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

MEIO AMBIENTE DIGITAL E A AUTORIA DELITIVA NOS CRIMES CIBERNÉTICOS

DIGITAL ENVIRONMENT AND THE CRIMINAL AUTHORSHIP IN CYBER CRIMES

Júlio César Batista Pereira [1]
Reinaldo Caixeta Machado [2]

Resumo

Os avanços da informática e da tecnologia têm sido palco diário de ameaças à sociedade de risco, capazes de afetar diversos seguimentos que repercutem na seara jurídica e em um ambiente que foge da naturalidade, tradicionalmente tutelado pelo Direito. O presente trabalho tem o objetivo de analisar quais as maiores dificuldades encontradas para a apuração e repressão da autoria delitiva nos crimes cibernéticos. Foi possível se chegar a um resultado de que o Brasil possuí vários pontos a serem melhorados para possibilitar que haja uma apuração e repressão da autoria delitiva eficiente voltada às condutas criminosas neste meio ambiente digital.

Palavras-chave: Autoria, Cibercrimes, Internet, Sustentabilidade

Abstract/Resumen/Résumé

Advances in information technology have been the daily scene of threats to the risk society, capable of affecting various follow-ups and bringing serious behaviors that have an impact on the legal field and in an environment that escapes from naturalness. The present work aims to analyze the greatest difficulties encountered for the calculation and depression of criminal authorship in cybercrime. At the end of the research, it was possible to arrive at a result, that Brazil has several points to be improved to enable an efficient investigation and repression of delitive authorship aimed at criminal conduct in this digital environment.

Keywords/Palabras-claves/Mots-clés: Authorship, Cybercrimes, Internet, Sustainability

[1] Graduado em Direito pelo Centro Universitário do Cerrado Patrocínio (UNICERP). E-mail: julioc. advo@gmail.com.

[2] Mestre pela Escola Superior Dom Helder Câmara. Especialista en Derecho Ambiental frente al Câmbio Climático y Agotamiento de los Recursos Naturales (Castilla La Mancha – ES). Professor. E-mail contato@reinaldomachadoadvocacia.com.br

1 INTRODUÇÃO

Para discorrer sobre os crimes cibernéticos propriamente ditos, necessário se faz a realização de breve abordagem histórica, para entender o surgimento e a evolução desses tipos de delitos. Sendo assim, segundo Wendt e Jorge "*[...] em 1946 foi criado o primeiro computador digital, que ficou mundialmente conhecido como Electronic Numerical Integrator and Computer (ENIAC)"* (WENDT; JORGE, 2013, p.5), e que por sinal pesava mais de 30 toneladas e tinha como medida em torno de 145m² (cento e quarenta e cinco metros quadrados).

Com isso, em 1969 teve início a Advanced Research Projects Agency Network (ARPANET), uma rede capaz de integrar computadores que estivessem distantes e que por intermédio dela fosse permitida a comunicação de dados, inicialmente interligando as Universidades da Califórnia (Los Angeles e Santa Bárbara), a Universidade de Stanford (Santa Cruz) e a Universidade de Utah (Salt Lake City) (BRASIL ESCOLA, 2021).

Desta forma, em 1973 a "ARPANET", alterou seu protocolo de dados para o TCP/IP[1] responsável pela transmissão de dados pela internet, utilizado atualmente. Tal protocolo é um conjunto de camadas responsáveis por determinadas tarefas, a exemplo da comunicação entre o servidor de internet e computador local. Além disso, a denominação Internet Protocol "IP" em português protocolo de internet, é um número exclusivo atribuído a cada computador quando conectado à internet, tem como função sua identificação (WENDT; JORGE, 2013, p.4).

Quanto ao surgimento dos crimes informáticos, os primeiros indícios remontam à década de sessenta, e se diferem dos crimes praticados na atualidade, todavia, visavam da mesma forma a sabotagem de dispositivo informático para obtenção de vantagem ilícita.

Dito isto, foi no final da década de oitenta, que o "ARPANET", passou a ser denominado enfim de internet, isto devido à criação do "World Wide Web"[2] mundialmente utilizado e conhecido como "WWW", que basicamente é um conglomerado de documentos conectados em hipermídia, e executados na internet, são as páginas que são acessadas por meio de navegador de internet, como exemplo "Google Chrome, Mozilla Firefox, entre outros".

Bem assim, por volta de 1990 a internet começou a evoluir no Brasil, e com a evolução da tecnologia e a popularização do computador foi instituído um novo lugar onde o homem estabelece relações sociais. Consequentemente surgiu a necessidade de entender esse novo meio social, visto que as pessoas adentram no ambiente cibernético em seu local de

1 TCP/IP – Transmission Control Protocol.
2 WWW – World Wide Web.

trabalho, em sua residência ou durante o seu lazer, acumulando e transitando informações, dados, imagens e sons.

Portanto com essa evolução tecnológica surgiram riscos e criminosos especializados em práticas delitivas nesse novo ambiente – ou meio ambiente, sendo necessário criar maneiras de coibi-los e assegurar os direitos fundamentais a todos.

Dessa forma, surgem indagações: sobre quais as dificuldades que as polícias investigativas encontram para apuração e repressão de autoria delitiva nos crimes cibernéticos? Quais as possíveis soluções?

Neste diapasão, ao longo do artigo será realizada diferenciação sobre importantes conceitos relacionados aos crimes cibernéticos, tais como meio ambiente cibernético e a sociedade de risco, hacker e crackers, quais os sujeitos ativos e passivos destes delitos, a diferença entre crime próprio e impróprio. Além disso, será realizada abordagem sobre local do crime, jurisdição, competência, os princípios da territorialidade e extraterritorialidade, bem como tecer breves comentários acerca do direito comparado, por fim, serão analisadas as leis do ordenamento jurídico brasileiro que regulamentam o uso da internet e a jurisprudência, bem como discorrer sobre a prova da materialidade, objetivando responder a problemática apresenta acima.

2 Desenvolvimento

2.1. Meio Ambiente Cibernético e a Sociedade de Risco

No Brasil, corriqueiramente quando se fala em meio ambiente logo denota-se à associação das pessoas por ambientes naturais, com notável exuberância, muitas vezes intocável pelos humanos. Dessa forma, segundo disposto no inciso I, do art. 3º, da Lei 6.938/81 "*Meio ambiente é definido como o conjunto de condições, leis, influências e interações de ordem física, química e biológica, que permite, abriga e rege a vida em todas as suas formas*" (BRASIL, 1981).

Importante destacar que diferente do que as pessoas associam, existem o meio ambiente cultural, do trabalho, patrimônio genético, natural e artificial. Sendo que o cultural não diz respeito exclusivamente a um ambiente físico e palpável, e compreende todo o patrimônio imaterial cultural de uma sociedade ou grupo social. Já meio ambiente do trabalho, é caracterizado pelos espaços onde os cidadãos executam sua atividade profissional. O patrimônio genético, um dos mais recentes e desconhecidos tipos de meio ambiente, nele está tudo relacionado ao desenvolvimento de pesquisas genéticas.

Sendo assim, o chamado meio ambiente natural engloba a fauna, a flora, a atmosfera, o solo. Por fim, o artificial o qual é objeto deste estudo está relacionado a todo espaço

construído, como equipamentos urbanos e edifícios comunitários, ou seja, é aquele construído pelo homem, é a ocupação do espaço natural, transformando-o em artificial.

De acordo com José Afonso da Silva, o conceito de meio ambiente deve ser globalizante, "*abrangendo a natureza original, a artificial e os bens culturais correlatos"* (SILVA, 2004). Sendo assim, meio ambiente não se limita apenas ao natural, mas a todo ambiente que sirva de alicerce para as relações sociais.

O direito ao meio ambiente equilibrado é um direito fundamental difuso, essencial à sadia qualidade de vida e para a dignidade da pessoa humana. É ao mesmo tempo direito e dever a sua preservação para as presentes e futuras gerações. Este direito foi reconhecido em 1972, na Conferência das Nações Unidas sobre o Meio Ambiente Humano e tem previsão no caput do artigo 225, caput, da Constituição Federal de 1988 "*Todos tem direito ao meio ambiente ecologicamente equilibrado*" (BRASIL, 1988).

Neste sentido, Ricardo Silva Coutinho, define o meio ambiente cibernético como:

> […] manifestação da criação humana e parte integrante do patrimônio imaterial, sobretudo representado pela tecnologia do espectro eletromagnético (ondas de rádio, TV, celular e internet) que deve estar a serviço do desenvolvimento (sustentável) e, portanto, lucro e desenvolvimento aliado à preservação do meio ambiente (COUTINHO, 2014, p. 226).

Sendo assim, é importante destacar que o meio ambiente cibernético está inserido no meio ambiente artificial, ou seja, é uma construção humana, que começou a ser discutida no Brasil no século XXI, pois foi a partir daí que começou um novo processo civilizatório moldando assim uma nova vida (FIORILLO, 2013, p. 494).

O meio ambiente cibernético advindo da evolução tecnológica constitui, pois, um novo ambiente em que o homem estabelece relações sociais. Sendo que o usuário adentra nesse ambiente virtual em seu local de trabalho, na sua casa em seu momento de lazer, transitando grandes quantidades de dados. É possível, por meio da informática e da telemática[3] que as pessoas se relacionam entre si e com empresas, comunicando-se, adquirindo conhecimentos e efetuando transações comerciais e bancárias.

A partir do momento em que o ser humano passa a interferir no meio ambiente surgem os riscos, e, com estes, a necessidade de se dar importância à defesa da dignidade dos usuários deste

3 Dicionário Informal. Telemática é o conjunto de tecnologias da informação e da comunicação resultante da junção entre os recursos das telecomunicações (telefonia, satélite, cabo, fibras ópticas etc.) e da informática (computadores, periféricos, softwares e sistemas de redes), que possibilitou o processamento, a compressão, o armazenamento e a comunicação de grandes quantidades de dados (nos formatos texto, imagem e som), em curto prazo de tempo, entre usuários localizados em qualquer ponto do Planeta. Disponível em: https://www.dicionarioinformal.com.br/diferenca-entre/telem%C3%A1tica/inform%C3%A1tica/. Acesso em: 16 jun. 2021.

novo ambiente. Em decorrência disso, o direito ao meio ambiente de qualidade se mostra indispensável para a manutenção da própria garantia da justiça e estabilidade social nas sociedades.

Com efeito, mesmo a era digital trazendo consigo vários benefícios, também está vinculada a riscos cada vez mais abstratos, ou seja, quando as decisões humanas rompem os pilares da certeza estabelecidos pela sociedade, como consequência os seus padrões de segurança.

Desta forma, entendesse que o termo sociedade de risco foi desenvolvido pelo teórico social alemão Ulrich Beck. Dito isso, entendesse que sociedade de risco é fruto do desenvolvimento do modelo econômico que surge na revolução industrial, a partir da organização da produção de bens por meio de um sistema de livre concorrência mercadológica.

A lógica desse sistema exige dos agentes produtores a busca incessante por novas tecnologias que permitam uma produção e distribuição em larga escala, de forma, a atingir um número maior de consumidores através da agregação de técnicas inovadoras. Esse processo de inovação acaba criando uma dinâmica peculiar onde a velocidade e intensidade do progresso da ciência não são acompanhados pela análise dos feitos decorrentes da utilização das novas tecnologias (BOTTINI, 2007, p. 36).

De acordo com o doutrinador italiano Mario Giuseppe Losano "*as transformações sociais até agora provocadas pela informática têm caráter irreversível e plasmarão cada vez mais a sociedade dos próximos anos*" (LOSANO, 1995. p. 365). Semelhante é o entendimento de Sílvio de Salvo Venosa, para quem "*[..] o computador passou a fazer parte da rotina do homem comum"* (VENOSA, 2003, p. 593).

Neste sentido, segundo pesquisa TIC Domicílios[4], realizada anualmente pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (CETIC), uma das principais pesquisas no país, o número de brasileiros que usam a internet continua crescendo: entre 2018 e 2019 subiu de 70% para 79% da população, o que equivale a 133,8 milhões de pessoas usando a internet regularmente em 2019.

Neste diapasão, segundo Eduardo Diniz Neto, o Direito Penal moderno tem uma relevante missão frente a sociedade de risco, pois com a proliferação de diversas novas espécies de crime, denominados de delitos de perigo, não se deve esperar a produção efetiva de danos, mas agir antes mesmo de acontecer, de uma forma preventiva, de modo a tutelar efetivamente o bem jurídico (NETO, 2010).

Dito isto, (SILVA, 2017) ressalta que a falta de políticas públicas capazes de evitar efetivamente a criminalidade é um ponto de preocupação e um fator que contribui para o

4 CETIC. TIC Domicílios. Disponível em: https://cetic.br/pesquisa/domicilios/. Acesso em: 02 out. de 2020.

crescente número da população carcerária brasileira, que é uma das maiores do mundo. Neste sentido, dados do Infopen[5] apontam que o Brasil possui uma população prisional de 773.151 pessoas privadas de liberdade em todos os regimes.

Sendo assim, é importante frisar o dever do Estado não só de reprimir, mas também de realizar políticas públicas eficientes para combater a criminalidade, como o de criar a cultura do uso consciente da internet e dos equipamentos eletrônicos, visando coibir riscos à sociedade e assegurar os direitos fundamentais de toda coletividade.

Por fim, tem-se que o meio ambiente oferece condições essenciais para a sobrevivência e evolução. Condições estas que vem acompanhadas de riscos que influem sobre a saúde, podendo causar graves consequências para a qualidade de vida e para o desenvolvimento humano. Desta forma, resta demonstrada a necessidade de haver políticas públicas objetivando um meio ambiente cibernético dentro do que prevê as normas vigentes e que esteja condizente aos interesses de uma sociedade moderna cada dia mais dependente da tecnologia.

2.2. Crimes Cibernéticos

A terminologia adequada para conceituar crime cibernético ainda não é algo pacificado doutrinariamente, vez que comumente são denominados de: crimes digitais, cibercrimes, crimes informáticos, crimes virtuais, entre outros.

Nesse sentido,

> [...] não há uma nomenclatura sedimentada pelos doutrinadores acerca do conceito de crime cibernético. De uma forma ou de outra o que muda é só o nome atribuído a esses crimes, posto que devem ser observados o uso de dispositivos informáticos, a rede de transmissão de dados para delinquir, o bem jurídico lesado, e ainda deve a conduta ser típica, antijurídica e culpável (DA SILVA, 2015, p. 39)

Sendo assim, neste estudo, será adotado o conceito de crime cibernético por entender ser este suficientemente abrangente, isto que abarca as diversas atividades ilícitas que são praticadas contra dados e sistemas de computadores.

Deste modo, crime cibernético pode ser entendido como condutas ilegais efetivadas através de utilização de dispositivos informáticos, conectados ou não à rede mundial de computadores, além de ações criminosas contra equipamentos tecnológicos, sistemas de informação ou banco de dados. Isso posto, é definido como uma ação típica, antijurídica e culpável.

> [...] são denominados de "crimes de informática" as condutas descritas em tipos penais realizadas através de computadores ou voltadas contra computadores,

5 INFOPEN. **Levantamento Nacional DE INFORMAÇÕES PENITENCIÁRIAS INFOPEN - JUNHO DE 2014**. Disponível em: https://www.justica.gov.br/news/mj-divulgara-novo-relatorio-do-infopen-nesta-terca-feira/relatorio-depen-versao-web.pdf. Acesso em: 16 jun. 2021.

> sistemas de informática ou os dados e as informações neles utilizados (armazenados ou processados) (CASTRO, 2020).

Esta modalidade de crime tem como fator exponencial a transnacionalidade, que torna possível que pessoas com mínimo conhecimento informático realize práticas criminosa contra indivíduos de quaisquer lugares do planeta, outro assim, o aumento exacerbado de terminais eletrônicos pessoais, tendo no rol exemplificativo o computador.

2.2.1. Hackers e Crackers

No estudo dos crimes cibernéticos, é necessário compreender inicialmente a diferença entre hacker e cracker. Pois, ambos, detêm grandes conhecimentos informáticos, sendo o fator ético o que os diferenciam.

Os Hackers ou também conhecidos como White-hats[6] são pessoas consideradas do "bem" que possuem grande conhecimento sobre computadores e superam os limites das máquinas e dos programas. Em geral, eles partem do princípio de que todo sistema de segurança possui uma falha, e a função deles é justamente de encontrá-la (ASSUNÇÃO, 2002, p.82). Importante destacar que estes especialistas apenas documentam as vulnerabilidades detectadas e as reportam para a empresa contratantes de seus serviços, juntamente com indicações de como solucioná-las, aumentando com isso a segurança da organização, evitando prejuízos gigantescos. Além disso, auxiliam as autoridades a desvendar delitos praticados no espaço virtual.

Lado outro, os denominados Crackers ou black-hats, são os considerados "maldosos", possuem alto grau de conhecimento e nenhum respeito, invadem sistemas e deixam sua "marca" ou podem destruí-los completamente. Hackers e Crackers estão sempre em conflito, guerras entre grupos é comum, e isso pode ser observado em fóruns de discussões e em grandes empresas, as quais contratam hackers para proteger seus sistemas.

Sendo assim, um exemplo deste conflito é a história do cracker Kevin Mitnick que invadiu o computador do analista de sistemas Shimomura[7], destruiu dados e roubou informações vitais. Shimomura é chamado de hacker pois usa sua inteligência para o bem e com seu grande conhecimento montou um honeypot (armadilha que consiste em criar uma falsa rede para pegar o invasor), sendo tal ferramenta efetiva para a responsabilização de Kevim sobre os danos a ele causados.

---

6 White-hat em português significa: chapéu branco, entretanto black-hat significa: chapéu preto, termos derivados de filmes faroestes cujos personagens usavam um chapéu (hat, em inglês) branco ou preto, de acordo com a sua índole boa ou má. Disponível em: https://www.avira.com/pt-br/blog/hacker-e-chapeus-black-white-gray-hat. Acesso em: 16 jul. 2021.

7 Tsutomu Shimomura é um cientista da computação e especialista em segurança de sistemas japonês radicado nos Estados Unidos.

Curiosamente, ao noticiar os fatos acima, a imprensa acabou por confundir os termos, descrevendo o criminoso Kevin Mitnick de hacker, há muito tempo este termo vem sendo erroneamente associado aos criminosos da Internet.

2.2.2. Sujeito Ativo e Passivo

Sujeitos do crime são as pessoas ou entes relacionados à prática e aos efeitos adversos da empreitada criminosa. De acordo com Cleber Rogério Masson, "*sujeito ativo é a pessoa que realiza direta ou indiretamente a conduta criminosa, seja isoladamente, seja em concurso"* (MASSON, 2019, p. 322).

Pode ser uma pessoa comum, sem grandes conhecimentos técnicos sobre informática, programação e internet, como também, podem ser uma pessoa com conhecimento técnico aprofundado, a título de exemplo o "cracker".

Com intuito de conceituar sujeito passivo o autor ainda lembra que*"[...] é o titular do bem jurídico protegido pela lei penal violada por meio da conduta criminosa. Pode ser denominado de vítima ou de ofendido*" (MASSON, 2019, p. 322)

Com efeito, pode ainda figurar como sujeito passivo duas ou mais vítimas em um único delito. Além disso, aduz que podem serem sujeitos passivos tanto pessoa física quanto pessoa jurídica (ORRIGO; FILGUEIRA, 2015).

Portanto, no crime cibernético, o sujeito passivo é aquela pessoa física ou jurídica que, individualmente ou em coletivo, venha sofrer qualquer tipo de prejuízo em sistemas informatizados.

2.2.3. Crimes Cibernéticos Próprios e Impróprios

A doutrina especializada, classifica os crimes cibernéticos em crimes impróprios ou "abertos" e crimes próprios conhecidos também como "exclusivamente cibernéticos".

Os delitos informáticos abrangem crimes e contravenção penais, além disso, têm aplicação tanto nos delitos praticados utilizando como meio a internet, bem como naqueles onde o computador é apenas ferramenta para a prática do crime ou contravenção penal.

Nesse mesmo sentido:

> [...] Crimes cibernéticos "abertos" são aqueles que podem ser praticados da forma tradicional ou por intermédio de computadores, ou seja, o computador é apenas um meio para a prática do crime, que também poderia ser cometido sem o uso dele. "Já os crimes exclusivamente cibernéticos" são diferentes, pois eles só podem ser praticados com a utilização de computadores ou de outros recursos tecnológicos que permitem o acesso à internet" (WENDT; JORGE, 2013, p.19).

Logo, nos crimes próprios só é possível sua prática através de equipamentos que permitem o acesso à internet. Sendo que o bem jurídico protegido não é a inviolabilidade dos programas, mas, sim, da informação armazenada nos dispositivos informáticos, isto é, dos dados, essa inviolabilidade por sua vez é a manifestação do direito à privacidade e intimidade presente no art. 5º, X, da Constituição Federal de 1998 (VIANNA , 2013. P.21).

Nos crimes impróprios, por outro lado, os equipamentos são apenas ferramentas, ou seja, meios para praticar o crime, visto que podem ser cometidos sem o uso deles, não havendo uma definição única para os bens jurídicos protegidos, tendo como exemplos: direito à vida, à liberdade, à honra, entre outros.

Dessa maneira, sem pretensão de exaurir o assunto, exemplos de crimes próprios são: falsificação de cartão, inserção de dados falsos em sistema de informações, interceptação telemática ilegal, invasão de dispositivo informático, modificação ou alteração não autorizada de sistema de informações. Em exemplificação aos crimes cibernéticos impróprios, tem-se: ameaça, crimes contra a honra, estelionato, *fake news*, furto, homicídio, homofobia, pedofilia, pornografia infantil, racismo, violação de direito autoral.

Por fim, nos crimes cibernéticos impróprios, considera-se possível a aplicação da norma penal para essas condutas, eis que a mesma dos crimes comuns, sendo apenas cometidos por *modus operandi* diferente.

2.2.4. Local do Crime, Jurisdição e Competência

O fator inicial para determinar jurisdição e competência, investigar e processar delitos, é a identificação do local do crime, para que então seja possível determinar o órgão responsável pela investigação, e, quando da fase processual conduzir a aplicação da legislação concernente ao fato praticado pelo agente.

No ordenamento jurídico brasileiro, conforme disposição legal do artigo 6° do Código Penal, para determinação do local do crime, adotou-se a teoria da ubiquidade, ou seja, o local do crime será onde ocorreu à ação ou omissão, onde produziu ou deveria produzir o resultado.

Em relação à jurisdição, nada mais é do que o poder que o Estado possui de realizar a aplicação do direito em determinado caso concreto, sendo realizada no Brasil pelo poder judiciário (FILHO, 2012, p.29). Ainda neste raciocínio, é possível descrever jurisdição como sendo:

> [...] A função atribuída a um terceiro imparcial de realizar o Direito de modo imperativo e criativo, reconhecendo/efetivando/protegendo situações jurídicas concretamente deduzidas, em decisão insuscetível de controle externo e com aptidão para tornar-se indiscutível. [...] (DIDIER, 2011. P.89)

No entanto, a jurisdição pode ser, em relação ao próprio objeto de apreciação, penal ou extrapenal, sendo que, em matéria penal ela consiste na realização do *jus puniendi*, ou seja, a aplicação da norma penal ao caso concreto, objetivando a repressão e a prevenção de condutas criminosas.

Ultrapassado o conceito de jurisdição, se faz necessário tratar de competência, pois, apesar do Estado conceder ao Judiciário o poder de dizer o direito, este também tem o dever de limitar esse poder, sendo que o faz por meio da competência, dessa maneira, competência é o limite da jurisdição ao Estado-Juiz. Inclusive, "*num universo de magistrados, a competência é conceituada como a medida ou delimitação da jurisdição*. [...]" (TÁVORA, 2017, p.387).

Sendo assim, competência é a divisão de tarefas que possibilita conferir funcionalidade à jurisdição. Desta maneira, há competência material deve ser estudada sobre três aspectos principais, sendo o primeiro relacionado a matéria *ratione materiae,* onde se busca identificar qual a justiça competente levando em conta a natureza da infração, conforme o inciso III, do art. 69 do CPP.

Bem assim, o segundo aspecto é em razão da pessoa, da função, *ratione personae* ou *ratione funcionae*, onde a pessoa a ser julgada detém o chamado foro de prerrogativa previsto no inciso VII, do art. 69, do CPP, isto é, em razão importância das funções desempenhadas por determinadas pessoas, estas serão julgadas originariamente perante o tribunal, como exemplo cabe ao STF julgar o Presidente da República em simples infrações penais.

Por conseguinte, resta esclarecer acerca do critério em razão do lugar *ratione loc*, previsto nos incisos I e II, do art. 69, do CPP que objetiva identificar o juízo competente tendo como parâmetro o local de consumação do delito, domicílio ou residência do réu.

Desta maneira, o Código de Processo Penal traz no art. 70, que a competência será via de regra determinada pelo local em que se consumar o delito, e em caso de tentativa, onde for praticado o último ato. Todavia, para identificar o juízo competente para julgar determinado feito, é necessário realizar análise dos critérios de competência apontados acima.

Com isso, a competência para processar os delitos cibernéticos, via de regra, é da Justiça Estadual, conforme jurisprudência firmada pelo STF:

> DIREITO PENAL E PROCESSUAL PENAL. AGRAVO INTERNO EM RECURSO EXTRAORDINÁRIO COM AGRAVO. CRIME DE RACISMO PRATICADO PELA INTERNET. COMPETÊNCIA. DISCUSSÃO JÁ DECIDIDA PELO SUPERIOR TRIBUNAL DE JUSTIÇA E SUPREMO TRIBUNAL FEDERAL. JUSTIÇA COMUM. 1. Tal como consta no parecer do Ministério Público Federal, a questão ora em análise competência jurisdicional para o julgamento de feito relativo à prática do crime de racismo via internet ' foi devidamente analisada em momento processual próprio, assentando-se na ocasião tanto no âmbito do STJ (em sede de conflito de competência), quanto no âmbito do

> STF (em sede de habeas corpus), o entendimento jurisprudencial prevalecente, qual seja, o de que o processo e julgamento do feito competia à Justiça Estadual. 2. A jurisprudência desta Corte é no sentido de que a divulgação de mensagens incitadoras da prática de crime pela rede mundial de computadores não é suficiente para, de per si, atribuir à prática do crime a demonstração de resultado além do território nacional (ACO 1.780, Rel. Min. Luiz Fux). Ainda nessa linha, veja-se o RE 1.053.961, Rel. Min. Dias Toffoli. 3. Agravo interno a que se nega provimento.[8]

Deste modo, importante destacar que é pacífico na Jurisprudência o entendimento de que a Justiça Federal é incompetente para julgar crimes em que o Brasil assumiu o compromisso de combater, se não presente a transnacionalidade da conduta, já que inexiste ofensa a bem de interesse ou serviço da União, é inclusive o que se extrai do artigo 109 da CF/88, que traz a competência da Justiça Federal.

Entretanto, exceção a esse entendimento, é no caso relativo à prática de crimes de publicação de imagens, por meio da internet, contendo conteúdos pornográficos envolvendo crianças ou adolescentes, conforme jurisprudência do Supremo Tribunal Federal:

> EMBARGOS DE DECLARAÇÃO NO RECURSO EXTRAORDINÁRIO. MATÉRIA CRIMINAL. OBSCURIDADE SANADA COM A COMPLEMENTAÇÃO DA TESE FIXADA. EMBARGOS ACOLHIDOS. 1. Os embargos de declaração não constituem meio hábil para reforma do julgado, sendo cabíveis somente quando houver no acórdão omissão, contradição ou obscuridade, o que ocorre no presente caso. 2. Reconhecida a obscuridade apontada nos embargos, a tese referente ao Tema 393 da repercussão geral passa a ter a seguinte redação: Compete à Justiça Federal processar e julgar os crimes consistentes em disponibilizar ou adquirir material pornográfico, envolvendo criança ou adolescente, quando praticados por meio da rede mundial de computadores (arts. 241, 241-A e 241-B da Lei nº 8.069/1990). 3. Embargos de declaração acolhidos.[9]

Sendo assim, importante destacar que o Supremo Tribunal Federal no dia 02/10/2020 certificou o trânsito em julgado do Leading Case[10] RE 628624, do respectivo Tema 393, apontando novas linhas protetivas do direito, tornando competente a Justiça Federal para julgar crimes cibernéticos onde se adquira ou divulgue materiais pornográficos, envolvendo criança ou adolescente.

2.2.5. Princípio da Territorialidade e da Extraterritorialidade

O princípio da territorialidade adotado pelo Brasil preconiza que a lei aplicável será a do local do ato praticado, ou seja, independente da nacionalidade do autor do crime ou da

8 STF - AgR ARE: 1169322 DF - DISTRITO FEDERAL 0098316-59.2012.8.07.0001, Relator: Min. ROBERTO BARROSO, Data de Julgamento: 29/03/2019, Primeira Turma, Data de Publicação: DJe-069 05-04-2019.

9 STF - RE: 628624 MG, Relator: EDSON FACHIN, Data de Julgamento: 18/08/2020, Tribunal Pleno, Data de Publicação: 11/09/2020.

10 Leading case é "uma decisão que tenha constituído em regra importante, em torno da qual outras gravitam" que "cria o precedente, com força obrigatória para casos futuros", segundo Guido Fernando Silva Soares em sua obra Common Law: Introdução ao Direito dos EUA (1ª ed., 2ª tir. RT, 1999, p. 40-42).

vítima, aplicar-se-á a lei brasileira, com exceções de alguns casos dispostos expressamente no artigo 5° do Código Penal.

Desta forma, quando no crime cibernético o sujeito ativo está no Brasil, torna-se mais fácil a aplicação deste princípio, já que o fato praticado pelo agente é tipificado como crime. No entanto, há casos em que, no país onde se originou o comando do delito o ato seja típico, porém, no local onde se deu o resultado fático o ato seja atípico.

A internet por ser uma rede mundial de computadores, ou seja, um espaço sem fronteiras físicas, possibilita que um criminoso possa estar, no Japão, por exemplo, e efetuar um ataque cibernético a um internauta no Brasil, sendo que, no atual cenário, dificilmente o criminoso seria punido, pois certamente ele estaria sobre regimento de normas diferentes, bem como, se submeteria a outro poder soberano, não estando sujeito às normas brasileiras.

Entretanto, há algumas situações excepcionais em que a legislação penal brasileira poderá ser aplicada em crimes cometidos em território estrangeiro, por expressa disposição legal do artigo 7° do Código Penal. Todavia, na prática, é de difícil aplicação, haja vista que cada país possuí suas próprias legislações.

Sendo assim, a solução indicada se encontra no Direito Internacional, onde existe a Convenção sobre Crimes Cibernéticos, também conhecida como Convenção de Budapeste, a qual foi celebrada em 2001 e tendo entrado em vigor em 2004, conta hoje com 62 Estados partes e com 10 países observadores. Em dezembro de 2019, o Comitê de Ministros do Conselho da Europa convidou o Brasil a aderir à convenção. Sendo que, eventual adesão proporcionará às autoridades brasileiras acesso mais ágil a provas eletrônicas sob jurisdição estrangeira, além de tornar a cooperação jurídica internacional voltada à perseguição penal dos crimes cibernéticos mais efetiva.

2.2.6. Breves Considerações Acerca do Direito Comparado

Após analisar a legislação brasileira sobre os crimes cibernéticos, a título complementar à presente pesquisa, pertinente uma breve comparação com a legislação dos Estados Unidos, para verificar como este país vem tratando do fenômeno, vez que os crimes cibernéticos romperam os limites territoriais e estão presentes indistintamente em todo o mundo.

Com relação aos Estados Unidos, tem-se que a primeira legislação sobre crimes cibernéticos trata das transferências eletrônicas de fundos e foi criada pelo congresso na

década de 1980, chamada de Electronic Communication Privacy Act (ECPA3[11] - Lei de Privacidade de Comunicação Eletrônica) amplamente utilizada pelo FBI[12] e NSA[13], além de servir como ponto de partida para outros países.

Poucos anos depois, foi aprovada a legislação federal Computer Fraud and Abuse Act[14] (CFAA - Lei de Fraude e Abuso de Computadores), que ainda está em vigor e já passou por diversas revisões devido a rapidez com que os crimes evoluem. Ainda com intuito de coibir esses delitos no ano de 2000, foi criado o (IC36 - Centro de Denúncias de Crimes na Internet).

Tendo em vista que as medidas adotadas não eram suficientes em 2016 foi lançado o Cybersecurity National Action Plan, plano governamental determinando uma maior interação do governo com empresas privadas, visando providenciar ferramentas necessárias para fortalecer a segurança nacional cibernética e proteger a economia do país. Sendo que em 2018 ocorreu a proclamação Presidencial para o mês nacional de conscientização sobre segurança cibernética[15].

Sendo assim, há de se ressaltar que neste país norte-americano, são adotadas penas de multa e prisão bem severas como meio de coibir delitos cibernéticos como no caso emblemático do ativista e respeitado pesquisador de Harvard Aaron Hillel Swartz[16] que poderia pegar até 35 anos em prisão federal e ter de pagar US $ 1 milhão em multas por acusações relacionadas a fraude eletrônica, fraude de computador e obtenção ilegal de informações de um computador protegido, por ter invadido as redes de computador do Instituto de Tecnologia de Massachusetts para obter acesso ao JSTOR e baixar 4,8 milhões de artigos acadêmicos e distribuí-los, terminando de forma trágica com seu suicídio em 2013.

Por fim, tem-se que os Estados Unidos sempre está em busca de meios eficientes para combater os crimes cometidos no ciberespaço, adotando punições severas para quem pratica esse tipo de delito, revisando legislações antigas, criando novas, bem como conscientizando a população sobre segurança cibernética, o que é contrário ao ordenamento jurídico brasileiro, vez que as penas são brandas e há poucas legislações específicas sobre crimes cibernéticos, bem como não há políticas públicas eficientes no sentido de criar uma cultura de uso consciente do meio ambiente cibernético.

---

11 BJA. **Electronic Communications Privacy Act of 1986 (ECPA)**. Disponível em: https://it.ojp.gov/privacyliberty/authorities/statutes/1285. Acesso em: 16. jun. 2016.
12 FBI. **The Cyber Threat**. Disponível em: https://www.fbi.gov/investigate/cyber. Aceso em: 16 jun. 2021.
13 NSA. **What We Do**. Disponível em: https://www.nsa.gov/what-we-do/. Acesso em: 16 jun. 2021.
14 CORNELL. 18 U.S. Code § 1030 - Fraud and related activity in connection with computers. Disponível em: https://www.law.cornell.edu/uscode/text/18/1030. Acesso em: 16 jun. 2021.
15 CIO. **Presidential Proclamation on National Cybersecurity Awareness Month**, 2018. Disponível em: https://www.cio.gov/2018/09/28/cybersecurity-awareness-month.html. Acesso em: 16 jun. 2021.
16 Disponível em: https://www.nytimes.com/2011/07/20/us/20compute.html

2.3. Legislações

2.3.1. Lei 12.737/2012 - Lei Carolina Dieckmann

A lei 12.737/12[17] é conhecida como lei "Carolina Dieckmann" por possuir ligação direta com a atriz que teve suas fotos nuas divulgadas na internet. Essa lei classifica como crime casos similares a este em que ocorre a invasão de aparelhos terminais, conectados ou não à internet.

Foi sancionada em 30 de novembro de 2012 pela então Presidenta da República Dilma Rousseff. Oriunda do projeto de Lei 2793/2011 proposto pelo deputado Paulo Teixeira (PT-SP), sendo uma lei voltada para crimes virtuais e delitos informáticos. Na qual altera o Código Penal acrescentando os artigos 154-A e 154-B, além de incluir tipificação de novos delitos aos artigos 266 e 298 do mesmo diploma.

Sendo assim o artigo 154-A da referida lei, passou a tipificar o delito de "invasão de dispositivo informático", dispondo que comete esse tipo de delito quem:

> Art. 154-A - Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita [...] (BRASIL, 1940).

Observa-se que na redação do artigo, o legislador não especificou quem é a vítima deste delito, deixando margem à interpretação, que a mesma não precisa ser a proprietária do dispositivo invadido, logo, as pessoas e ou empresas que utilizam uma lan house, por exemplo, terão o mesmo amparo legal.

Igualmente, o delito tipificado no art. 154-A da referida lei, traz duas condutas independentes, ou seja, a primeira invadir dispositivo informático "mediante violação indevida de mecanismo de segurança", e a segunda, a invasão de dispositivos para a "instalação de vulnerabilidades", sendo condutas absolutamente independentes, ou seja, não são cumulativas para realização do verbo do tipo.

Percebe-se também, algumas falhas existentes no art. 154-A da referida lei, posto que, se o agente dolosamente invadir um dispositivo informático, visualizar imagens e documentos da vítima, não modificando ou destruindo nenhum dado, o fato será considera atípico, pois não se encaixaria no tipo penal do art. 154-A.

Desta forma, para a realização do núcleo do tipo, ou seja, "invadir dispositivo informático" o agente tem que cometer "mediante violação indevida de mecanismo de

17 BRASIL. Lei no. 12737 de 30 de novembro de 2012. **Tipificação criminal de delitos informáticos**. Diário Oficial da União, Brasília, 30 de novembro de 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 23 mai. 2021.

segurança", isto é, através da "ruptura", do sistema de segurança do dispositivo informático, sendo que, se, por exemplo, no dispositivo não existir "antivírus", ou o mesmo estiver desativado, a conduta do agente não poderá ser enquadrada no tipo penal, ou seja, a conduta será considerada atípica. Nesse sentido,

> [...] as "ações prejudiciais atípicas" são aquelas condutas, praticadas na/através, da rede mundial de computadores, que causam algum transtorno e/ou prejuízo para a vítima, porém não existe uma previsão penal, ou seja: o indivíduo causa algum problema para a vítima, mas não pode ser punido, no âmbito criminal, em razão da inexistência de norma penal com essa finalidade. Por exemplo, o indivíduo que invade o computador de um conhecido sem o objetivo de obter, alterar ou excluir dados ou informações ou sem violar um "mecanismo de segurança" não será indicado nem preso, pois esses fatos não são criminosos, por não se adequarem ao art. 154-A do Código Penal. Por outro lado, o causador do transtorno pode ser responsabilizado na esfera civil, como, por exemplo, ser condenado a pagar indenização em virtude dos danos morais/materiais produzidos (WENDT, E.; JORGE, 2013. p.19).

Conforme o exposto, sendo o fato atípico, nada impede de que a vítima cobre o responsável na esfera cível por eventuais danos morais e materiais sofridos, porém o agente não responderá no âmbito criminal, dada a atual inexistência de legislação que tipifique a conduta praticada.

2.3.2. Lei 12.965/2014 – Marco Civil da Internet

Recentemente, devido às grandes discussões a respeito de elaboração de normas que viessem estabelecer regras mais efetivas sobre o uso da internet no Brasil, foi promulgada a lei 12.965/14, conhecida como marco civil da internet. Esse título foi reservado, pois representa trazer de forma pioneira uma legislação que busca proteger os direitos fundamentais de liberdade de expressão e proteção à intimidade.

Além do mais, esta lei veio regulamentar com base nos princípios gerais do Direito e na própria Constituição Federal de 1988, direitos e deveres dos usuários da internet, bem como, orientações para atuação do Estado.

No entanto, vislumbra-se a necessidade de um estudo mais aprofundado em relação ao aspecto criminal do marco civil da internet, posto que, as complicações investigativas para a apuração de crimes cometidos no âmbito virtual são imensuráveis, uma vez que, os rastros digitais podem ser facilmente alterados ou até mesmo apagados, necessitando portando de máxima cooperação possível das instituições de segurança, bem como, de compartilhamento de informações para lograr êxito na aplicação da legislação.

Assim sendo, a função principal desta lei, é permitir que os órgãos de segurança pública responsáveis por determinada investigação, possa requisitar dados cadastrados junto

aos provedores de serviço de internet, bem como, a imposição destes em armazenar dados de conexão por determinado período de tempo, com finalidade de simplificar o rastreamento do IP (internet protocol) suspeito.

2.3.3 **Da Prova da Materialidade nos Crimes Cibernéticos**

Para discorrer especificamente sobre as provas produzidas quando da prática de crimes cibernéticos, se faz necessária a conceituação do que é prova, bem como onde está disciplinada no ordenamento jurídico brasileiro.

Diante disso, pode-se entender prova como método utilizado em investigação ou processo, para a comprovação da existência e genuinidade de circunstâncias alegadas. Nesse mesmo sentido Fernando Capez, descreve que prova:

> Do latim *probatio*, é o conjunto de atos praticados pelas partes, pelo juiz (CPP, arts. 156, I e II, 209 e 234) e por terceiros (p. ex., peritos), destinados a levar ao magistrado a convicção acerca da existência ou inexistência de um fato, da falsidade ou veracidade de uma afirmação. Trata-se, portanto, de todo e qualquer meio de percepção empregado pelo homem com a finalidade de comprovar a verdade de uma alegação (CAPEZ, 2018. p.364).

Sendo assim, prova é todo meio lícito para demonstrar a existência e a veracidade de um fato, seja na fase de investigação ou no curso do processo. No entanto, divide esse conceito em dois sentidos, objetivo e subjetivo, onde no primeiro refere-se ao meio utilizado para comprovação, ou seja, o objeto de comprovação seja documento, perícia, testemunha. Já no sentido subjetivo, a prova é a convicção que se forma no espírito do juiz quanto à verdade dos fatos (ALVIM, 2018, p. 375)

A produção de prova constitui um direito fundamental consubstanciado na ampla defesa, no contraditório e no devido processo legal, assegurado no art. 5º, XXXV, LIV e LV. Todavia, não tem caráter absoluto, possuindo limites mesmo sendo um direito garantido constitucionalmente.

> Para a consecução de tão gigantesca tarefa, são disponibilizados diversos meios ou métodos de prova, com os quais (e mediante os quais) se espera chegar o mais próximo possível da realidade dos fatos investigados, submetidos, porém, a um limite previamente definido na Constituição Federal: o respeito aos direitos e às garantias individuais, do acusado e de terceiros, protegidos pelo imenso manto da inadmissibilidade das provas obtidas ilicitamente (PACELLI, 2015, p. 175).

Além da inadmissibilidade das provas obtidas por meios ilícitos, previsto no art. 5º, LVI[18], Constituição Federal de 1988, no Código de Processo Penal, também vigoram

18 Art. 5º, LVI da Constituição Federal – "são inadmissíveis, no processo, as provas obtidas por meios ilícitos" (Brasil 1988). Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 16 jun. 2021.

limitações ao princípio da liberdade dos meios de prova, o art. 155, parágrafo único, determina que sejam observadas as restrições da lei civil. Já o art. 158 do mesmo sistema, torna indispensável o exame de corpo de delito para as infrações que deixarem vestígios, não podendo ser suprido pela confissão do acusado; o art. 479, caput, que veda durante o julgamento, a leitura de documento ou a exibição de objeto que não tiver sido juntado aos autos com a antecedência mínima de três dias úteis, dando-se ciência à outra parte.

Deste modo, com o aumento da utilização de computadores e da internet para a prática de crimes, ensejou a necessidade de apuração dos crimes praticados através rede mundial de computadores. Foi assim que surgiu a computação forense[19], cujo objetivo é, por meio reconstituição dos eventos encontrados, determinar se o computador em análise foi utilizado para a realização ou não de condutas ilícitas ou não autorizadas.

As investigações se iniciam com base nas evidências e informações coletadas. Deste modo, nos crimes virtuais, as evidências poderão ser retiradas de qualquer dispositivo eletrônico. Sendo assim, em decorrência da volatilidade dos dados e facilidade com que tais provas podem ser modificadas, perdidas ou até apagadas, as provas eletrônicas deverão passar por perícias técnicas rigorosas para serem aceitas em processos, de forma a garantir a validade e integridade dos resultados.

Pelo fato de se desenvolverem e de se consumarem em ambiente virtual, caracterizado pela inexistência física do sujeito ativo, vez que o criminoso está presente exclusivamente no espaço cibernético, os crimes virtuais geralmente são considerados de significativa complexidade.

No entanto, para colher provas de vestígios deixados nos crimes cibernéticos, as polícias investigativas desenvolveram programas e técnicas forenses, como o EnCase[20], um poderoso software capaz de recuperar dados apagados de dispositivo eletrônico, pois produz uma cópia binária exata da unidade de disco ou da mídia original, depois a verifica gerando valores para os arquivos de imagem relacionados e atribuindo valores aos dados. Essas verificações e balanços revelam quando provas foram falsificadas ou alteradas, mantendo todas as provas digitais legalmente válidas para os processos judiciais, possibilitando que peritos tenham êxito nas buscas de provas contidas nas mídias analisadas.

19 A computação forense é a ciência responsável por elucidar os fatos, através da utilização de métodos científicos na coleta, validação, identificação das evidências digitais, para que se possa punir os infratores. (Ramos, 2017). Disponível em: https://pantheon.ufrj.br/bitstream/11422/6911/1/EDRamos.pdf. Acesso em: 16 jun. 2021.

20 HOLPERIN, M; LEOBON, R. Análise Forense. Disponível em: https://www.gta.ufrj.br/grad/07_1/forense/encase.html. Acesso em: 16 jun. 2021.

No tocante, a vulnerabilidade de modificação característica dos documentos digitais exige a nomeação de perito tecnicamente qualificado para afirmar a autenticidade do documento. Apesar da precisão da computação forense, a coleta de evidências se torna frágil. Quando feita erroneamente, violando disposições de direito material ou princípios constitucionais, pode tornar a prova ilícita ou invalidá-la

Tendo em vista o cuidado exigido por esse tipo de perícia, o maior problema jurídico em relação à produção de provas nos crimes virtuais é o despreparo da polícia investigativa e da perícia. Haja vista a insuficiência de profissionais preparados para esse tipo de investigação, de forma a atender exigências técnicas de coleta e guarda a fim de evitar os questionamentos que venham a surgir sobre a identidade da prova e a licitude de sua obtenção.

No Brasil, existem poucas delegacias de polícia civil especializadas na investigação de crimes cibernéticos, havendo apenas nas capitais de alguns Estados[21]. Já na Polícia Federal o combate aos crimes virtuais é responsabilidade da Unidade de Repressão a crimes cibernéticos (URCC).

Deste modo, para que a sanção penal seja aplicada ao indivíduo que figura como imputado, é necessária a comprovação de que este indivíduo tenha praticado a conduta caracterizada como crime cibernético. Não basta a simples dedução, inferência ou conhecimento superficial sobre a autoria do delito.

Principalmente em relação aos crimes virtuais, a correta identificação do acusado é uma grande preocupação, para que a pretensão punitiva seja justa e direcionada àquele que realmente cometeu o crime cibernético. Essa preocupação é ainda maior, em relação a identificação do autor, quando se considera, por exemplo, a facilidade que os criminosos têm em se apropriar de senhas e códigos de acesso alheios e utilizá-los para aplicar golpes financeiros ou invadir sistemas por meio dessa identidade.

As condutas ilícitas praticadas na internet têm como característica o anonimato on-line, uma vez que o ambiente virtual em que estes crimes são praticados são caracterizados pela ausência de espaço físico. Os criminosos que acessam a rede mundial de computadores se utilizam de técnicas para ocultar sua verdadeira identidade e conduta, podendo, assim, assumir qualquer identidade que não a sua, onde "*o anonimato on-line fornece uma liberdade inatingível no mundo real*" (COLLI, 2010, p.87).

Ao se considerar a possibilidade de identificação do computador, esse anonimato on-line torna-se relativo. A princípio, o anonimato on-line é apenas aparente, porque o mais

21 SAFERNET. Delegacias Cibercrimes. Disponível em: https://new.safernet.org.br/content/delegacias-cibercrimes. Acesso em: 16 jun. 2021.

anônimo dos sujeitos poderá ter o seu computador identificado ao se conectar à rede mundial de computadores, através do endereço IP atribuído ao computador quando da conexão.

A saber, no direito digital, a identificação de um computador é feita por meio do endereço IP, número que é atribuído a cada usuário ou internauta, toda vez que uma conexão for estabelecida com a rede mundial de computadores. Além de permitir a identificação virtual, o IP descreve todo o tráfego de rede e acessos feito pelo usuário em determinado período (PINHEIRO , 2013, p. 308).

Em suma, apesar da aparente facilidade na identificação de um usuário, quando se considera que a localização através do endereço IP permite a identificação de um computador e não, efetivamente, do autor do delito. Dito isto, o óbice decorrente da identificação da autoria está em correlacionar o computador e o sujeito que o opera em determinado espaço de tempo.

Por fim, a instauração de uma investigação baseada somente na mera presunção de suspeição decorrente da titularidade de um contrato de acesso à internet, por exemplo, estaria orientada pela responsabilização objetiva do direito penal, que deve ser repudiada a todo o custo (COLLI, 2010, p.87).

3 CONSIDERAÇÕES FINAIS

Com isso em relação ao princípio da territorialidade e da extraterritorialidade o Brasil preconiza que a lei aplicável será a do local do ato praticado. Entretanto, há algumas situações em que a legislação penal brasileira poderá ser aplicada em crimes cometidos em outros países, todavia, na prática, é de difícil aplicação, haja vista que cada país possuí suas próprias legislações. Com isso, seria importante que o Brasil aderisse à Convenção de Budapeste pois proporcionará às autoridades brasileiras acesso mais ágil a provas eletrônicas sob jurisdição estrangeira, além de tornar a cooperação jurídica internacional voltada à perseguição penal dos crimes cibernéticos mais efetiva.

Quanto às legislações pertinentes sobre o tema, possuem as Leis 12.965/14 conhecida com o marco civil da internet e a Lei 12737/12 conhecida como Lei Carolina Dieckmann, sendo que está última possuí falha pois se o agente dolosamente invadir dispositivo informático sem que haja violação de mecanismo de segurança, visualize imagens e documentos da vítima, mas não modificar ou destruir nenhum dado, não se encaixa no art. 154-A, será considerado fato atípico, pois não preenche os núcleos do tipo.

Ao final da pesquisa verificou-se que há dificuldades quanto a apuração e repressão da autoria delitiva referente aos crimes cibernéticos. Quando se inicia investigações com base em informações e evidências por meio de qualquer dispositivo eletrônico, o que dificulta é a

volatilidade dos dados e a facilidade com que tais provas podem ser modificadas, perdidas ou até apagadas. Além disso, pela inexistência física do sujeito ativo, a apuração de autoria nos crimes cibernéticos é considerada de extrema complexidade, pois mesmo identificando o dispositivo informático utilizado no crime por meio do IP, não efetivamente identificará o autor do delito.

Outro ponto a ser observado é que mesmo com a precisão da computação forense, a coleta de evidências se torna frágil, pois quando feita violando disposições de direito material ou princípios constitucionais, pode-se tornar a prova ilícita ou invalidá-la. Com isso, o despreparo da polícia investigativa e da perícia, somado à existência de poucas delegacias especializadas acaba dificultando ainda mais a apuração da autoria.

Com isso, dentre as possíveis soluções para a problemática, tem se que a criação de políticas públicas eficientes, de Delegacias especializadas em apurar delitos cibernéticos em todos os Estados do país, aderir à convenção de Budapest, além de instituir legislações específicas, objetivando abranger os mais diversos delitos praticados. Para que assim seja possível através de medidas preventivas e repressivas diminuir o número de crimes cibernéticos cometidos no país.

REFERÊNCIAS BIBLIOGRÁFICAS

ALVIM, J. E. **Carreira. Teoria geral do processo**. 21. ed. rev. e atual. – Rio de Janeiro: Forense, 2018, p. 375

ASSUNÇÃO, M. F. A**. O Guia do Hacker Brasileiro.** Editora: Visual books, 1 de janeiro de 2002, p. 82.

BOTTINI, Pierpaolo Cruz, 2007, p. 36, apud BARBOSA, Karlos Alves. **Sociedades de risco e os crimes de perigo abstrato**. Disponível em: https://repositorio.ufu.br/bitstream/123456789/13216/1/SociedadeRiscoCrimes.pdf. Acesso em: 20 jun. 2021.

BRASIL ESCOLA. Internet. Disponível em: https://brasilescola.uol.com.br/informatica/internet.htm. Acesso em 20 de junho de 2021.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Brasília, DF: Presidência da República, 2016. 496 p. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 30 ago. 2020.

BRASIL. Decreto-Lei 2.848, de 07 de dezembro de 1940. **Código Penal**. Diário Oficial da União, Rio de Janeiro, 31 dez.

BRASIL. Lei no. 12737 de 30 de novembro de 2012. **Tipificação criminal de delitos informáticos**. Diário Oficial da União, Brasília, 30 de novembro de 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 23 mai. 2021.

BRASIL. Lei no. 6938 de 31 de agosto de 1981. **Política Nacional de Meio Ambiente**. Diário Oficial da União, Brasília, 31 de agosto de 1981. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l6938.htm. Acesso em: 23 mai. 2021.

CAPEZ, Fernando. **Curso de processo penal**. 25. ed. – São Paulo: Saraiva Educação, 2018, p. 364.

CASTRO, Aldemario Araújo. **A internet e os tipos penais que reclamam ação criminosa em público**. p.1. Disponível em: http://egov.ufsc.br/portal/sites/default/files/anexos/13308-13309-1-PB.pdf. Acesso em 02 de novembro de 2020.

COLLI, Maciel. Cibercrimes: **limites e perspectivas à investigação policial de crimes cibernéticos**. Curitiba: Juruá, 2010, p. 87.

COUTINHO, Ricardo Silva. **O meio ambiente digital e a tutela dos bens culturais**. Revista Brasileira de Meio Ambiente Digital e Sociedade da Informação, São Paulo, v. 1, n. 1, 2014, p. 226.

DA SILVA, Patrícia Santos. **Direito e crime cibernético**: análise da competência em razão do lugar no julgamento de ações penais. Brasília: Vestnik, 2015, p. 20.

DIDIER JR., Fredie. **Curso de Direito Processual Civil**. 13ª Ed. Salvador: Editora Jus Podivim, 2011, p. 89.

FILHO, Greco V. **Manual de Processo Penal**. 9. Ed. São Paulo: Editora Saraiva, 2012, p. 29.

FIORILLO, Celso Antonio Pacheco. **Curso de Direito Ambiental Brasileiro**. 14ª ed. Saraiva. 2013, p. 494.

https://www.ipea.gov.br/portal/index.php?option=com_content&view=article&id=29413:-obrasil-precisa-investir-em-politicas-de-prevencao-acriminalidade&catid=28:diest&directory=1. Acesso em: 30 ago. 2020

LOSANO, Mario Giuseppe. **A informática jurídica vinte anos depois**. Revista dos Tribunais, Rio de Janeiro, ano 84, v. 715, maio/1995. p. 365.

MASSON, Cleber Rogério. **Direito Penal**: parte geral. 13. Ed. Rio de Janeiro: Forense; São Paulo: Método, 2019 p. 322.

NETO, E. D. **Sociedade de Risco, Direito Penal e Política Criminal**. Ensaio: Revista de Direito Público, Londrina, v. 5, n. 2, 2010.

ORRIGO, G. M. A.; FILGUEIRA, M. H. B. **Crimes cibernéticos**: uma abordagem jurídica sobre os crimes realizados no âmbito virtual. 2015. Disponível em: https://jus.com.br/artigos/43581/crimes-ciberneticos-uma-abordagem-juridica-sobre-oscrimes-realizados-no-ambito-virtual. Acesso em: 01 nov. 2020

PACELLI, E. **Curso de processo penal**. 21. ed. rev., atual. e ampl. – São Paulo: Atlas, 2017, p. 175.

PINHEIRO, Patrícia Peck. **Direito Digital**. São Paulo: Editora Saraiva, 2013, p. 308.

SILVA. F. D. S. **O Brasil precisa investir em políticas de prevenção à criminalidade**. Ipea, 2017. Disponível em: https://www.ipea.gov.br/portal/index.php?option=com_content&view=article&id=29413&Itemid=6. Acesso em: 03 out. 2021

SILVA, José Afonso da. **Direito ambiental constitucional.** 5. ed. São Paulo: Malheiros, 2004.

TÁVORA. N; ALENCAR. R. R. Curso de direito processual penal. 12. ed. rev., e atual. Salvador: Ed. JusPodivm. 2017, p. 387.

VENOSA, Sílvio de Salvo. **Direito civil**: direitos reais. 3. ed. São Paulo: Atlas, 2003, v. 5. p. 593.

VIANNA, Túlio; MACHADO, Felipe. **Crimes informáticos**. Belo Horizonte: Fórum, 2013, p.21.

WENDT, E.; JORGE, H. V. N. **Ameaças e Procedimentos de Investigação**. 2ª ed. Rio de Janeiro: Editora Brasport, 2013, p. 5