acordo com pesquisa do Centro Regional para o Desenvolvimento de Estudos sobre a Sociedade da Informação[1], três a cada quatro brasileiros têm acesso à internet, totalizando

[1] CENTRO REGIONAL DE ESTUDOS PARA O DESENVOLVIMENTO DA SOCIEDADE DA INFORMAÇÃO. Três em cada quatro brasileiros já utilizam a Internet, aponta pesquisa TIC domicílios 2019. **Notícias CETIC-BR**, maio 2021. Disponível em: https://cetic.br/pt/noticia/tres-em-cada-quatro-brasileiros-ja-utilizam-a-internet-aponta-pesquisa-tic-domicilios-2019/#:~:text=TIC%20Domic%C3%ADlios%202019-,Tr%C3%AAs%20em%20cada%20quatro%20brasileiros%20j%C3%A1%20utilizam%20a,aponta%20pesquisa

134 milhões de pessoas, sendo a navegação feita por dispositivos móveis, computadores, televisões e videogames.

Neste contexto, para adentrar no tema deste artigo, faz-se necessário, primeiramente, uma breve contextualização histórica sobre o desenvolvimento da internet e o surgimento do cibercrime.

A internet foi criada pelos americanos durante a Guerra Fria, em 1969, recebendo o nome de Arpanet, com o objetivo principal de elaborar uma rede de comunicação imune aos soviéticos e que possibilitasse a comunicação militar (LIMA, 2017, p.11).

Com o fim desse período, a permanência do uso dessa rede passou para os cientistas, que a expandiram em nível global através das universidades e de seus computadores com finalidade acadêmico-científica.

No Brasil, esse meio de comunicação ganhou notoriedade em 1995, quando o Ministério da Ciência e Tecnologia criou o Comitê Gestor da Internet com função de fomentar o desenvolvimento do serviço e recomendar padrões e técnicas para seu uso, sendo fornecida pela Embratel na modalidade discada e consolidando-se no país, em 1997, ao ser oferecida por empresas privadas a bancos, empresas e universidades, que adquiriam o produto com uso constante, estimando cerca de 5 milhões de usuários brasileiros no final do século (LIMA, 2017, p.12).

Em 2002, em função da estabilidade econômica nacional e da melhoria da infraestrutura do setor de telecomunicações, o uso de computadores e da internet foi unificado para todas as classes sociais, alcançando os índices supracitados na atualidade.

Quanto ao cibercrime, Jesus (2016, p.16) explica que sua primeira ocorrência foi registrada durante a década de 1960, na modalidade de alteração, cópia e sabotagem de sistemas computacionais, bem como que o termo "hacker[2]" já era usado durante a década de 1970, nos Estados Unidos, sendo a Flórida, o Estado pioneiro a legislar sobre informática.

Quanto à primeira iniciativa internacional no combate ao crime digital, essa ocorreu por meio da realização da Conferência sobre Aspectos Criminológicos do Crime Econômico, em 1976, seguida pela Convenção de Budapeste[3] , em 2000, ambas realizadas pelo conselho europeu.

%20TIC%20Domic%C3%ADlios%202019&text=Apesar%20do%20aumento%20significativo%20nos,milh%C3%B5es%20de%20pessoas)%20seguem%20desconectados. Acesso em: 20 ago. 2021.

[2] Quem invade sistemas computacionais ou computadores para acessar informações confidenciais ou não autorizadas, apontando possíveis falhas nesses sistemas (DICIO, 2020).

[3] CONVENÇÃO DE BUDAPESTE. **Convenção sobre o Cibercrime**. 2001. Disponível em: http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf . Acesso em: 20 ago. 2021.

Essa última conferência resultou em um documento internacional que traz, em seu preâmbulo, o objetivo de proteger a sociedade contra a criminalidade no ciberespaço através da adoção de legislação adequada e cooperação internacional, frente às profundas mudanças provocadas pela digitalização e globalização permanente das redes informáticas.

Destaca-se que sua finalidade principal é a de criar normas comuns aos países signatários para possibilitar a cooperação internacional, mas não impede que cada Estado escolha como usará o tratado em sua legislação nacional.

Para alcançar esse objetivo, o texto resultante dessa convenção foi dividido em quatro capítulos e 48 artigos, sendo o primeiro capítulo referente às terminologias usadas no texto; o segundo capítulo aborda as medidas cabíveis em nível nacional, englobando o direito penal material, como as infrações relacionadas com computadores, conteúdo ou violação de direito autoral e outras formas de responsabilização e sanções, bem como o direito processual penal; o terceiro capítulo trata da cooperação internacional e o último traz as disposições finais.

Quanto ao Direito Penal Material, o tratado classifica o cibercrime em nove categorias, sendo:

> a) Acesso ilícito - Art. 2º: da prática intencional de acesso ilícito a um sistema informático ou parte dele;
> b) Intercepção ilícita - Art. 3º: da prática intencional a interceptação não autorizada;
> c) Dano provocado nos dados - Art. 4º: da prática intencional à danificação, a exclusão de dados, a deterioração, a alteração ou supressão não autorizada de dados;
> d) Sabotagem informática - Art. 5º: da prática intencional, a perturbação grave e não autorização quando do funcionamento de um sistema informático mediante inserção, transmissão, danificação, eliminação, deterioração, alteração ou supressão de dados;
> e) Utilização indevida do dispositivo - Art. 6º: da prática intencional e ilícita, a saber: produção, venda, aquisição para efeitos de utilização, importação, distribuição e suas outras formas e estar em possa de material criminoso;
> f) Falsificação informática - Art. 7º: da prática intencional e ilícita, a introdução, a alteração, a exclusão ou a supressão de dados dos quais não resultem em autenticidade;
> g) Burla informática - Art. 8º: da prática intencional e ilícita, prejuízo patrimonial causado a outrem por meio de qualquer introdução, alteração, exclusão ou supressão de dados, bem como, qualquer interferência nas funções de um sistema informático com a intenção de benefício econômico;
> h) Infrações relacionadas com pornografia infantil - Art. 9º: quando da prática de forma intencional e ilegítima por meio de um sistema informático: produção, oferta, disponibilização, difusão, posse e deverá abranger a todos os menores de 18(dezoito) anos de idade; e i) Infrações relacionadas a violação de direitos autorais e conexos - Art . 10º (BUDAPESTE, 2000).

O artigo 11 dá a liberdade para que cada Estado adote as medidas cabíveis para aqueles que tentarem e/ou foram cúmplices da prática ilícita, determinando também, no artigo 13, que cada um adote sanções eficazes, proporcionais e dissuasivas, incluindo penas privativas de liberdade e pecuniárias a fim de evitar reincidência.

Sobre o Direito Processual Penal, o tratado dispõe que cada membro adotará medidas legislativas e outras necessárias para criar poderes e procedimentos para investigação e procedimento penal, cabendo a apreensão de materiais informáticos relacionados às infrações constante no direito penal material, cometidas por meio informático ou com prova eletrônica.

Em âmbito nacional, Jesus (2016, p.24) menciona que o Brasil é o quarto país no mundo com maior número de ameaças virtuais, tendo atingido 77 mil brasileiros em 2011, causando-lhes prejuízos de até R$104 bilhões, sendo R$ 900 milhões só em fraudes bancárias e roubo de senhas.

Esse índice foi atualizado pelo Norton Cyber Security (2017)[4], que informou que o país passou a ser o segundo no ranking de número de casos de crimes virtuais, afetando 62 milhões de pessoas e prejudicando US$ 22 bilhões.

Cabe mencionar que o país não é signatário da Convenção de Budapeste, tendo, entretanto, sido por ela influenciado, ao promulgar as Leis nº 12.735/2012 e 12.737/2012, que alteraram o Código Penal Brasileiro ao abordarem a temática do crime cibernético, sendo aspectos dessas legislações estudados no próximo tópico.

3 DIREITO DIGITAL E A CLASSIFICAÇÃO PENAL DO CIBERCRIME

Conforme mencionado, através da globalização e suas tecnologias, a humanidade evoluiu em vários aspectos, sendo que, através da internet e da informática, essa evolução tornou-se constante, tendo em vista que a maioria dos cidadãos passam grande parte de seu dia *online*, compartilhando seu cotidiano, recebendo e compartilhando notícias e resolvendo problema em um *click.*

Nesse sentido, sendo o Direito uma ciência sociocultural, fez-se necessário que os estudos jurídicos se voltassem para esse novo ramo e seus efeitos na vida das pessoas, surgindo, então, o Direito Cibernético, que cuida de valores éticos e das relações oriundas da informática e do ciberespaço.

> (...) o Direito Digital não se limita à Internet, sendo a própria evolução do Direito onde a Internet é um novo recurso que deve ser juridicamente atendido, como todas as outras inovações que estejam por vir.
> Em tal realidade, o maior comprometimento dos operadores do Direito Digital é evitar qualquer tipo de arbitrariedade. Por isso, a discussão dos projetos de lei sobre temas que envolvem informática, Internet, e-commerce, crimes digitais, deve ser promovida

[4] UOL. Brasil é o segundo país no mundo com maior número de crimes cibernéticos. Uol **Notícias**: São Paulo, 2018. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2018/02/15/brasil-e-o-segundo-pais-no-mundo-com-maior-numero-de-crimes-ciberneticos.htm. Acesso em: 20 ago. 2021.

> através de um diálogo direto com a sociedade civil, envolvendo empresas e organizações sociais (...)
> As características do Direito Digital, portanto, são as seguintes: celeridade, dinamismo, autorregulamentação, poucas leis, base legal na prática costumeira, uso da analogia e solução por arbitragem (PINHEIRO, 2016, p.82).

Quanto aos cibercrimes, a autora explica que legislar sobre essa matéria é extremamente difícil e delicado, tendo em vista que "sem a devida redação do tipo penal, corre-se o risco de acabar punindo o inocente" (PINHEIRO, 2016, p.378).

Ratificando o posicionamento de Patrícia Pinheiro, Jesus (2016, p. 47) afirma que "nosso Decreto-Lei n. 2.848/40, embora tutele a maioria dos delitos informáticos, é omisso em questões onde a informática deveria ser o bem protegido pelo Direito Penal".

Entretanto, diante da repercussão midiática do caso da atriz global que teve seu celular invadido e fotos íntimas vazadas, foi sancionada a Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, em uma referência ao caso mencionado, elevando a informática ou a privacidade e a integridade dos dados informáticos a um bem juridicamente tutelado e inserindo o cibercrime na legislação brasileira.

3.1 Conceituação e tipo penal

Segundo as recomendações da *Organization for Economic Cooperation and Development* (OECD, 1986) mencionadas por Jesus (2016, p. 49), crime digital é:

> (...) qualquer comportamento ilegal, antiético ou não autorizado, envolvendo processamento automático e transmissão de dados, podendo implicar a manipulação de dados ou informações, falsificação de programas, o acesso e/ou uso não autorizado de computadores e redes (JESUS *apud* OECD, 2016, p.49).

Pinheiro (2016, p. 380) entende ainda que não se trata de crime de fim por natureza, ou seja, "crime cuja modalidade só ocorra em ambiente virtual (...). Isso quer dizer que o meio de materialização da conduta criminosa pode ser virtual, mas, em certos casos, o crime não".

Sobre essa classificação, o Supremo Tribunal Federal entende que o crime eletrônico pode ser crime de meio ou crime-fim, atacando-se o próprio ambiente virtual ou sistema de dados, conforme julgado do Habeas Corpus nº 84561/PR pelo Ministro Joaquim Barbosa:

> CRIME DE COMPUTADOR: PUBLICAÇÃO DE CENA DE SEXO INFANTO-JUVENIL (E.C.A., ART. 241), MEDIANTE INSERÇÃO EM REDE BBS/INTERNET DE COMPUTADORES, ATRIBUÍDA A MENORES: TIPICIDADE: PROVA PERICIAL NECESSÁRIA À DEMONSTRAÇÃO DA AUTORIA: HC DEFERIDO EM PARTE.

> 1. O tipo cogitado - na modalidade de 'publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente' - ao contrário do que sucede por exemplo aos da Lei de Imprensa, no tocante ao processo da publicação incriminada é uma norma aberta: basta-lhe à realização do núcleo da ação punível a idoneidade técnica do veículo utilizado à difusão da imagem para número indeterminado de pessoas, que parece indiscutível na inserção de fotos obscenas em rede BBS/Internet de computador.
> 2. Não se trata no caso, pois, de colmatar lacuna da lei incriminadora por analogia: uma vez que se compreenda na decisão típica da conduta criminada, o meio técnico empregado para realizá-la pode até ser de invenção posterior à edição da lei penal: a invenção da pólvora não reclamou redefinição do homicídio para tornar explícito que nela se compreendia a morte dada a outrem mediante arma de fogo.
> 3. Se a solução da controvérsia de fato sobre a autoria da inserção incriminada pende de informações técnicas de telemática que ainda pairam acima do conhecimento do homem comum, impõe-se a realização de prova perícia (BRASIL, Supremo Tribunal Federal. HC 84561/PR. Rel. Min. Joaquim Barbosa. Brasília, out. 2004) [5].

Para este artigo, adotar-se-á a conceituação de cibercrime como sendo fato típico e antijurídico cometido por meio da ou contra a tecnologia da informação.

O legislador brasileiro, por meio da Lei nº 12.737/12, dispôs sobre a tipificação penal de delitos informáticos, alterando o CPB em seus artigos 154, 266 e 298, especificando os crimes informáticos de invasão de dispositivo informático; interrupção de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública e falsificação de documento particular, inserindo a modalidade falsificação de cartão.

Quanto à primeira alteração, o art. 154 teve incorporado o art. 154-A e 154-B que dispõem:

> Art. 154-A. Invadir disposto informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismos de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita
> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos (BRASIL, 2012).

Para a conduta é prevista pena de detenção de 03 (três) meses a 1 (um) ano e multa, advertindo que a sanção é aplicável também a quem produz, oferece, vende ou difunde dispositivos ou programas de computadores que tem por objetivo permitir a prática da conduta criminosa, sendo que se de tal invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais/industriais, informações sigilosas ou o controle

[5] BRASIL. Supremo Tribunal Federal. **HC 84561/PR**. Rel. Min. Joaquim Barbosa. Brasília, 05 out. 2004. Disponível em: http://www.stf.jus.br/arquivo/informativo/documento/informativo364.htm#Crime%20pela%20Internet:%20Publica%C3%A7%C3%A3o%20de%20Cenas%20de%20Sexo%20Envolvendo%20Crian%C3%A7as%20e%20Adolescentes%20(HC/84561). Acesso em 12 set. 2021.

remoto não autorizado do dispositivo invadido em prejuízo econômico, a pena será de 06 (seis) meses a 02 (dois anos), majorando-se de um a dois terços, se houver divulgação, comercialização ou transmissão a outrem, dos dados e informações obtidos.

Ainda, caso o crime seja cometido contra chefes do executivo, legislativo, judiciário e dirigente máximo da administração pública direta e indireta federal, estadual, municipal ou do Distrito Federal, a pena aumentará de um terço a metade.

Quanto à segunda alteração, quem "interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento" sofrerá pena de detenção de um a três anos e multa, sendo a sanção dobrada, caso o crime seja cometido em situação de calamidade pública.

Por fim, a terceira alteração acrescentou ao crime de falsificação de documentação particular a falsificação de cartão, equiparando tal objeto a documento particular, imputando ao agente pena de reclusão de um a cinco anos. Assim, diante das modificações feitas pela Lei Carolina Dieckmann, os crimes virtuais previstos na legislação penal brasileira são:

Quadro 1: Crimes virtuais tipificados

CRIME	CONDUTA	PREVISÃO LEGAL
Invasão de dispositivo informático	Acesso sem autorização a dados automatizados de dispositivos eletrônicos com intenção ilegítima.	Art. 154-A do CPB
Interceptação ilegítima	Uso de meios técnicos, em transmissões não públicas, para interceptação e captura de dados e informações	Art. 10 da Lei nº 9.296/96
Dano informático	Danificar, apagar, deteriorar, alterar ou eliminar dados informáticos	Art. 154-B e Art. 163 do CPB
Interferência em sistemas	Conduta dolosa que causa obstrução grave, intencional e ilegítima, ao funcionamento de um sistema informático, por meio da introdução, transmissão, danificação, eliminação, deterioração ou supressão de dados informático	Art. 154-A do CPB
Falsidade ou fraude informática	Introdução, alteração, eliminação ou supressão intencional e ilegítima de dados informáticos, produzindo dados não autênticos, com a intenção de que sejam considerados ou utilizados legalmente como se fossem autênticos	Art. 299 do CPB Se praticado por funcionário público contra a Administração Pública: art. 313-A do CPB.
Furto de dados ou vazamento de informações	Copiar ou mover, indevidamente, informações protegidas ou confidenciais	Art. 154-A, §1º do CPB

Fonte: Elaborado pelos autores com dados extraídos de Jesus (2016, p.42).

Especificamente no Brasil, Pinheiro (2016, p.381) explica que os crimes virtuais mais comuns são aqueles que usam da informática para prática de estelionato e divulgação de

pornografia infantil, visando resultados financeiros e sedo uma ramificação do crime organizado.

Como é matéria jurídica relativamente nova, a classificação doutrinária para o tipo penal dos crimes digitais não é padronizada, assim, será usada neste trabalho, aquela dada por Jesus (2016, p.23) que a divide em:

> a) crimes informáticos próprios: em que o bem jurídico ofendido é a tecnologia da informação em si. Para estes delitos, a legislação penal era lacunosa, sendo que, diante do princípio da reserva penal, muitas práticas não poderiam ser enquadradas criminalmente;
> b) crimes informáticos impróprios: em que a tecnologia da informação é o meio utilizado para agressão a bens jurídicos já protegidos pelo Código Penal brasileiro. Para estes delitos, a legislação criminal é suficiente, pois grande parte das condutas realizadas encontra correspondência em algum dos tipos penais;
> c) crimes informáticos mistos: são crimes complexos em que, além da proteção do bem jurídico informático (inviolabilidade dos dados), a legislação protege outro bem jurídico. Ocorre a existência de dois tipos penais distintos, cada qual protegendo um bem jurídico;
> d) crime informático mediato ou indireto: trata-se do delito informático praticado para a ocorrência de um delito não informático consumado ao final. Em Direito Informático, comumente um delito informático é cometido como meio para a prática de um delito-fim de ordem patrimonial. Como, por exemplo, no caso do agente que captura dados bancários e usa para desfalcar a conta corrente da vítima. Pelo princípio da consunção, o agente só será punido pelo delito-fim (furto) (JESUS, 2016, p.54).

Podem ser citados como exemplos de crimes impróprios, a pedofilia e a pornografia infantil (art. 247 do Estatuto da Criança e do Adolescente), crimes contra a propriedade, contra o Estado e incolumidade pública, falsa identidade, racismo, etc.

Cumpre mencionar que há o uso da analogia ao Código Penal para tipificar a maioria desses ilícitos penais, já previstos pela lei, sendo mais objetiva a sua identificação e punição em contrapartida aos demais, por serem crimes comuns.

3.2 Perfil do criminoso digital, competência e lugar do crime informático

Conforme mencionado no tópico acima, o criminoso digital pode ser qualquer pessoa com os mínimos conhecimentos de informática e tecnologia. Nas palavras de Silva (2004, p.03):

> O perfil do criminoso, baseado em pesquisa empírica, indica jovens, inteligentes, educados, com idade entre 16 e 32 anos, do sexo masculino, magros, caucasianos, audaciosos e aventureiros, com inteligência bem acima da média e movidos pelo desafio da superação do conhecimento, além do sentimento de anonimato, que bloqueia seus parâmetros de entendimento para avaliar sua conduta como ilegal, sempre alegando ignorância do crime e, simplesmente, ‘uma brincadeira’. (SILVA, 2004.p.3).

Quanto à competência para julgar os cibercrimes, essa está nos artigos 5º ao 7º do CPB, referindo-se a crimes cometidos em território nacional. Assim, se o crime foi cometido contra bens da União ou se por Convenção ou Tratado o Brasil se obrigou a reprimir (art. 109, IV/CF), a Justiça Federal será a competente para julgá-lo; quanto aos crimes comuns, esses serão remetidos à Justiça Comum ou ao Juizado Especial Criminal, de acordo com a pena prevista, sendo que para o concurso de crimes, será sanção do crime mais grave.

Quanto ao lugar do crime, o CPB adota a teoria da ubiquidade, sendo local do ato ilícito aquele onde ocorreu a ação ou omissão, no todo ou em parte, bem como onde foi produzido o resultado.

De acordo com art. 70, §2º do CPB, quando a execução do crime tenha ocorrido no exterior, a competência será do local da infração, destacando-se que, conforme art. 7º, II, §2º, a e b do CPB, tratando-se crime praticado por brasileiro contra vítima no Brasil, a conduta praticada pelo agente será considerada ilícita em ambos os países.

Vale mencionar, por fim, que o criminoso pode, também, programar robôs para dispararem ofensas e publicar *fake news* na Internet a fim de atingir uma determinada pessoa, como foi feito no caso do Inquérito nº 4.781/19 da Polícia Federal, em que descobriram que um agente programou robôs para dar publicidade a ofensas contra a honra e dignidade dos membros do Supremo Tribunal Federal.

3.3 Da investigação e provas do cibercrime

Conforme mencionado no item anterior, para que o cibercrime seja consumado, há, impreterivelmente, a necessidade do corpo de delito nos materiais encontrados.

Como corpo de delito entende-se "o conjunto de vestígios deixados pela infração penal" e o exame de corpo de delito como a "análise e o registro feito por peritos acerca do material observado" (EMAG, 2017, p. 180). Nesse sentido, para evitar erros técnicos de julgamento e para garantir o devido processo legal, o Código de Processo Penal impõe como regra a realização desse exame para comprovar a materialidade delitiva, conforme art. 158 e ainda:

> No caso dos crimes cibernéticos, o exame supracitado é inevitável: não havendo como confirmar de modo seguro a sua existência e sua extensão sem constatar o caminho lógico percorrido pelo criminoso dentro do ambiente virtual, até mesmo determinando a origem dos atos executórios (EMAG, 2017, p.183).

Já o Marco Civil da Internet (MCI), Decreto nº 8.771/16, determina que os provedores de conexão e aplicação devem guardar informações de usuários que utilizaram determinado serviço, como a data e hora da conexão, além de excluir os dados de usuários tão logo termine o prazo de retenção, sendo de 06 meses para provedores de aplicação[6] e 01 ano para provedores de conexão[7] (BRASIL, 2016).

Destaca-se que os provedores de Internet, nacionais ou estrangeiros que descumprirem o disposto acima, podem sofrer as sanções do art. 12 do MCI, sendo a mais efetiva a de multa de até 10% do faturamento do grupo econômico no Brasil no seu último exercício.

Dessa análise e coleta de informações são formadas as provas que pode ser arquivos digitais, registros de servidores, o histórico de navegadores, fotos e vídeos, e-mails e registros de conversas online. Entretanto, essas provas são voláteis, podendo ser rapidamente danificadas ou alteradas, dificultando a investigação ou identificação de criminosos, razão pela qual a coleta de tais vestígios segue rigorosos mecanismo de preservação.

No contexto dos crimes digitais, esses rastros tornam-se evidências, sendo essenciais para a comprovação da materialidade do crime, bem como para definir sua autoria para que o juízo possa atuar. Assim, após a identificação do imóvel de onde partiram os acessos à internet, cumprem-se os mandados de busca e apreensão, priorizando os materiais que possam conter vestígios digitais:

> (...) Faz-se a arrecadação ou apreensão do material que não foi excluído pela avaliação de conteúdo, com descrição detalhada dos materiais. Efetua-se uma explanação do procedimento executado para avaliação do conteúdo das mídias digitais, seja no auto circunstanciado da busca, seja em documento apartado. Em alguns crimes, como dispõe o art. 241-B da Lei n.º 8.069/90, que trata da posse de material contendo cena de sexo explícito ou pornográfica envolvendo criança ou adolescente, esse documento formaliza os procedimentos realizados na busca que trouxeram convicção à equipe e às testemunhas para a prisão em flagrante, se identificado o proprietário daquele material (EMAG, 2017, p.2017).

Há, ainda, a opção de cópia dos dados para aquelas hipóteses em que os vestígios estão em grandes servidores de empresas ou acessíveis apenas na nuvem, sendo útil, também, para fornecê-los à vítima.

[6] Provedor de aplicação é a pessoa física ou jurídica que utiliza do acesso à internet para prestar serviços, como de e-mail, de hospedagem etc. (EMAG, 2017, p.23).

[7] Provedor de conexão é a pessoa jurídica fornecedora de serviços que possibilitam o acesso dos consumidores à internet, como a Tim, Claro, Vivo etc. (EMAG, 2017, p.23).

A fim de elucidar com um caso concreto o que foi disposto até aqui, cita-se o inquérito nº 4.781/19, realizado a mando do Supremo Tribunal Federal, para investigar os autores de ataques virtuais à honra, imagem e credibilidade dos ministros da corte[8].

Durante a investigação, policiais federais apreenderam aparelhos eletrônicos dos suspeitos, que também tiveram suas contas das redes sociais bloqueadas, sendo que, no laudo pericial, os investigadores relataram que identificaram a existência de um mecanismo coordenado de criação e divulgação das mensagens entre os investigados, feito por robôs, com o objetivo de atingir número considerável de pessoas.

Por fim, quanto ao momento da realização da prova técnica, essa pode ser feita logo no início da investigação, sendo que no caso dos crimes virtuais, deve ser feita ainda na fase inquisitiva para viabilizar o indiciamento do investigado e auxiliar a formação de opinião do Ministério Público.

4 PERSPECTIVAS FUTURAS PARA A LEGISLAÇÃO BRASILEIRA SOBRE O TEMA

No bojo dessa revolução tecnológica digital, cabe ao Direito, aos três poderes e as autoridades se atualizarem para acompanharem a evolução constante dos meios eletrônicos e informáticos, bem como a velocidade em que informações são divulgadas, para que possam efetivamente aplicar as normas sancionadas, proporcionando uma sociedade de informação minimamente segura.

> O maior problema jurídico dos crimes virtuais é a raridade de denúncias e, pior, o despreparo da polícia investigativa e de perícia para apurá-las. Embora já seja possível fazer boletins de ocorrência pela internet, são poucas as equipes e profissionais preparados para a investigação de um crime virtual (PINHEIRO, 2016, p. 382).

A autora também pondera que o maior impulso para os cibercrimes é dado pela crença de que o ciberespaço é um ambiente marginal, um "submundo em que a ilegalidade impera" (PINHEIRO, 2016, p. 384), tendo em vista que a sociedade acredita que esse meio não é devidamente vigiado e os crimes não são adequadamente punidos. Além disso, diz que há três razões para o aumento dos crimes digitais:

[8] GAZETA DO POVO. Como a PF chegou a suspeitos de fake news contra STF e de qual crime eles são acusados. **Jornal Online Gazeta do Povo**: Brasília, 27 maio 2020. Disponível em: https://www.gazetadopovo.com.br/republica/policia-federal-suspeitos-propagar-fake-news-contra-stf/. Acesso em: 08 set. 2021.

> 1ª) Crescimento dos usuários de internet e demais meios eletrônicos, principalmente junto à baixa renda (classes C e D) e que se tornam vítimas fáceis, pois ainda não possuem cultura de uso mais seguro. 2ª) Quanto mais pessoas no meio digital, os bandidos profissionais (quadrilhas) também migram, e então há maior ocorrência de incidentes. 3ª) Falta de conscientização em segurança da informação, a maior parte das pessoas acham que nunca vai ocorrer com ela, empresta senha, deixa o computador aberto e ligado, não se preocupa em usar ferramentas de modo diligente, isso somado com uma dose de inocência (PINHEIRO, 2016, p. 392).

Diante desses fatos, há que se acompanhar as medidas tomadas pelo governo federal no intuito de atualizar a legislação penal brasileira quanto à prática das modalidades de cibercrime. Nesse sentido, destacam-se os decretos nº 9.637/2018 e nº 10.222/2020, bem como a publicação da Lei nº 14.155/2021.

4.1 Decreto nº 9.637/2018, Decreto nº 10.222/2020 e a Lei nº 14.155/21

Diante do cenário de constante evolução na tecnologia da informação, o governo federal publicou o Decreto nº 9.637/2018, instituindo a Política Nacional de Segurança da Informação (PNSI). Sua finalidade é de "assegurar a disponibilidade, a integralidade, a confidencialidade e a autenticidade da informação a nível nacional" (BRASIL, 2018) usando como instrumentos a Estratégia Nacional de Segurança Cibernética (E-Cyber) e os planos nacionais, que deverão conter:

> Art. 6º A Estratégia Nacional de Segurança da Informação conterá as ações estratégicas e os objetivos relacionados à segurança da informação, em consonância com as políticas públicas e os programas do Governo federal, e será dividida nos seguintes módulos, entre outros, a serem definidos no momento de sua publicação:
> I - segurança cibernética;
> II - defesa cibernética;
> III - segurança das infraestruturas críticas;
> IV - segurança da informação sigilosa; e
> V - proteção contra vazamento de dados.
> Parágrafo único. A construção da Estratégia Nacional de Segurança da Informação terá a ampla participação da sociedade e dos órgãos e das entidades do Poder Público (BRASIL, 2018).

Em 05 de fevereiro de 2020, o presidente Jair Bolsonaro publicou o Decreto nº 10.222 no qual aprova a Estratégia Nacional de Segurança Cibernética (E-Cyber), referindo-se às principais ações que o governo federal pretende colocar em prática entre 2020 e 2023 na área da segurança cibernética, incumbindo aos órgãos e entidades federais possibilitar a implementação das ações estratégicas previstas, dispondo:

> Os rápidos avanços na área de tecnologia da informação e comunicação resultaram no uso intenso do espaço cibernético para as mais variadas atividades, inclusive a oferta de serviços por parte do Governo federal, em coerência com as tendências globais. Entretanto, novas e crescentes ameaças cibernéticas surgem na mesma proporção, e colocam em risco a administração pública e a sociedade.
> Desse modo, proteger o espaço cibernético requer visão atenta e liderança para gerenciar mudanças contínuas, políticas, tecnológicas, educacionais, legais e internacionais. Nesse sentido, o Governo, a indústria, a academia e a sociedade em geral devem incentivar a inovação tecnológica e a adoção de tecnologias de ponta, e manter constante atenção à segurança nacional, à economia e à livre expressão (BRASIL, 2020).

O texto legal menciona que a tecnologia utilizada na segurança sistêmica deve apoiar as políticas que "garantam os princípios fundamentais da autenticidade e da integridade de dados e prover mecanismo para proteção da legitimidade contra sua alteração ou eliminação não autorizada" (BRASIL, 2020), bem como que as informações coletadas devem ser acessíveis apenas para pessoas, processo ou entidades autorizadas.

Por meio da E-Cyber, a administração pública federal quer tornar o Brasil mais próspero e confiável no ambiente digital, aumentar a resiliência brasileira às ameaças cibernéticas e fortalecer a atuação brasileira em segurança cibernética no cenário internacional.

Para tanto, conforme os subitens 2.3.1 ao 2.3.10 do anexo do decreto, o governo pretende: fortalecer as ações de governança cibernética; estabelecer um modelo centralizado de governança no âmbito nacional; promover ambiente participativo, colaborativo, confiável e seguro, entre setor público, privado e sociedade, elevar o nível de proteção do governo; elevar o nível de proteção das infraestruturas críticas nacionais e aprimorar o arcabouço legal sobre a segurança cibernética; incentivar a concepção de soluções inovadoras em segurança cibernética; ampliar a cooperação internacional do Brasil em segurança cibernética; ampliar a parceria, em segurança cibernética, entre setor público, setor privado, academia e sociedade e elevar o nível de maturidade da sociedade em segurança cibernética.

Seguindo essa lógica, o presidente da República também sancionou o Projeto de Lei nº 4.554/2020, culminando na publicação da Lei nº 14.155/21, visando alterar o Código Penal Brasileiro “para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet” (BRASIL,2021). A partir de então, quem invadir dispositivo eletrônico alheio, sem prévia autorização, com o objetivo de obter, modificar ou destruir dados/informações ou de instalar programas invasores para obter vantagem ilícita sofrerá pena de reclusão, de 1 a 4 anos e multa. Ainda, se desse fato resultar prejuízo econômico, a pena será aumentada de 1 a 2/3, sendo que, se dessa conduta o criminoso obter conteúdo eletrônico privado e sigiloso, a pena de reclusão passará para 02 a 05 anos, e multa.

Quanto ao crime de furto mediante fraude, se esse for cometido por meio de "dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo" (BRASIL, 2021), a pena será de reclusão, de 04 a 08 anos e multa. Ainda, se essa conduta for praticada mediante servidor localizado fora do Brasil, a pena será aumentada de 1/3 a 2/3 e de 1/3 ao dobro, se o ato for feito contra idoso ou vulnerável.

Entretanto, apesar dessas medidas, cumpre destacar que o Brasil é o 66º no ranking da ONU de tecnologia da informação; sendo que, de 2019 para 2020, o número de denúncias de crimes cibernéticos dobrou, passando de 75.428 para 156.692 por ano, o que representa o maior número de casos desde que a Central Nacional de Denúncias de Crimes Cibernéticos começou a contabilizá-los, em 2014. [9]

Ocorre que, na prática, o Estado é omisso na disponibilização de meios para que a polícia possa chegar aos criminosos, bem como não faz a devida divulgação das orientações das medidas de prevenção a serem tomadas pela sociedade, como as contidas no anexo do Decreto nº 10.222/2020, influenciando no aumento dos índices supramencionados.

5 CONCLUSÃO

Ao final deste artigo, conclui-se que a legislação penal brasileira não é suficiente para proteger os cidadãos contra os cibercrimes. No presente cenário de ameaças e evolução cibernéticas, os cibercrimes e as legislações que visam sua prevenção e punição devem ser tratadas como uma questão social a serem discutidas em todos os âmbitos, de maneira colaborativa.

Um exemplo, neste contexto, seria a criação de uma plataforma ou sistema que possibilite o compartilhamento de ameaças virtuais através de boletins ou alertas ao acessar determinada página, aplicativo etc.

Outra possibilidade seria a ação conjunta entre os participantes da administração pública direita e indireta e empresas privadas para criação de um necessário alinhamento estratégico e operacional nas ações concernentes ao ciberespaço, através, por exemplo de manuais, diretrizes e condutas para tratamento de potenciais incidentes, bem como regras de verificação de segurança nos dispositivos informáticos de todos os funcionários, auditorias

[9] DENÚNCIAS de crimes cometidos pela internet mais que dobram em 2020. **G1**, 09 fev. 2021. Disponível em https://g1.globo.com/economia/tecnologia/noticia/2021/02/09/numero-de-denuncias-de-crimes-cometidos-pela-internet-mais-que-dobra-em-2020.ghtml. Acesso em 03 out. 2021.

anuais, comunicação aos consumidores em caso de incidente que comprometa a segurança de seus dados em função de atualização de seu dispositivo, etc.

Destaca-se que o modelo centralizado de gestão de segurança virtual é viável e eficaz, sendo utilizado pelos Estados Unidos, Reino Unido, Portugal, Malásia e outros países que centralizaram o tema em um órgão determinado com autoridade para regulamentar as ações específicas, apresentando bons resultados, conforme consta no anexo I do Decreto nº 10.222/2020.

Além disso, o governo deveria dar maior enfoque e divulgação do disposto em sua legislação sobre o tema através da própria rede social e mecanismos de telecomunicação, de maneira a incentivar a prevenção aos ataques e denúncias, bem como de conscientizar a sociedade da sua importância na identificação e captação dos cibercriminosos.

Outro ponto importante mencionado pelos doutrinadores ao longo do trabalho é o investimento em capacitação dos profissionais na área da investigação para que consigam obter a prova digital de maneira rápida e eficaz para punir os criminosos.

No campo jurídico, uma lei específica sobre a segurança cibernética e cibercrimes teria a finalidade de alinhar essa ações governamentais e sociais a fim de diminuir a incidência dos crimes digitais e dar maior segurança para os brasileiros usarem a Internet e seus benefícios, bem como para não prejudicar drasticamente a economia nacional com os rombos já mencionados.

Destaca-se que os meios, como a aprovação da reforma no Código Penal e a E-Cyber já existem, cabendo aos interessados e a sociedade se empenharem para colocá-los em prática.

6 REFERÊNCIAS

BRASIL. Decreto-Lei 2.848, de 07 de dezembro de 1940. Código Penal. **Diário Oficial da União**: Brasília, 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm . Acesso em: 17 ago. 2021.

BRASIL. Lei nº 9.296, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. **Diário Oficial da União**: Brasília, 1996. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm#:~:text=10.,a%20quatro%20anos%2C%20e%20multa. Acesso em: 07 set. 2021.

BRASIL. Supremo Tribunal Federal. **HC 84561/PR**. Rel. Min. Joaquim Barbosa. Brasília, 05 out. 2004. Disponível em: http://www.stf.jus.br/arquivo/informativo/documento/informativo364.htm#Crime%20pela%20Internet:%20Publica%C3%A7%C3%A3o%20de%20Cenas%20de%20Sexo%20Envolvendo%20Crian%C3%A7as%20e%20Adolescentes%20(HC/84561). Acesso em: 12 set. 2021.

BRASIL. Lei 12.735 de 30 de novembro de 2012. Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei no 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei no 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. **Diário Oficial da União**: Brasília, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm . Acesso em: 17 ago 2021.

BRASIL. Lei 12.737 de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. . **Diário Oficial da União**: Brasília, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 17 ago. 2021.

BRASIL. Decreto nº 9.637, de 26 de dezembro de 2018.
Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. **Diário Oficial da União**: Brasília, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9637.htm. Acesso em: 12 set. 2021.

BRASIL. Decreto nº 10.222, de 5 de fevereiro de 2020.
Aprova a Estratégia Nacional de Segurança Cibernética. **Diário Oficial da União**: Brasília, 2020. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419. Acesso em 12 set. 2021.

BRASIL. Lei nº 14.155, de 27 de maio de 2021. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. **Diário Oficial da União**: Brasília, 2021. Disponível em: https://legis.senado.leg.br/norma/34016289/publicacao/34016562. Acesso em: 03 out. 2021.

BRASIL. Tribunal Regional Federal da 3a Região. Escola de Magistrados. **Investigação e prova nos crimes cibernéticos**. São Paulo : EMAG, 2017.

CENTRO REGIONAL DE ESTUDOS PARA O DESENVOLVIMENTO DA SOCIEDADE DA INFORMAÇÃO. Três em cada quatro brasileiros já utilizam a Internet, aponta pesquisa TIC domicílios 2019. **Notícias CETIC-BR**, maio 2020. Disponível em: https://cetic.br/pt/noticia/tres-em-cada-quatro-brasileiros-ja-utilizam-a-internet-aponta-pesquisa-tic-domicilios-2019/#:~:text=TIC%20Domic%C3%ADlios%202019-,Tr%C3%AAs%20em%20cada%20quatro%20brasileiros%20j%C3%A1%20utilizam%20a,aponta%20pesquisa%20TIC%20Domic%C3%ADlios%202019&text=Apesar%20do%20aumento%20significativo%20nos,milh%C3%B5es%20de%20pessoas)%20seguem%20desconectados. Acesso em: 20 ago. 2021.

CONVENÇÃO DE BUDAPESTE. **Convenção sobre o Cibercrime**. 2001. Disponível em: http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf. Acesso em: 20 ago. 2021.

DENÚNCIAS de crimes cometidos pela internet mais que dobram em 2020. **G1**, 09 fev. 2021. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/02/09/numero-de-denuncias-de-crimes-cometidos-pela-internet-mais-que-dobra-em-2020.html. Acesso em: 03 out. 2021.

GAZETA DO POVO. Como a PF chegou a suspeitos de fake news contra STF e de qual crime eles são acusados. **Jornal Online Gazeta do Povo**: Brasília, 27 mai. 2020. Disponível em: https://www.gazetadopovo.com.br/republica/policia-federal-suspeitos-propagar-fake-news-contra-stf/. Acesso em: 08 set. 2020.

HACKER. In: DICIO, Dicionário Online de Português. Porto: 7Graus, 2020. Disponível em: https://www.dicio.com.br/hacker/#:~:text=Significado%20de%20Hacker,apontando%20poss%C3%ADveis%20falhas%20nesses%20sistemas.&text=%5BPejorativo%5D%20Indiv%C3%ADduo%20que%20invade%20outros,programas%20com%20prop%C3%B3sitos%20ilegais%3B%20cracker. Acesso em: 30 ago. 2020.

JESUS, Damásio de. **Manual de crimes informáticos** / Damásio de Jesus, José Antonio Milagre. – São Paulo: Saraiva, 2016.

SILVA, Mauro Marcelo de Lima e. **Os crimes digitais, hoje. Polícia revela o perfil do criminoso na Internet**. Disponível em: http://www.egov.ufsc.br/portal/sites/default/files/anexos/29333-29351-1-PB.htm. Acesso em: 07 set. 2021.

PINHEIRO, Patrícia Peck. **Direito Digital**. 6.ed.rev.,atual. e ampl. São Paulo: Saraiva, 2016.

UOL. Brasil é o segundo país no mundo com maior número de crimes cibernéticos. Uol **Notícias**: São Paulo, 2018. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2018/02/15/brasil-e-o-segundo-pais-no-mundo-com-maior-numero-de-crimes-ciberneticos.htm. Acesso em: 20 ago. 2020.