UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO DE CIÊNCIAS JURÍDICAS
DEPARTAMENTO DE DIREITO

Matheus Faraco de Medeiros da Silva

A PROTEÇÃO DOS DADOS PESSOAIS CONTRA CIBERCRIMES FRENTE AO PROJETO DE LEI Nº 879 DE 2022

Florianópolis
2023

Matheus Faraco de Medeiros da Silva

A PROTEÇÃO DOS DADOS PESSOAIS CONTRA CIBERCRIMES FRENTE AO PROJETO DE LEI Nº 879 DE 2022

Trabalho de Conclusão de Curso submetido ao curso de Direito do Centro de Ciências Jurídicas da Universidade Federal de Santa Catarina como requisito parcial para a obtenção do título de Bacharel em Direito.

Orientadora: Profa. Dra. Chiavelli Facenda Falavigno

Florianópolis

2023

da Silva, Matheus Faraco de Medeiros
A PROTEÇÃO DOS DADOS PESSOAIS CONTRA CIBERCRIMES FRENTE AO PROJETO DE LEI Nº 879 DE 2022 / Matheus Faraco de Medeiros da Silva ; orientadora, Profa. Dra. Chiavelli Facenda Falavigno, 2023.
83 p.

Trabalho de Conclusão de Curso (graduação) - Universidade Federal de Santa Catarina, Centro de Ciências Jurídicas, Graduação em Direito, Florianópolis, 2023.

Inclui referências.

1. Direito. 2. Dados Pessoais. 3. Cibercrime. 4. Direito Penal Informático. 5. Privacidade. I. Falavigno, Profa. Dra. Chiavelli Facenda. II. Universidade Federal de Santa Catarina. Graduação em Direito. III. Título.

AGRADECIMENTOS

A fé de Jota. O amor de Vera. O suporte de Gláucia. O inconformismo de Marcello. A perseverança de Rodrigo. A genialidade de Lia. O cuidado de Athos. O carinho de Isadora. O companheirismo de João Gabriel. A confiança de Pedro. A honestidade de Julia. A dedicação de Artur. A amizade de Italo. A companhia dos largados. A solicitude de Ana Carolina. A orientação de Chiavelli. A loucura dos empresários juniores de Santa Catarina. A prestatividade dos Escoteiros do Brasil.

Todas essas pessoas, e seus respectivos atributos, foram base, impulso e afago ao longo da graduação. Foram responsáveis por me ensinar a ter coragem de sonhar, e ousadia de agir.

A todos estes, dedico esse trabalho como forma de agradecimento e gratidão.

RESUMO

O avanço da tecnologia, que agregou benefícios para a sociedade, também é a causa de novos riscos e perigos para. Nessa linha, os dados pessoais possuem alta valorização no mercado e estão frequentemente envolvidos em atividades prejudicais à privacidade individual. Buscando minimizar os efeitos nocivos, o Estado recorre ao Direito Penal, com a ideia de promover uma maior tutela sobre a matéria. Com isso em mente, a presente monografia tem como direcionamento compreender as implicações práticas do PL 9879/2022, analisando as consequências penais na proteção dos dados pessoais contra cibercrimes. Para isso, utilizou-se de pesquisas qualitativas e descritivas, explorando levantamentos bibliográficos mediante revisões de literaturas e legislações disponíveis. Quanto ao método, aplicou-se o dedutivo, partindo de uma premissa geral e maior que é a privacidade e a proteção de dados pessoais, para uma análise mais centralizada na aplicação do projeto de lei. O trabalho contempla inicialmente sobre a evolução da ideia de privacidade, e as normas nacionais e internacionais relacionadas à internet e dados pessoais. Posteriormente, analisa as transformações no Direito Penal, especialmente o Direito Penal Informático, em relação aos seus conceitos e tipificações. Por fim, apresenta o histórico legislativo e a construção do PL 879/2022, apontando desafios e possíveis adaptações para a melhor tutela dos dados pessoais.

Palavras-chave: Dados pessoais; Cibercrime; Direito Penal Informático

ABSTRACT

The advancement of technology, which has brought benefits to society, is also the cause of new risks and dangers. In this regard, personal data holds high value in the market and is frequently involved in activities harmful to individual privacy. To minimize the detrimental effects, the State resorts to Criminal Law, with the aim of providing greater protection in this matter. The present dissertation aims to comprehend the practical implications of PL 9879/2022, analyzing the criminal consequences in the protection of personal data against cybercrimes. To achieve this, qualitative and descriptive research was conducted, exploring bibliographic surveys through reviews of available literature and legislation. As for the methodology, a deductive approach was employed, starting from the broader premise of privacy and the protection of personal data, leading to a more focused analysis of the application of the bill. The study initially encompasses the evolution of the concept of privacy and the national and international regulations related to the internet and personal data. Subsequently, it examines the transformations in Criminal Law, particularly in the field of Cybercrime Law, regarding its concepts and typification. Finally, it presents the legislative history and the development of PL 879/2022, highlighting challenges and potential adaptations for the better safeguarding of personal data.

Keywords: Personal data; Cybercrime; Cybercrime Law

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados
CP	Código Penal
ECA	Estatuto da Criança e do Adolescente
EC	Emenda Constitucional
GDPR	*General Data Protection Regulation*
LGPD	Lei Geral de Proteção de Dados Pessoais
MCI	Marco Civil da Internet
MP	Ministério Público
PL	Projeto de Lei
TJ	Tribunal de Justiça

SUMÁRIO

1 INTRODUÇÃO

Se, por um lado restam poucas dúvidas quanto à dependência e envolvimento da sociedade com a internet e dispositivos eletrônicos, ainda existem lacunas no que tange a regulamentação desse comportamento e a proteção dos bens e das pessoas envolvidas. Muito se fala da “Era dos dados” e da “Sociedade em rede”, mas como o direito pode ser mais efetivo na tutela dessa realidade? (SOUZA, 2021)

O conceito de privacidade, que se iniciou remetendo a uma ideia de ser deixado só, foi modificando-se ao longo do tempo refletindo o comportamento e os interesses da sociedade em cada época. Pela sua função social, o direito foi simultaneamente adaptando-se para atender às mudanças e regulamentar as novas situações, almejando a promoção da paz, da ordem e da justiça, além de fornecer soluções para conflitos entre indivíduos ou grupos. (NADER, 2014)

Na prática, o indivíduo que outrora estabelecia suas relações no formato *offline*, com aspecto material e baixo dinamismo, migrou para o mundo *online* com conexões e ferramentas virtuais, e um alto fluxo de bens imateriais. Por sua vez, o direito buscou, e ainda busca, regulamentar essa nova realidade com a criação de leis e ajustes constitucionais. (CALLEGARI; ANDRADE, 2020)

Neste contexto, nota-se uma “releitura” da ideia de sociedade do risco, do sociólogo alemão Ulrich Beck, pois o mesmo progresso de modernização que impacta positivamente no desenvolvimento tecnológico e científico, cria também ameaças e outras consequências nocivas ao indivíduo em uma espécie de efeito colateral. (CALLEGARI; ANDRADE, 2020) Dentro de todas essas inovações tecnológicas há também novas ações danosas, chamadas de cibercrime, que se caracterizam por atos que lesionam bens jurídicos, violam a privacidade e ferem a proteção de dados pessoais em ambiente virtual.

Estudos, notícias e pesquisas internacionais colocam o Brasil como um dos países que mais sofre pela falta de cibersegurança no mundo, alertando para a responsabilidade do Estado na proteção e na investigação de tais delitos. Entretanto, o Estado não vem apresentando êxito na prevenção conscientizadora e acaba recorrendo ao Direito Penal de forma frequente e extensiva. (BARBOSA, 2022)

Seguindo a Convenção de Budapeste, principal norma penal internacional sobre cibercrime, o Brasil busca uma tutela mais efetiva da privacidade por meio de Leis como a Lei 12.737 de 2012 e a Lei 14.155 de 2021 além de projetos como o PL 879 de 2022. Em relação aos dados pessoais, as normativas ainda são iniciais e abstratas, divergindo assim da grande valoração e importância que esse tipo de dado possui nos dias de hoje.

Partindo desta explanação, o presente trabalho busca analisar como o Direito se comporta, sobretudo o Direito Penal, em relação ao seguinte problema: O Projeto de Lei 879/2022 garante a tutela penal dos dados pessoais contra cibercrimes? Com base neste questionamento, a presente monografia pauta-se na análise das consequências penais na proteção dos dados pessoais contra cibercrimes com a aplicação prática do referido projeto.

Para isso, utilizou-se de pesquisas exploratórias descritivas, recorrendo a levantamentos bibliográficos por meio de revisões de literaturas e legislações disponíveis. Quanto à metodologia, aplica-se o método dedutivo, visto que se inicia por premissas maiores e gerais, a privacidade e a proteção de dados pessoais, para chegar em uma análise mais específica da aplicação do projeto de lei mencionado.

De forma segmentada, o primeiro capítulo se propõe a apresentar um panorama sobre a temática de privacidade, abordando a conceituação do tema ao longo da história, além de discorrer sobre normas nacionais e internacionais relevantes, e suas implicações na proteção de dados pessoais. Em termos práticos, analisa-se a modificação da ideia de privacidade, a regulamentação da internet e as normativas sobre dados pessoais no mundo e no Brasil.

O capítulo 2, por sua vez, é voltado para as adaptações no Direito Penal em relação as mudanças da sociedade e sua função social de regulamentar as novas situações. Para isso, os objetivos específicos deste capítulo são: explicar o que é Direito Penal informático, bem jurídico informático e cibercrime, discorrer sobre os novos riscos e ameaças aos indivíduos no mundo virtual, além de apresentar dados já coletados e casos sobre o cibercrime no território brasileiro.

Por fim, o último capítulo trata de uma análise direcionada ao PL 879/2022, apresentando inicialmente o histórico legislativo já percorrido, para que depois se possa analisar o projeto em questão, apontando desafios e possíveis adaptações. Nesta finalização, propõe-se a observar sobre a utilização do Direito Penal, bem como explorar as particularidades dos crimes em espécie mencionados no PL,

procurando, a partir dessas apurações, verificar se a hipótese que motivou este trabalho é confirmada ou não.

2 A PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

Para analisar a tutela penal dos dados pessoais com eficiência é necessário observar como a defesa da privacidade e a proteção de dados pessoais são historicamente tratadas no Brasil e no direito de outras nações. Com esse objetivo, o capítulo será direcionado para a construção da temática da privacidade no mundo, expondo também a influência de ordenamentos estrangeiros na construção brasileira, além de normas nacionais e suas implicações na proteção de dados pessoais no Brasil.

Parte-se de um aspecto geral e mais amplo da privacidade mundial, com destino a uma análise mais direcionada aos dados pessoais na abrangência nacional.

2.1 HISTÓRICO LEGISLATIVO E A PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO FUNDAMENTAL

Os primeiros estudos publicados sobre o tema da privacidade costumam ser relacionados a Warren e Brandeis, em virtude do artigo "*The Right to Privacy*", publicado no final do século XIX. Samuel Warren era um jurista americano, e na época, a divulgação não autorizada de fatos íntimos sobre o casamento de sua filha ilustrou a necessidade de privacidade da burguesia americana, que buscava um "direito de ser deixado em paz", o *"the right to be let alone*". (WARREN; BRANDEIS, 1890)

No início, refletindo a vontade burguesa de afastamento, construiu-se um paradigma de relação zero, excluindo a comunicação e a troca de informações entre os sujeitos. Neste contexto do capitalismo americano, a pirâmide social não era apenas uma questão teórica, de aspecto monetário ou classista, pois além da segregação espacial e financeira, havia também um desejo de impedir o fluxo de informações, criando "bolhas sociais". (DONEDA, 2019)

Posteriormente, em termos de norma internacional, a Declaração dos Direitos Humanos inaugurou em 1948 relevante dispositivo sobre a privacidade com o seu artigo 12: “Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques.” (“Declaração Universal dos Direitos Humanos”, 1948) Nota-se que o foco seguia direcionado para a privação, no sentido de conservar informações apenas e unicamente com os envolvidos direto, sem qualquer espécie de compartilhamento.(“Declaração Universal dos Direitos Humanos”, 1948)

Com o tempo, os movimentos sociais, fluxos de informações, avanços tecnológicos e outras mudanças sociais agitaram o direito à privacidade. Por sua vez, a privacidade expandiu suas fronteiras, alcançou novos sujeitos, criou realidades e tornou-se presente em situações inéditas até então. Simultaneamente, as informações coletivas passaram a ser valorizadas no mercado mundial, tanto para entes públicos como para empresas privadas que buscavam coletar e analisar o comportamento dos indivíduos para gerar preciosos bancos de dados.(CANCELIER, 2017)

No documentário “O Dilema das Redes” pode-se constatar que o próprio indivíduo é impactado por essa busca por dados, pois ao mesmo tempo em que se torna "refém" do sistema e fornece informações para poder usufruir de bens e serviços, também busca referências e informações de outras pessoas. As últimas décadas do século XXI foram marcadas por grandes lançamentos de redes sociais, como Orkut, Facebook, Twitter, Instagram, LinkedIn e, mais recentemente, o TikTok, que virtualmente quebram as fronteiras entre comunidades e conectam pessoas de diferentes realidades de forma cada vez mais instantânea e monetizada. Isso por sua vez abre espaço não só para ambições empresariais, mas também para o mundo do crime que começa a considerar o ambiente virtual como algo promissor.(ORLOWSKI, 2020)

Observa-se uma evolução no conceito de privacidade, afastando-se da ideia de ser deixado sozinho, sem o envolvimento de terceiros em suas informações, para uma ideia de direito de controle, em que cada pessoa deseja ter o poder de controlar para onde, como e para quem suas informações serão direcionadas. Neste movimento, a disciplina da privacidade passou a ser estruturada especialmente em torno dos dados pessoais, dando origem a uma nova ramificação de estudos: a

proteção de dados pessoais. Essa por sua vez reúne princípios e fundamentos muito similares aos da própria proteção da privacidade: a tutela da personalidade e da dignidade do indivíduo, mas agora em um ambiente caracterizado pela rede, tanto no sentido de conexão pessoal, mas também no sentido de informatização[1]. (CANCELIER, 2017; RODOTÀ, 2008)

Neste panorama, começaram a surgir normativas específicas sobre o tema da proteção de dados, destacando-se a Lei Geral de Proteção de Dados do Estado alemão de Hesse, de 1970, que é tratada por muitos como um marco legislativo pioneiro na apresentação da proteção de dados como um modelo normativo autônomo. O exemplo germânico serviu de base para diversos documentos locais no continente europeu, que posteriormente culminaram na Diretiva 95/46/CE da União Europeia, lançada em 1995 com o objetivo de definir e unificar princípios fundamentais na proteção de dados pessoais no velho continente.(CONSELHO DA UNIÃO EUROPEIA, 1995)

A Diretiva foi substituída em 2016 pelo Regulamento UE nº 2016/679, apelidado de *General Data Protection Regulation* (GDPR), que trouxe referências mais direcionadas e específicas para a proteção de dados pessoais, considerando sobretudo o avanço tecnológico vivenciado durante os mais de 20 anos de intervalo entre os dois documentos. Tendo em vista a relevância europeia nos debates jurídicos e na movimentação do mercado mundial, o texto do GDPR se tornou premissa para a construção de muitos textos legais sobre o assunto, incluindo a Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709 de 2018), que será assunto muito abordado neste trabalho.(UNIÃO EUROPÉIA, 2016)

Também no século XXI, a Carta dos Direitos Fundamentais da União Europeia apresentou, em 2000, o respeito pela vida privada e a proteção de dados pessoais de forma separada, em artigos diferentes, ainda que complementares. A Carta prevê inclusive que, em relação aos dados pessoais, deve existir uma autoridade[2] independente para a fiscalização de regras sobre o tema, apontando assim para a especificidade da matéria. (UNIÃO EUROPÉIA, 2000)

---

[1] De acordo com o Dicionário Houaiss da Língua Portuguesa, “informatização” é um substantivo feminino que se refere ao processo de introdução e utilização de tecnologias da informação e comunicação em um determinado contexto, como empresas ou organizações governamentais. (HOUAISS, 2009)

[2] “O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente”(UNIÃO EUROPÉIA, 2000)

Na realidade brasileira, a Constituição Federal de 1988 retoma a ideia de vida privada, adicionado no artigo 5º, dos direitos e garantias fundamentais, o inciso X com a seguinte redação: “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”. (BRASIL, 1988) Verifica-se assim um viés individualista e restritivo criando uma lógica onde toda informação se torna um segredo. O que é meu, é meu, e ninguém pode ter acesso.

Nessa tendência mais pessoal, surge a PEC Nº 17/2019, que na época buscava aumentar a relevância dos dados pessoais, inclusive nos meios digitais, com a seguinte justificativa:

> [...] De fato, a privacidade tem sido o ponto de partida de discussões e regulações dessa natureza, mas já se vislumbra, dadas as peculiaridades, uma autonomia valorativa em torno da proteção de dados pessoais, de maneira, inclusive, a merecer tornar-se um direito constitucionalmente assegurado.

A ideia inicial era alterar o inciso XII[3] do Art 5º, que comparado ao inciso X[4] do mesmo item é um texto mais recente e, por isso, mais próximo da realidade social. Além do caráter temporal, pode-se analisar que o inciso X apresenta um perfil mais abstrato, listando a intimidade e a honra, ao passo que o XII elenca direitos mais concretos como a correspondência e os dados de uma forma genérica.(OLIVEIRA, 2022)

Além do dispositivo na Magna Carta de 1988, outras legislações estaduais e nacionais trataram do direito pessoal frente a seus dados. São exemplos: a Lei estadual do Rio de Janeiro nº 824 de 28 de dezembro de 1984, relacionada ao acesso de informações em bancos de dados, e a Lei Estadual de São Paulo nº 5.702, de 5 de junho de 1987, que previa não só o acesso, mas a retificação dos dados. Ambas não estão mais em vigor pois foram substituídas pela LGPD de abrangência federal.(OLIVEIRA, 2022)

No âmbito nacional, o Código de Defesa do Consumidor (CDC - Lei Nº 8.078 de 1990) possui uma seção específica para tratar sobre os bancos de dados, e dispõe sobre outras garantias para os indivíduos sobre suas informações. Ainda que por lógica tenha restringido seu alcance para as relações de consumo, seus

---

[3] “XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;”(BRASIL, 1988)

[4] X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;(BRASIL, 1988)

direcionamentos podem ser muito bem aplicados em outros cenários. Por sua vez, a Lei de acesso à informação, Lei nº 12.527/2011, retoma pontos sobre o acesso e a qualidade das informações, além de categorizá-las de acordo com seu sigilo. O documento também traz à tona o mecanismo do consentimento como forma de fortalecer a vontade do indivíduo no que se refere ao compartilhamento e uso das informações pessoais. (OLIVEIRA, 2022)

Todos esses movimentos convergiram para a promulgação da Emenda Constitucional nº 115/2022 que elevou a Proteção de Dados Pessoais ao grupo de direitos e garantias fundamentais. A medida constitucional fixou a competência privativa da União para legislar sobre o tema, bem como para organizar e fiscalizar a proteção e o tratamento de dados pessoais, demonstrando total alinhamento à ideia de que os dados circulam pelo território de forma livre e constante. Tal definição de competência também impacta diretamente na Autoridade Nacional de Proteção de Dados (ANPD), uma vez que proporciona valores e poderes maiores para sua atuação.(Proposta de Emenda à Constituição Nº 17, de 2019, 2019)

Embora o resultado tenha sido uma alteração constitucional, cabe abordar que a decisão não foi algo unânime no meio jurídico, pois na visão de alguns, a proteção de dados já estaria incluída na Constituição Federal. Anderson Schreiber é um dos que diverge da decisão do Congresso Nacional argumentando que a proteção de dados já poderia ser encontrada de forma explícita tanto no (Art 5º, X) como também na cláusula geral da dignidade da pessoa humana (Art 1º, III). Schreiber considera que “Quando um jurista admite uma alteração inútil, mas simbolicamente bem-vinda, do texto constitucional, perde o critério que deveria seguir em relação a outras alterações, que deverá tolerar quando bem-vindas aos olhos de outro.”.(SCHREIBER, 2019)

De modo geral, percebe-se que as leis brasileiras foram construídas com base nas referências de outras nações, e ainda que o texto constitucional aborde a privacidade, é algo ainda abstrato, com o objetivo final de proteção, mas sem um direcionamento concreto para as questões práticas de "como proteger". No mais, embora outras normas como o CDC e a Lei de Acesso à Informação sejam mais detalhistas e concretas, apresentam contextos muito específicos para a relação consumerista e para o acesso dos cidadãos às informações públicas.

Nessa linha, para minimizar tal lacuna, parte-se para a análise do Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014) e da LGPD, apresentando

como tais diretrizes protegem os dados pessoais de forma mais prática e direcionada.

2.2 O MARCO CIVIL DA INTERNET

Discutido desde a década de 1995, o MCI foi contemporâneo ao início da comercialização da rede de internet no Brasil, sendo sancionado apenas em 2014. Desde então percebe-se mudanças significativas no uso da internet e na forma como a legislação lida com o ambiente digital.(SIQUEIRA, 2023)

Sem uma normativa na linha do MCI, o ambiente virtual era uma “terra sem lei”, um local pouco regulamentado, no qual a regra do mercado sempre podia prevalecer em favor dos interesses das grandes empresas, em detrimento dos usuários. Da mesma forma, governos de países como os Estados Unidos da América utilizavam do meio informático em suas políticas e estratégias internacionais de forma não regularizada.(SIQUEIRA, 2023)

A construção do texto foi realizada com a participação de diversos autores, destacando-se o Ministério da Justiça, o Centro de Tecnologia e Sociedade da Escola de Direito da FGV-RJ, o Comitê Gestor da Internet (CGI)[5], além de consultas públicas que permitiram a participação civil. O trabalho coletivo resultou na apresentação de um projeto de lei ao Congresso Nacional, registrado sob o nº 2.126/2011, convertido em lei três anos depois.(SANTOS, 2021)

Neste período as descobertas sobre as políticas de vigilância dos Estados Unidos por meio da Agência de Segurança Nacional Americana (NSA), aceleraram os trabalhos sobre o texto. A confirmação de que o Brasil era um dos países monitorados mobilizou até a então presidente Dilma Rousseff, que participou de alguns debates e buscou agilizar a finalização da redação.(BBC NEWS BRASIL, 2014)

Como visualizado em outras normas, na lista de princípios do MCI a privacidade e a proteção de dados pessoais são apresentas de forma separada[6], seguindo a linha da Carta dos Direitos Fundamentais da União Europeia de

[5] Composto por representantes do setor governamental, do setor empresarial, do terceiro setor e da comunidade acadêmica, o CGI.br constitui um modelo de governança na internet pioneiro, com base nos princípios de multissetorialidade, multilaterialidade, transparência e democracia.

[6] Respectivamente inciso II e III do Art 3º. II - proteção da privacidade; III - proteção dos dados pessoais, na forma da lei;

considerar a existência de duas matérias de direito distintas, ainda que complementares. Com isso, percebe-se que o direcionamento aplicado por outras legislações, voltado ao comportamento social “offline”, reflete-se também em uma lei mais relacionada ao mundo virtual, alterando apenas o cenário fático da regulamentação para um ambiente cibernético[7].

Apesar disso, o rol de princípios foi criticado por alguns operadores do direito que consideram a presença de fundamentos redundantes, dispensáveis, e não inovadores no MCI. As críticas pautavam-se na comparação com os princípios já expostos na Constituição Federal, que abordam os mesmos ideais expostos no MCI, como pode ser visto no quadro 1.

Texto da Constituição Federal	Texto do Marco Civil da Internet
Art.5º, X: “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”	Art.7°, I, dispõe que é direito dos usuários da internet a: “inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano moral e material decorrente de sua violação”
Art 5º, XII: “é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal”	Art.7°, II e III: “II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;”

Quadro 1: Comparação entre a Constituição Federal e Marco Civil da Internet (TOMASEVICIUS FILHO, 2016)

Para essa corrente doutrinária, a existência de uma norma jurídica repetitiva prejudica a aplicação do direito visto que redações similares tendem a aumentar as possibilidades de interpretação e dificultam o direcionamento legal. Mesmo que tenha sido trabalhado por anos, e contado com a contribuição de diversos personagens, TOMASEVICIUS FILHO (2016) considera que no texto do MCI há um desalinhamento à finalidade do ordenamento jurídico no sentido de inovar, uma vez que a normativa deveria surgir “acrescentando normas necessárias à regulação dos

[7] O termo cibernético visa à relação, ou um controle de processos, entre seres vivos e máquinas. (Manual descomplicado de direito digital). Ambiente cibernético é um termo utilizado para descrever o espaço virtual em que ocorrem as atividades relacionadas à tecnologia da informação e comunicação.

comportamentos, eliminando aquelas que não mais atendem às necessidades sociais".(TOMASEVICIUS FILHO, 2016, p. 279)

Apesar das inúmeras críticas, com o advento do MCI o Brasil passou a ter uma norma direcionada ao mundo digital, inserindo o Estado com maior destaque nesse meio, indicando de forma expressa: obrigações, direitos, agentes, termos técnicos e procedimentos relacionados.(FAVORITO, 2014) A partir do MCI, a presença do Estado possibilitou ao poder público a competência de atuação no ambiente virtual, garantindo e ordenando o acesso e a utilização da internet. (SIQUEIRA, 2023) Cabe, porém, frisar, que o legislador acabou sendo penalmente omisso na construção do texto, deixando de fora sansões e direcionamentos penais.

Por outro lado, a participação mais ativa do governo nesse ambiente despertou algumas insatisfações, sobretudo no que diz respeito a liberdade de expressão e a autonomia das empresas privadas. Atualmente, projetos de lei estão em tramitação na Câmara justamente para abordar esses temas, como se percebe com o PL 2393/2021[8] o PL 2401/2021[9], sendo que ambos se encontram vinculados ao PL 2630/2020[10].

Em suas justificativas, o primeiro sustenta que seu objetivo é o de proteger a liberdade de expressão dos usuários de redes sociais, enquanto o segundo almeja coibir o controle arbitrário dos provedores de internet quanto a retirada e moderação dos conteúdos publicados. Esse tipo de debate costuma se relacionar com situações de *fake news*[11], eleições e investigações criminais, além de comumente envolver os provedores de internet[12] e a matéria de responsabilidade civil, como podemos visualizar na jurisprudência pátria:

> RECURSO ESPECIAL. OBRIGAÇÃO DE FAZER E REPARAÇÃO CIVIL. DANOS MORAIS E MATERIAIS. PROVEDOR DE SERVIÇOS DE INTERNET. REDE SOCIAL "ORKUT". RESPONSABILIDADE SUBJETIVA. CONTROLE EDITORIAL. INEXISTÊNCIA. APRECIAÇÃO E NOTIFICAÇÃO

[8] Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2289026, acessado em 31/03/2023)

[9] Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2289026, acessado em 31/03/2023)

[10] Disponível em: https://www.camara.leg.br/propostas-legislativas/2256735, acessado em 06/05/2023

[11] "O termo Fake News ganhou força mundialmente em 2016, com a corrida presidencial dos Estados Unidos, época em que conteúdos falsos sobre a candidata Hillary Clinton foram compartilhados de forma intensa pelos eleitores de Donald Trump" (Disponível em: https://brasilescola.uol.com.br/curiosidades/o-que-sao-fake-news.htm , acessado em 22/03/2023)

[12] Pessoa jurídica fornecedora de serviços que consistem em possibilitar o acesso de seus consumidores à internet. (https://www.migalhas.com.br/depeso/211753/os-conceitos-de-provedores-no-marco-civil-da-internet , acessado em 22/03/2023)

> JUDICIAL. NECESSIDADE. ART. 19, § 1º, DA LEI Nº 12.965/2014 (**MARCO CIVIL DA INTERNET**). INDICAÇÃO DA URL. MONITORAMENTO DA REDE. **CENSURA PRÉVIA**. IMPOSSIBILIDADE. RESSARCIMENTO DOS HONORÁRIOS CONTRATUAIS. NÃO CABIMENTO.
> (STJ - REsp: 1568935 RJ 2015/0101137-0, Relator: Ministro RICARDO VILLAS BÔAS CUEVA, Data de Julgamento: 05/04/2016, T3 - TERCEIRA TURMA, Data de Publicação: DJe 13/04/2016) **(Grifos próprios)**[13]

> ELEIÇÕES 2016 - **RECURSO ELEITORAL** - PROPAGANDA ELEITORAL NEGATIVA - **FACEBOOK - PERFIL ANÔNIMO** – [...] 2. **Perfil anônimo com mensagens desfavoráveis e ofensivas ao candidato, de modo a caracterizar a propaganda eleitoral negativa.** 3. O art. 19, § 1º, da Lei Federal nº 12.965/14, que instituiu o **Marco Civil da Internet no Brasil**, dispõe que a decisão judicial que determina a retirada de conteúdo gerado por terceiros deverá conter, sob pena de nulidade, a identificação clara e específica do conteúdo considerado irregular, a fim de permitir a localização inequívoca do material. [...]
> (TRE-ES - RE: 3945 SERRA - ES, Relator: SAMUEL MEIRA BRASIL JUNIOR, Data de Julgamento: 28/11/2016, Data de Publicação: PSESS - Publicado em Sessão, Volume 18:47, Data 28/11/2016) **(Grifos próprios)**

Além dos projetos já abordados, o PL 2630/2020, que propõe uma denominada Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet, demonstra ser o mais popular no momento, justamente por agrupar uma grande lista de outros projetos de leis. O atual texto da proposta, que é apelidado de "PL das *fake News",* se propõe a inserir a proteção de dados pessoais e a privacidade como princípios (apresentados em conjunto[14]) mas faz também menção direta aos princípios do próprio MCI e da LGPD.(SILVA, 2023)

Trata-se de mais uma normativa direcionada para a regulamentação do meio virtual no sentido de ordenar o que pode ou não ser publicado, compartilhado e retirado desse ambiente. Embora proponha a criação de um crime em espécie[15], o delito estaria ligado a matéria eleitoral, seguindo a tendência de todo o texto e seus

---

[13] [...] 2. A responsabilidade dos provedores de conteúdo de internet em geral depende da existência ou não do controle editorial do material disponibilizado na rede. Não havendo esse controle, a responsabilização somente é devida se, após notificação judicial para a retirada do material, mantiver-se inerte. Se houver o controle, o provedor de conteúdo torna-se responsável pelo material publicado independentemente de notificação. Precedentes do STJ. 3. Cabe ao Poder Judiciário ponderar os elementos da responsabilidade civil dos indivíduos, nos casos de manifestações de pensamento na internet, em conjunto com o princípio constitucional de liberdade de expressão (art. 220, § 2º, da Constituição Federal). 4. A jurisprudência do STJ, em harmonia com o art. 19, § 1º, da Lei nº 12.965/2014 (Marco Civil da Internet), entende necessária a notificação judicial ao provedor de conteúdo ou de hospedagem para retirada de material apontado como infringente, com a indicação clara e específica da URL - Universal Resource Locator

[14] VI - a proteção de dados pessoais e da privacidade

[15] Art. 50. Promover ou financiar, pessoalmente ou por meio de terceiros, mediante uso de conta automatizada e outros meios ou expedientes não fornecidos diretamente pelo provedor de aplicações de internet, divulgação em massa de mensagens que contenha fato que sabe inverídico, que seja capaz de comprometer a higidez do processo eleitoral ou que possa causar dano à integridade física e seja passível de sanção criminal. Pena: reclusão, de 1(um) a 3 (três) anos e multa.

consequentes debates. Nesse contexto, os interesses políticos, a atuação da imprensa e a interferência de grandes plataformas, como Google e Meta, dificultam a construção da norma.(JORNAL NACIONAL, 2023)

Apesar do envolvimento indireto dos dados pessoais nos movimentos legislativos e nas referências jurisprudenciais, percebe-se que o principal enfoque é o de regulamentar o que pode ou não ser inserido no meio digital, o que pode ou não ser mantido no mesmo, e como deve ser mantido. Assim o MCI, Leis e projetos relacionados, atuam muito mais no sentindo de monitorar e fiscalizar o comportamento dos usuários e dos provedores de internet, afastando-se de uma atuação pela tutela dos dados pessoais contra ataques cibernéticos.(BRASIL, 2014)

Demonstrando tal situação, os ministros Dias Toffoli e Luiz Fux, convocaram a 38ª Audiência Pública do Supremo Tribunal Federal, realizada em março de 2023 com a participação de diversos especialistas do setor privado e governamental para tratar sobre a responsabilidade dos provedores de internet diante de conteúdos de terceiros frente ao Marco Civil da Internet. As falas dos representantes centralizaram-se em questões sobre notícias falsas, liberdade de expressão e interpretação do Marco de acordo com a Constituição.(“Audiência Pública: mais 15 expositores participam do debate sobre Marco Civil da Internet”, 2023)

Ainda que o Art 12º do MCI[16] considere que suas sanções próprias não eliminam a aplicação das demais sanções cíveis, criminais ou administrativas, o seu trecho sancionador é voltado para pessoas jurídicas, e envolve pontos financeiros e operacionais na aplicação de multas, advertências e restrições. Suas penalizações são centralizadas na esfera civil e administrativa, sem criar qualquer tipo de crime, tampouco alterar algum dispositivo no Código Penal.

Em 2021, algumas alterações foram propostas na Medida Provisória nº 1.068/2021[17], todavia o Congresso Nacional, apoiado pelo parecer da Ordem dos Advogados do Brasil, rejeitou e devolveu a MP considerando que as alterações eram

[16] Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa: I - advertência, com indicação de prazo para adoção de medidas corretivas; II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção; III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11.

[17] Altera a Lei nº 12.965, de 23 de abril de 2014, e a Lei nº 9.610, de 19 de fevereiro de 1998, para dispor sobre o uso de redes sociais

inesperadas e causariam insegurança jurídica para os envolvidos. (ATO DECLARATÓRIO DO PRESIDENTE DA MESA DO CONGRESSO NACIONAL Nº 58, DE 2021, 2021) As sugestões versavam principalmente sobre os agentes estrangeiros e o cenário eleitoral, pouco acrescentando na análise penal e na defesa contra cibercrimes. Na incidência de um cibercrime, a aplicação do MCI seria direcionada para a responsabilização dos provedores e para os trabalhos investigativos no processo penal uma vez que o documento não possui sanções penais em sua redação.

Utilizando os crimes envolvendo pornografia como comparativo, nota-se que, mesmo o Código Penal apresentando como crime a “divulgação de cena de estupro ou de cena de estupro de vulnerável, de cena de sexo ou de pornografia” em seu artigo 218[18] e aplicando ainda a agravante em casos envolvendo crianças (artigo 61, II, h), encontramos, também, uma série de artigos mais específicos no Estatuto da Criança e do Adolescente (ECA) tutelando sobre o tema, do Art 241 ao 241-E. No entanto, nada similar é discutido ou citado no MCI.

Embora o MCI tenha sido sancionado na vigência da Lei Carolina Dieckmann (Lei nº 12.737/2012), pouco se avançou na prevenção e na investigação de crimes cometidos integralmente no meio digital. Alguns dispositivos e princípios se relacionam ao tema, porém a inexistência de um diploma legal específico sobre a proteção de dados pessoais tornou-se cada vez mais um empecilho à efetividade do princípio constitucional da intimidade e da vida privada (inciso X, da Constituição Federal), bem como para a correta e clara delimitação das atividades e ações envolvendo dados pessoais.(GIACCHETTA; MENEGUETTI, 2014)

Nesse contexto, as próximas páginas serão dedicadas a análise de normativas relevantes sobre a proteção de dados pessoais, partindo do âmbito internacional (*General Data Protection Regulation)* para o nacional (Lei Geral de Proteção de Dados Pessoais).

2.3 NORMATIVAS DIRECIONADAS A PROTEÇÃO DE DADOS PESSOAIS

[18] [18]Art. 218-C. Oferecer, trocar, disponibilizar, transmitir, vender ou expor à venda, distribuir, publicar ou divulgar, por qualquer meio - inclusive por meio de comunicação de massa ou sistema de informática ou telemática -, fotografia, vídeo ou outro registro audiovisual que contenha cena de estupro ou de estupro de vulnerável ou que faça apologia ou induza a sua prática, ou, sem o consentimento da vítima, cena de sexo, nudez ou pornografia: Pena - reclusão, de 1 (um) a 5 (cinco) anos, se o fato não constitui crime mais grave.

Seguindo a nova arquitetura organizacional na chamada “Quarta revolução industrial”, onde a informação ocupa papel central para o desenvolvimento da economia, o tratamento dos dados pessoais passou a ser uma preocupação, ao passo que sua regulamentação se tornava uma lacuna cada vez maior.(GOMES; BITTENCOURT, 2019) Para muitos, os dados pessoais ocupam a figura de novo petróleo nos dias atuais, tendo em vista o valor econômico que tais informações podem gerar para órgãos públicos e empresas.(SHAHUL, 2018)

Independentemente se de forma concreta ou invisível, a informação é coletada, agrupada e tratada, compondo grandes bancos de dados principalmente no meio digital, onde a conexão das informações ocorre de forma mais acelerada. Nas palavras de EUGENIA FINKELSTEIN; FINKELSTEIN (2019, p.290) a utilização desses bancos de dados “encontra-se numa zona cinzenta, uma vez que nem o usuário nem o Poder Público sabem exatamente a forma da utilização destas informações”.

O desenvolvimento da economia digital e a crescente utilização de dados pessoais demostrou uma certa dificuldade de a legislação acompanhar os avanços na regulação desse mercado. Embora o MCI regulamente o ambiente virtual, as regras e diretrizes são escassas para os novos comportamentos nesse meio, sobretudo em pontos sobre responsabilidades, conceitos, procedimentos, sanções e fiscalizações.(DERBLI, 2019)

No Brasil, os dois principais documentos que versam sobre este tema são o documento europeu, GDPR, e o diploma brasileiro, a LGPD. Na prática, a norma internacional foi a base protagonista para a criação da norma nacional e ambas serão analisadas nos tópicos a seguir.

2.3.1 General Data Protection Regulation

Na Europa, movimentos iniciados em 2012 resultaram na aprovação do *General Data Protection Regulation* (GDPR - Regulamento Geral sobre a Proteção de Dados) no ano de 2016. A norma entrou em vigor em 2018 com objetivo não só de atualizar e centralizar as legislações dos países europeus, mas principalmente “ampliar o escopo de proteção à privacidade e modernizar a legislação para desafios tecnológicos, econômicos e políticos atuais, com aqueles decorrentes do advento da internet”.(MALDONADO; BLUM, 2019)

Ainda que não entre em detalhes penais, a redação do Regulamento reconhece que existem novos desafios na matéria da proteção penal tendo em vista a globalização e seus efeitos relacionados a evolução da tecnologia.(UNIÃO EUROPÉIA, 2016) Tal situação ressalta a função social do direito, que deve se adaptar constantemente às mudanças da sociedade e regulamentar novas situações para promover a paz, a ordem e a justiça no contexto vigente, além de fornecer soluções para conflitos entre indivíduos ou grupos.(NADER, 2014)

Conceitualmente, o texto europeu define como "dado pessoal"[19] dados "diretos" como nome, dados de contato, número de passaporte, e outras informações que se relacionam diretamente a uma pessoa física, mas também informações indiretas, como registros médicos, dados de navegação e placa de carro. Apesar de não estarem diretamente ligados a um indivíduo, esses dados podem ser combinados com outras informações para identificar o titular dos dados.(UNIÃO EUROPÉIA, 2016)

Em relação às sanções, o foco mais uma vez é em questões administrativas, que inclusive já movimentaram bilhões de euros a título de multas. Segundo a pesquisa do escritório de advocacia multinacional DLA Piper[20], os órgãos reguladores europeus aplicaram €2,9 bilhões em multas da GDPR, com destaque para o órgão irlandês, o *Data Protection Commission*, que autuou a *Meta Platforms* em €405 milhões por supostas falhas na proteção dos dados pessoais das crianças no Instagram.(MULCAHY, 2023)

Na esfera penal, o documento prevê apenas que:

> *[...] efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, e de livre circulação desses dados, é objeto de um ato jurídico da União específico.*(PARLAMENTO EUROPEU, 2016)

O trecho em questão faz menção à Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, o qual aborda sobre o tratamento de dados pessoais realizado *"pelas autoridades competentes para efeitos de prevenção, investigação,*

---

[19] *informação relativa a uma pessoa singular identificada ou identificável (titular dos dados); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular.* (UNIÃO EUROPÉIA, 2016)

[20] https://www.dlapiper.com/en-gb

deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados".(PARLAMENTO EUROPEU, 2016) Neste documento, o foco é regulamentar a atuação estatal na cooperação jurídica-policial durante investigações e processos judiciais, criando balizas sobre quais dados podem ser utilizados e como devem ser tratados ao longo das etapas processuais. Dessa forma, a abordagem sobre os cibercrimes em si e a tutela penal ficam direcionadas pela Convenção de Budapeste, que será trabalhada em outros capítulos do presente trabalho.

2.3.2 Lei Geral de Proteção de Dados Pessoais

A normativa europeia da GDPR foi elemento de forte inspiração para a elaboração de um documento brasileiro. Da mesma forma, suas orientações relacionadas a questões fiscalizatórias, doutrinárias e jurisprudências podem servir de base para outros Estados como o Brasil.(OLIVEIRA, 2022) O avanço das novas tecnologias e o movimento legislativo de outros países aceleraram a construção de uma norma local sobre a proteção de dados pessoais, pois o Brasil era requisitado por padrões equivalentes em seu território.

Considerando que os dados vão e vem de forma livre e constante, em rotas migratórias que não exigem passaportes, cabia ao Brasil ao menos acompanhar as diretrizes construídas por outras nações, sobretudo aquelas mais relevantes no quesito socioeconômico como as da União Europeia. De forma geral, BIONI; RIELLI (2021) elencam quatro principais fatores que justificam a promulgação da LGPD: (i) o escândalo a Cambridge Analytica; (ii) a entrada em vigor do GDPR; (iii) o desejo brasileiro de ingressar no Organização para a Cooperação e Desenvolvimento Econômico (OCDE) e (iv) a articulação interna na Câmara dos Deputados para a aprovação das alterações na Lei do Cadastro Positivo que envolvia a própria LGPD.

A LGPD teve origem no PL da Câmara n° 53 de 2018 o qual foi aprovado em regime de urgência pelo Plenário do Senado em julho de 2018[21] e já publicado, no mês seguinte, no Diário Oficial com prazo de 18 meses para entrar em vigência. Em março de 2020, no contexto da pandemia causada pelo Coronavírus, entrou em

[21] https://www12.senado.leg.br/noticias/materias/2020/09/18/lei-geral-de-protecao-de-dados-entra-em-vigor acessado em 04/04/2023

cena o PL nº 1179 de 2020[22] o qual abordava sobre o regime jurídico emergencial e transitório das relações jurídicas de Direito Privado no período da pandemia e impactou o andamento de algumas tramitações no Congresso Federal.

No mesmo contexto de pandemia e reordenamento social, a Medida Provisória 959/2020[23] pretendia adiar a entrada em vigor da LGPD para maio de 2021 enquanto a Lei nº 14.010/2020[24] postergou as sanções administrativas para o dia 1º de agosto de 2021. Toda essa dinâmica legislativa terminou apenas em setembro de 2020, no último dia possível para que o Presidente se pronunciasse sobre a matéria, permitindo assim, que a LGPD entrasse em vigor de fato a partir do dia 18 de setembro de 2020.(RODRIGUES, 2021)

Em âmbito nacional, a LGPD é vista como um avanço significativo na proteção de dados pessoais. A partir de uma demanda social, debates vieram à tona relacionando os dados pessoais com outras temáticas do direito como a responsabilidade civil, tributação e questões penais, como proposto neste trabalho. Também cabe mencionar, que a presença da LGPD provocou mudanças no pensamento das organizações privadas, que passaram a considerar a proteção de dados pessoais na revisão dos seus processos internos e na construção da cultura corporativa.(LUGATI; ALMEIDA, 2022)

2.3.2.1 Conceitos da LGPD

Considerando o avanço da tecnologia e seus impactos na sociedade, a redação da lei apresenta de forma taxativa, e logo em seu primeiro artigo, que sua aplicação ocorre tanto no meio físico como no digital.[25] O legislador utiliza do Artigo 5º para conceituar termos relevantes na leitura do texto e aplicação da lei, tendo como ponto de partida justamente o “dado pessoal”[26]. Seguindo a linha expansionista da GDPR, o conceito engloba as informações de pessoas naturais, identificada de forma direta, ou identificável através de cruzamento de outras

[22] https://www25.senado.leg.br/web/atividade/materias/-/materia/141306 acessado em 04/04/2023
[23] https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv959.htm acessado em 04/04/2023
[24] https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14010.htm acessado em 04/04/2023
[25] “Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais**, inclusive nos meios digitais**, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.” (grifos próprios) (BRASIL, 2018)
[26] I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

informações. Assim, o que prevalece é “o fato de estar vinculada a uma pessoa, revelando ou podendo revelar algum aspecto objetivo desta”.(DONEDA, 2021)

No contexto informático, tais dados podem ser aqueles inseridos no meio, como nome, e-mail, CPF e os mais variados tipos de documentos, mas também os dados gerados pelo uso da internet, a exemplo de *cookies*[27], *Internet Protocol* (IP)[28], histórico do navegador, histórico de compras. São informações que podem ser tratadas em um equipamento *offline*, mas que costumam sem guardadas e operadas em rede, nos armazenamentos em nuvem[29].(VAINZOF, 2020)

O conceito de “dado” é ramificado para “dados pessoais sensíveis”[30] , “dados pseudoanonimizados” e “dados anonimizados”[31]. A definição dos sensíveis é taxativa na LGPD, que elenca quais são os dados considerados sensíveis, mas por outro lado, a questão da anonimização, total ou parcial, levanta algumas lacunas e subjetividades, tanto por sua redação na Lei mas principalmente pelo perfil utópico da anonimização.

BIONI (2020) argumenta que o processo de anonimização tem demonstrado ser algo falível, e considera um mito a ideia de que os dados pessoais podem ser completamente anonimizados com absoluta eficiência. O autor também propõe o debate sobre a ambiguidade e certa contradição do objetivo de anonimização dos dados pessoais:

> [...] leis que adotam o conceito expansionista de dados pessoais e, ao mesmo tempo, estabelecem uma dicotomia deste com dados anônimos correriam o risco de serem tautológicas. Isso porque haveria uma redundância normativa, já que dados anônimos seriam, em última análise, potencial e provavelmente, dados relacionados a uma pessoa identificável.(BIONI, 2020, p.192)

De modo geral, e recorrendo a um comparativo com a GDPR, temos que os dados anônimos não identificam e não são capazes de identificar um titular de

---

[27] Os cookies são pequenos arquivos criados por sites visitados e que são salvos no computador do usuário, por meio do navegador. Disponível em: https://www.techtudo.com.br/noticias/2013/05/o-que-e-o-ip-descubra-para-o-que-serve-e-qual-e-seu-numero.ghtml. Acesso em: 5 abr. 2023

[28] O IP (ou Internet Protocol) é uma identificação única para cada computador conectado a uma rede. Disponível em: https://www.techtudo.com.br/noticias/2018/10/o-que-sao-cookies-entenda-os-dados-que-os-sites-guardam-sobre-voce.ghtml. Acesso em: 5 abr. 2023.

[29] O armazenamento em nuvem elimina a necessidade de comprar e gerenciar sua própria infraestrutura de armazenamento de dados, oferecendo agilidade, escalabilidade e durabilidade com acesso aos dados a qualquer hora e em qualquer lugar.

[30] II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

[31] III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

dados.(PARLAMENTO EUROPEU, 2016) Com isso, o quadro 2 demonstra como VAINZOF (2020) propõe a definição de cada tipo de dado.

Categoria	**Dados pessoais diretos**	**Dados pessoais indiretos**	**Dados pessoais pseudonimizados**	**Dado anonimizado**
Definição	Identifica diretamente uma pessoa natural, sem a necessidade de outras informações, como CPF, CPF, titula eleitoral, nome (se não houver homônimos)	Torna a pessoa natural identificável, pois necessitam de informações adicionais para identificá-la, como gostos, interesses, hábitos de consumo, profissão, sexo, idade e geolocalização	Dado que perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro	Não são dados pessoais: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento

Quadro 2: Definição dos tipos de dados, de acordo com Rony Vainzof – (VAINZOF, 2020)

Embora o meio virtual seja mais propício à anonimização dos dados pessoais em comparação ao ambiente físico, o processo em questão depende de habilidades e recursos técnicos específicos além de alto investimento financeiro por parte das organizações. Dessa forma, são raras as situações em que um cibercriminoso encontra um banco de dados pessoais integralmente anonimizado.

Prosseguindo com a redação da LGPD há a descrição de dois personagens fundamentais na prática da lei: operador e o controlador.

> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

Mesmo que o trecho cite a possibilidade de uma pessoa natural ocupar o papel desses agentes, o mais comum, quando estamos analisando o contexto informático e digital, é encontrar pessoas jurídicas nessas funções. Nesta linha, a Autoridade Nacional de Proteção de Dados (ANPD) afirmou que a definição de operador e controlador dependem do contexto fático e do seu caráter institucional.

Assim, não são considerados operadores ou controladores os indivíduos subordinados tais como funcionários, servidores públicos ou as equipes de trabalho

de uma organização. No caso de uma pessoa jurídica, a organização é o agente de tratamento para fins da LGPD, estabelecendo as regras para o tratamento de dados pessoais a serem executados por seus representantes e prepostos. Os subordinados obedecem aos direcionamentos do controlador e não se confundem com a definição de operador.(AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS, 2022)

Sintetizando o contexto, podemos utilizar do quadro 3 para visualizar uma situação hipotética:

EXEMPLO	**PAPEL COM BASE NA LGPD**			
	MARIA	**HOSPITAL SAÚDE**	**SAÚDE TECH**	**PACIENTES**
Maria é médica empregada do Hospital Saúde, constituído sob a forma de associação civil sem fins lucrativos. Nessa condição, atua como principal representante do hospital junto a um serviço de armazenamento de dados de pacientes em nuvem, analisando exames, gerando documentos e assinando os contratos correspondentes. O serviço de armazenamento é fornecido pela empresa Saúde Tech.	Não se caracteriza como agente de tratamento	Controlador	Operador	Titulares de dados pessoais

Quadro 3: Exemplo e definição de agentes de tratamento Baseado em AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS, 2022)

No contexto hipotético, o Hospital Saúde e a empresa Saúde Tech são os agentes com as maiores e principais responsabilidades frente à LGPD, devendo atender os direitos dos titulares de dados, as bases legais e os princípios da lei.

2.3.2.2 Princípios da LGPD relacionados ao combate do cibercrime

A LGPD apresente uma lista com dez princípios em seu Art 6º e outras questões sobre bases legais ao longo do texto, no entanto apenas os princípios da segurança e o da prevenção serão analisados de forma individual tendo em vista a temática e delimitação do presente trabalho.

A) Princípio da segurança [32]

O cerne desse princípio é o de manter os dados pessoais em um ambiente seguro, constantemente monitorado e aprimorado no quesito segurança, com as melhores e mais modernas ferramentas. Para isso, PESTANA (2020) argumenta que os “agentes de tratamento devem utilizar medidas técnicas e administrativas aptas a proteger os dados pessoais” não somente em relação aos eventos dolosos, mas também acidentais, quer seja ou não resultado de negligência, imprudência ou imperícia.

As medidas de segurança devem considerar as ameaças internas da organização a exemplo dos acessos de colaboradores, além das ameaças externas como os ataques cibernéticos. Já o nível de exigência não pode ser presumido e deve ser proporcional ao risco do tratamento, com base em avaliações técnicas que analisem o tamanho do banco de dados, o tipo de dado e sua relevância, considerando ainda possíveis direcionamentos da ANPD em relação aos padrões técnicos. (VAINZOF, 2020)

B) Princípio da prevenção[33]

Embora esteja contemplado de forma indireta no princípio anterior, o legislador optou por apresentar a prevenção de forma ainda mais específica. De qualquer forma, trata-se de uma “reiteração, uma vez que a proteção dos dados, antes, durante a após tratamento é um dever imposto a aqueles que os acessam e os utilizam, sendo abrangidos pelo princípio da segurança”. (PESTANA, 2020)

Sob outra perspectiva, PESTANA (2020) propõe que a análise deste princípio seja feita com referência à conceituação de “Privacy by design”. Nessa cultura corporativa, a organização atua de forma mais proativa do que reativa, tratando a privacidade como elemento fundamental na construção de processos e

[32] “VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;”(BRASIL, 2018)

[33] “VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;”(BRASIL, 2018)

ferramentas, desde o marco zero e sem afetar a qualidade do projeto. (VAINZOF, 2020)

Essa filosofia de proteção e prevenção no mundo corporativo ganha relevância ainda maior quando se observa o Art 43 da LGPD[34]. O tópico aborda sobre a exclusão da responsabilidade dos agentes e considera como uma das possibilidades as situações em que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros.(BRASIL, 2018) Nestes casos, a responsabilização pode recair sobre a vítima do evento danoso ou terceiros, afastando o nexo causal entre a ação ou omissão do agente de tratamento e o dano gerado.

Segundo BRUNO (2020) esse contexto gera debates sobre situações como a invasão de um sistema que armazena dados pessoais por um agente mal-intencionado e não autorizado. Considerando que o agente mal-intencionado é um terceiro, seria esse exemplo uma culpa de terceiro ou não? Para o autor, a segurança absoluta dos sistemas informáticos é algo utópicos pois como ele argumenta: “nenhum sistema é à prova de falhas ou vulnerabilidades, até porque a tecnologia de invasões evolui na mesma proporção (ou até mais rápido) que a tecnologia para defesa desses incidentes".

Neste cenário, para os agentes de tratamento que desejem se afastar, total ou parcialmente da responsabilidade, é importante registrar e armazenar comprovações de suas medidas de segurança preventivas. Tais medidas poderão ser consideradas pelo julgador e/ou pela ANPD, em caso de litígios ou sanções.[35] Prova disso, é o recorte jurisprudencial do Tribunal de Justiça de São Paulo:

> Não se pode fechar os olhos a uma dura e triste realidade: os sistemas computacionais não são 100% indevassáveis. Aí estão os hackers para demonstrar que a muralha digital, inclusive aquela erguida nos grandes centros tecnológicos mundiais, ostenta um certo grau de vulnerabilidade.
> Em semelhante cenário, que coonesta a asserção da apelante de que terceiros, à sua revelia, acessaram o sistema da apelada, a melhor solução para o caso, inspirada na ideia da régua lésbica da equidade proposta por Aristóteles, é a divisão, pela metade, dos prejuízos decorrentes da emissão

[34] Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem: I - que não realizaram o tratamento de dados pessoais que lhes é atribuído; II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

[35] Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:[...] § 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios: [...] VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei; IX - a adoção de política de boas práticas e governança;

> fraudulenta de passagens (TJSP, Apelação 1083389- 32.2015.8.26.0100, Rel. Des. Antonio Nascimento, j. 25.08.2016).

Diante deste contexto, com menção direta a ações maliciosas de alguns agentes, abre-se margem para conectar o tema com o Direito Penal, sobretudo no seu aspecto julgador e punitivo. Em contrapartida, assim como as normas já analisadas neste trabalho precisaram se adaptar a um novo contexto com elementos virtuais, cabe também verificar como o Direito Penal se organiza para se encaixar nessa nova realidade.

3 O DIREITO PENAL INFORMÁTICO E OS ATAQUES CIBERNÉTICOS CONTRA OS DADOS PESSOAIS

A informação que antes era predominantemente tratada na forma física, passou a ser processada cada vez mais no meio virtual, com maior alcance e velocidade. (SYDOW, 2023) Com isso, nasce uma nova realidade na qual os indivíduos e suas atividades se aglomeram em um novo ambiente chamado de ciberespaço, que por sua vez é formado pelo conjunto de redes da Internet. (SANTOS, 2015) No ciberespaço, os indivíduos podem interagir sem presença física, estabelecendo diversas e valiosas relações por meio de dados e conexões virtuais.

Pensando na ideia de sociedade de risco[36], se por um lado ganha-se dinamismo, por outro há uma diminuição na proteção criminal, visto que esse progresso da modernização causa novas ameaças como efeito colateral indesejado. (CALLEGARI; ANDRADE, 2020). A construção jurídica opera em menor velocidade quando comparada a evolução tecnológica, e como apresenta SANTOS (2015): “à medida que aumenta o número de utilizadores no Ciberespaço aumentam também as expectativas de que as normas legais do mundo real sejam igualmente aplicáveis”.

Tais expectativas nascem pela repercussão de cibercrimes dos mais variados tipos, realizados de forma frequente, perigosa e violadora de direitos fundamentais.(SOBRINHO; GROTT, 2022) Parte considerável dessas expectativas e

[36] Expressão criada pelo sociólogo alemão Ulrich Beck no contexto da degradação ambiental após a Revolução Industrial. Trata-se de uma reflexão pelo fato de o ser humano, após um período de desenvolvimento tecnológico e científico desenfreado, perceber as consequências destrutivas e nocivas desses avanços sem limites.(CALLEGARI; ANDRADE, 2020)

a sensação de insegurança são alimentadas pela atuação midiática que destaca os conflitos de seu interesse e os assuntos dignos de maior preocupação, mas não discute de forma equivalente sobre as reais causas de criminalidades e formas efetivas de diminuí-las.(FLORES, 2017; NASCIMENTO JUNIOR, 2016)

De forma consequente, as autoridades legislativas direcionam suas atuações para atender as demandas mais destacadas pela mídia e pela sociedade, recorrendo muitas vezes para a matéria penal, considerando ser esta a área do direito mais rigorosa e relevante para a proteção da sociedade.(FLORES, 2017) Entretanto, em muitos casos esse direcionamento é feito de forma desproporcional e desorganizada, ferindo a ideia de intervenção mínima do Direito Penal.

Utilizar o Direito Penal como único mecanismo de resolução da criminalidade cibernética tende a gerar uma criação indiscriminada de leis confusas e carentes de conhecimento técnico.(NASCIMENTO JUNIOR, 2016) Recorrendo a outros casos como comparativo, nota-se que crimes ambientais e crimes de droga não foram plenamente resolvidos com a aplicação individual do Direito Penal e ainda impactam negativamente em outros problemas jurídicos como por exemplo o super encarceramento.

De modo geral, a expansão do Direito Penal decorre de uma série de fatores, tais como: o surgimento de novos interesses, a aparição de novos riscos, a sensação social de insegurança, a identificação da maioria social com a vítima do delito, além do descrédito de outras instâncias de proteção.(MACRI JÚNIOR; MACRI, 2017) Nesse contexto, ainda que se reconheça os problemas envolvendo o alargamento do Direito Penal, é necessário analisar como a matéria se reordenou - e se reordena - para contemplar as novas realidades, com o objetivo de garantir, ou ao menos contribuir para a tutela dos bens jurídicos relevantes para a sociedade tecnológica.

Tal análise parte da definição e classificações dos cibercrimes, sua alocação no Direito Penal e o bem jurídico envolvido, passando depois para a exposição sobre o impacto da Convenção de Budapeste no Brasil e os ataques cibernéticos aplicados no cenário brasileiro.

3.1 O CIBERCRIME E O BEM JURÍDICO INFORMÁTICO

A aplicação do direito no ambiente informático apresenta de imediato algumas dificuldades não só para a definição de termos e conceitos, mas também para identificar quais são os valores protegidos pela dogmática penal.(D'AVILA; DOS SANTOS, 2016) A divergência conceitual pode ser observada por exemplo com a variedade dos nomes das delegacias especializadas da Polícia Civil nos estados brasileiros: Delegacia Especial de Repressão aos Crimes Cibernéticos (DRCC-DF), Delegacia de Repressão aos Crimes de Informática (DRCI – SC), Delegacia de Repressão a Crimes Eletrônicos (DRCE – ES), entre outras.(BARRETO; KUFA; SILVA, 2022)

Doutrinalmente, também não há alinhamento conciso sobre um conceito específico para se referir à criminalidade no contexto informático, sendo comum encontrar diferentes grafias como cibercrime, crime informático, crime cibernético etc. Nenhum dos termos consegue escapar de imperfeições conceituais e acabam não conseguindo contemplar todos os sentidos possíveis dessa nova categoria criminal.(SOUZA, 2021) De toda forma, para padronizar ao longo do trabalho, adotarei o termo cibercrime, seguindo a nomenclatura utilizada na Convenção de Budapeste, principal documento internacional sobre o tema.

Quanto a sua definição, existem duas principais correntes doutrinárias; a tripartida, e a bipartida.(BRITO, 2014) A primeira, considera o cibercrime como "todo o ato em que o computador serve de meio para atingir um objetivo criminoso, ou em que o computador é alvo simbólico desse ato ou em que o computador é objeto de crime"(MARQUES; MARTINS, 2006). Por sua vez, a ideia bipartidária analisa apenas se a infração é algo próprio e originário do ambiente tecnológico ou se deriva de delitos já tipificados no Código Penal. (BARRETO; KUFA; SILVA, 2022)

Ultrapassada as questões conceituais, parte-se para a análise das duas linhas doutrinárias, seguida da exploração sobre o bem jurídico envolvido e protegido nos cibercrimes.

3.1.1 Divisão tripartidária dos cibercrimes

De acordo com essa corrente, o cibercrime é um fato típico, ilícito e culpável cometido por meio da tecnologia da informação ou contra esta.(FILHO, 2021) Sua ramificação ocorre principalmente com base na finalidade da ação e no bem jurídico

envolvido para dividir os cibercrimes em três grupos: puros, mistos e impróprios ou comuns.

- **Cibercrimes Puros:** Todas e quaisquer condutas ilícitas que objetivam afetar a integridade lógica ou física do sistema computacional. São crimes informáticos propriamente ditos que atingem, ou buscam atingir, o *software* (programa), o *hardware* (componente físico como monitor, teclado), sistemas e/ou os dados e as informações neles utilizadas.(FILHO, 2021)

Na prática jurisprudencial, tal classificação pode ser ilustrada no crime de invasão de dispositivo, como discutido no Tribunal de Justiça de São Paulo[37]:

- **Cibercrimes Misto:** São aqueles em que os meios computacionais são cruciais para a efetivação da conduta. Ainda que o bem jurídico lesado no caso seja diverso do informático, a utilização de uma ferramenta informática é condicionante para o delito. A ocorrência dessas ações atinge não só a tecnologia da informação, mas também outro bem tutelado pelo Direito Penal.(FILHO, 2021)

Segundo disponibilizado pelo Instituto Brasileiro de Ciências Criminais (IBCCRIM), exemplos de cibercrimes mistos são as transferências ilícitas de valores nos *home-banking*[38] realizadas por um criminoso que diariamente retira pequenas quantias de diferentes de contas-correntes e transfere para uma única conta. Trata-se de uma versão atualizada e dependente do meio informático sobre o crime de “lavagem de dinheiro”, que é tema central das Lei nº 9.613 de1998[39] e nº 12.683 de 2012[40].

- **Cibercrimes Impróprios ou Comuns:** Reúne os delitos em “que os dispositivos computacionais são utilizados apenas como instrumento para a realização de um delito já tipificado pela lei penal”.(FILHO, 2021) Em outras

[37]Apelação. Invasão de dispositivo informático. Art. 154-A do CP. Sentença absolutória. Pretendida condenação do acusado. Não cabimento. Negativa do réu. Provas nos autos que não são seguras para sua condenação. Aplicação do princípio do in dubio pro reo. Absolvição que fica mantida. Recurso não provido. (TJ-SP - APR: 00717029420168260050 SP 0071702-94.2016.8.26.0050, Relator: Xisto Albarelli Rangel Neto, Data de Julgamento: 28/09/2020, 13ª Câmara de Direito Criminal, Data de Publicação: 28/09/2020)

[38] Também chamado de internet banking permite que você acesse suas contas bancárias a qualquer hora e de qualquer lugar, desde que tenha acesso à internet. Disponível em: https://exame.com/invest/guia/o-que-e-internet-banking-como-acessar-e-para-que-serve/ acessado em 21/04/2023

[39] Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras - COAF, e dá outras providências

[40] Altera a Lei nº 9.613, de 3 de março de 1998, para tornar mais eficiente a persecução penal dos crimes de lavagem de dinheiro.

palavras, são crimes que já eram previstos na legislação penal e foram adaptados para as novas conjunturas sociais.

Tais alterações justificam-se pela necessidade de atender os princípios penais da legalidade e da taxatividade, pois como argumenta BITENCOURT (2011) a lei penal deve “estabelecer quais são as condutas puníveis e as sanções a elas evitando ao máximo redações ambíguas, contraditórias, vagas ou desatualizadas”.

Na prática, a maior parte dessas adaptações gera novas qualificadoras para os casos em que o delito seja cometido por meio ou com o auxílio de dispositivo eletrônico ou informático, como, por exemplo, as mudanças aplicadas pela Lei nº 14.155 de 2021 que incluiu no código penal o § 4º-B[41] no Art 155 do CP (furto) e criou a “fraude eletrônica” prevista no § 2º-A[42] no Art 171 do CP (estelionato). Além desses, os crimes do capítulo contra a honra (Art 138 ao Art 145 do CP) também podem compor o grupo dos cibercrimes impróprios, sobretudo nas situações que envolvem notícias e comentários publicados em sites ou redes sociais[43].

3.1.2 Divisão bipartidária dos cibercrimes

A corrente bipartidária defende a utilização de apenas dois grandes grupos do cibercrime; o próprio e o impróprio. Tal aplicação tem certa semelhança com a divisão tradicional do Direito Penal em que os delitos comuns possuem sujeito ativo indeterminado, podendo ser praticados por qualquer um, e os delitos próprios ou especiais exigem determinado perfil do autor.(PRADO, 2019)

Ainda que os crimes próprios pressuponham certas habilidades e conhecimentos do delinquente, o fator determinante desta separação é a ferramenta e o ambiente da ação, e não as qualificações do sujeito ativo. Em relação à divisão

---

[41] § 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é 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.

[42] § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.

[43] QUEIXA CRIME CONTRA A HONRA. DIFAMAÇÃO E INJÚRIA. SUPOSTA OFENSA PROFERIDA POR MÍDIA SOCIAL. DEPUTADO FEDERAL. IMUNIDADE PARLAMENTAR. ART. 53, CAPUT, CF. ABRANGÊNCIA. OFENSA GENÉRICA. AUSÊNCIA DE ELEMENTO SUBJETIVO. REJEIÇÃO. (STF - Pet: 5956 DF - DISTRITO FEDERAL 0011594-63.2016.1.00.0000, Relator: Min. ROSA WEBER, Data de Julgamento: 06/03/2018, Primeira Turma, Data de Publicação: DJe-068 10-04-2018)

anterior, a ideia bipartida busca minimizar as dificuldades da categorização, sobretudo no que se refere aos crimes mistos e impróprios.(SYDOW, 2023)

- **Cibercrimes Próprios:** São os cibercrimes que são praticados por computador e são também consumidos em meio eletrônico, violando sua disponibilidade, integridade e/ou confidencialidade. (ALMEIDA et al.,2015) Caracterizam-se pela sua autonomia e distinção das infrações positivadas no Código Penal tendo em vista que acompanharam o surgimento e a evolução do computador e da internet.(MATSUYAMA; LIMA, [s.d.])

Comparando com a corrente anterior, equivalem aos cibercrimes puros, nos quais os sistemas, equipamentos, e os dados inseridos nesses elementos são os protagonistas da ação. De forma concreta cabem aqui os crimes: invasão de dispositivo informático (Art 154-A), inserção de dados falsos em sistema de informações (Art 313-A) e interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública (Art 266), todos previstos no Código Penal.

- **Cibercrimes Impróprios:** São aqueles delitos que se utilizam de mecanismos informáticos como ferramenta, sendo que outros meios poderiam ser igualmente escolhidos para isso. Em outras palavras, a máquina ou o sistema informático é o instrumento para realização de condutas ilícitas já previstas no Código Penal. Neste caso, não há a essencialidade da informática como meio, sendo apenas mais uma possibilidade de realização.(DOS SANTOS, 2021)

Em geral, as justificativas legislativas argumentam sobre a necessidade de frear o crescimento acelerado dessas variações criminais, sustentando que são imprescindíveis instrumentos sancionadores para punir esses crimes de forma mais rigorosa.

Nesse grupo de crimes com uma nova roupagem, podemos encontrar previsões mais taxativas como o Art 241-A do ECA[44], que cita “meios informáticos” em sua redação, mas também outras possibilidades como nos crimes de extorsão e

[44]Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente

perseguição (respectivamente Art 158[45] e 147-A[46] do CP) que garantem a tutela penal em qualquer meio.(DOS SANTOS, 2021)

Tratando-se de uma divisão fortemente hermenêutica, não se encontram muitas razões para tornar a análise das classificações algo confuso e massivamente debatido. Com isso, adotar a ideia bipartidária demonstra ser o caminho mais fluido para os estudos sobre o cibercrime, utilizando o meio de criação do delito como único fator de separação.

De toda forma, o mais valioso aqui é visualizar como o cibercrime pode ser estudado penalmente. Tais delitos constituem o Direito Penal Informático, um ramo do Direito Penal, sendo, portanto, tratados como Direito Público. Embora estejam dispostos na parte especial do código, o Direito Penal Informático possui um caráter transbordante, com uma atuação em escala global e não se restringem só a novos tipos penais, podendo interferir em novas análises em muitos artigos do Código. De certa forma, é uma vertente do Direito Penal aplicada em um contexto de tecnologia e imaterialidade.(SYDOW, 2023)

No ramo penalista informático, algumas ações exigem novos raciocínios, princípios e paradigmas. Se por um lado os cibercrimes impróprios ou comuns já possuem bem jurídico mais bem definido e detalhado, os cibercrimes tratados como puros ou próprios ainda não se estabilizaram no Código Penal e são frequentemente modificados.(SYDOW, 2023) Neste contexto, o direcionamento do presente trabalho se manterá para os cibercrimes puros e próprios, acompanhando a ideia de SYDOW (2023) de que nesses crimes o objetivo da conduta é necessariamente atingir o bem jurídico informático.

3.1.3 Bem jurídico informático

Compactuando com BUSATO (2017) a primeira etapa a ser trabalhada sobre bem jurídico consiste na diferenciação entre o bem jurídico e o objeto material do delito. Segundo PRADO (2019) o objeto está alocado no plano estrutural, sendo

[45] Art. 158 - Constranger alguém, mediante violência ou grave ameaça, e com o intuito de obter para si ou para outrem indevida vantagem econômica, a fazer, tolerar que se faça ou deixar de fazer alguma coisa:

[46] Art. 147-A. Perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade.

o elemento do fato, enquanto o bem jurídico “se evidencia no plano axiológico, isto é, representa o peculiar ente social de tutela normativa penal.” (PRADO, 2019)

Sua compreensão está conectada com a conjuntura de determinada sociedade, tendo em vista que cada grupo social possui demandas distintas, a depender do seu contexto e, consequentemente possui também tutelas diferenciadas.(ANANIAS et al., 2017) Partindo deste ponto, SYDOW (2023) afirma que: “não há dúvida de que hoje a informática assume grande parcela e elevada importância no desenvolvimento social e há um uso bastante considerável da tecnologia no cenário mundial”. Sendo influente para uma fração social relevante, legitima-se o surgimento de um novo bem jurídico tutelado pelo Direito Penal.

Tendo em vista que outros bens não corpóreos como a honra e a relação de consumo foram transformados em bens tutelados pelo Direito Penal, pressupõem-se a absoluta possibilidade do Direito Penal tutelar dados pessoais, informações e outros bens imateriais.(SYDOW, 2023) Além disso, tais bens já estão previstos no rol de Direitos Fundamentais da Constituição Federal, acompanhando assim a ideia de BECHARA (2009) de que os bens jurídicos protegidos pelo Direito Penal são a concretização dos valores constitucionais e direitos fundamentais.

Para ROSSINI (2003) e SYDOW (2023) os três principais elementos do direto penal informático são: integridade, confidencialidade e disponibilidade de sistemas informáticos, redes e dados informáticos, os quais devem ser agrupados em só bem jurídico, denominado segurança informática.

Com isso, o Direito Penal informático, sobretudo no que tange os cibercrimes próprios, busca a (i) integridade, dos sistemas e dados produzidos pelos usuários, para que ele mantenha sua qualidade e características originais; (ii) a confidencialidade, para que o titular do dado pessoal possa manter o controle sobre o que, como e para quem será permitido o acesso sobre tais dados; e (iii) disponibilidade, tanto do acesso ao meio virtual, mas principalmente o acesso aos dados e informações ali processados, uma vez que perder a capacidade de tratar os dados pode equivaler a perda dos mesmos. (ROSSINI, 2003; VIANNA; MACHADO, 2013 SYDOW, 2023)

3.1.4 Personagens do mundo digital: *hackers x crackers*

Ultrapassado o entendimento sobre as classificações do cibercrime e o bem jurídico tutelado, é importante diferenciar e conceituar os agentes envolvidos nesse tipo de delito.

Costuma-se colocar os *hackers* como responsáveis pelas infrações informáticas, porém trata-se aqui de uma definição equivocada. Na realidade, esse personagem atua para gerar algum tipo de informação que possa servir como conhecimento ou auxílio para terceiros, alertando sobre possíveis riscos e vulnerabilidades de sistemas ou organizações virtuais.(LÓSSIO, 2022) Ainda que estes se utilizem de conhecimentos técnicos específicos para realizar ações similares ao cibercrime, o objetivo final não é uma ação criminosa, mas sim uma conduta ética. (ZANIOLO, 2021)

Por outro lado, aqueles que realizam invasões e/ou armadilhas contrariando a lei, devem ser chamados de *crackers*. São estes que atuam de forma ilícita afim de obter vantagens financeiras ou outra questão material, coleta de informações, autopromoção ou apenas pela vontade de praticar o vandalismo.(LÓSSIO, 2022)

Cabe frisar que ambos os personagens possuem atuação predominantemente virtual, atuando com sistemas em redes e bancos de dados em nuvem como alvo ou porta de entrada para as ações. Além desses, há também cibercriminosos que atuam de forma física, e aproveitam-se de situações como por exemplo, o próprio furto ou o conserto de computadores e celulares, para modificar, retirar, adicionar dados ou outros elementos nos dispositivos.

Com isso, o conceito analítico de crime que o considera como ação típica, antijurídica e culpável, pode ser utilizado para diferenciar tais personagens. O *hacker* ainda que possa realizar ações tipificadas, ou seja, elementos descritos como puníveis na lei penal, exime-se da antijuridicidade pelas circunstâncias que autorizam suas ações, fazendo com que o fato não seja algo desaprovado pelo ordenamento jurídico.(BITENCOURT, 2011) Em contrapartida, o *cracker* realiza ações tipificadas, de forma antijurídica e culpável. Há um juízo de valor pela contradição entre a conduta praticada e as normas do ordenamento jurídico, além da reprovação sobre o fato em si, diante das circunstâncias concretas em que o sujeito age.(PRADO, 2019)

3.2 A CONVENÇÃO DE BUDAPESTE E SEUS IMPACTOS NO BRASIL

Os conceitos e debates sobre os cibercrimes e seus personagens possuem forte relação com as construções da Convenção sobre o Cibercrime, mais conhecida apenas por Convenção de Budapeste. O pacto resultou num documento aprovado no âmbito do Conselho da Europa e assinado na capital húngara em novembro de 2001. Atualmente, ocupa o papel de principal normativa internacional sobre o cibercrime, tendo como objetivos: (i) harmonizar as leis relacionadas aos crimes cibernéticos; (ii) apoiar a investigação desses crimes; e (iii) aumentar a cooperação internacional na luta contra esse tipo de crime.(ARAUJO, 2022)

O documento define termos como dados informáticos[47] e dados de tráfego[48], passando depois para a caracterização de tipos penais. É importante frisar que, mesmo considerando certas ações como crimes, a Convenção dá liberdade para cada país membro adotar as medidas legislativas e jurídicas necessárias para a classificação das ações como infrações penais em seu direito interno.(DE SIMAS, 2014)

Em paralelo a convenção de Budapeste, já existiam, discussões e Projetos de Leis no Brasil com o objetivo de promover uma convergência nacional com as tipificações e definições presentes na Convenção de Budapeste, ainda que o país não compusesse a lista de signatários. São exemplos, o PL 89/2003 e o PL 84/1999, com propostas para novos tipos penais, marcados por certo pioneirismo, porém combatidos em função das “tipificações genéricas e ambivalentes que tentavam introduzir no ordenamento jurídico brasileiro”(SANTOS, 2022).

Mesmo com algumas oposições, os debates e transformações iniciados com tais projetos resultaram em algumas mudanças relacionadas ao cibercrime no Código Penal. Essas mudanças podem ser visualizadas na atual redação do Código, com dispositivos penais que se relacionam com tópicos de Direito Penal material da Convenção internacional. O quadro 4 apresenta tais conexões, porém sem entrar no mérito da redação e dos conceitos utilizados.

[47]“qualquer representação de factos, de informações ou de conceitos sob uma forma susceptível de processamento num sistema de computadores incluindo um programa apto a fazer um sistema informático executar uma função”

[48]“dados informáticos relacionados com uma comunicação efectuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação”

Dispositivo nacional	Tópico da Convenção de Budapeste relacionado
Art 154- A do CP	Art 2º – Acesso ilegítimo; Art 4º Interferência de dados
Art 154-A § 1	Art 6º - Uso abusivo de dispositivo
Art 154- A § 4 do CP	Art 3º - Interceptação ilegítima
Art 171 § 2º do CP	Art 7º - Falsidade informática
Art 184 do CP	Art 10º Infrações relacionadas com a violação do direito de autor e dos direitos conexos
Art 241 ao 241-E do ECA	Cap II, Secção 1, Título III – Infrações relacionadas com o conteúdo

Quadro 4: Comparativo Código Penal e Convenção de Budapeste

Além do que foi exposto, as normas nacionais apresentam previsões para contemplar outras formas de responsabilidade, como a tentativa, a cumplicidade e a coautoria dessas infrações.

Ademais, a Convenção não só influenciou na construção legislativa local, mas também trouxe grande evidência para a importância da cooperação internacional. Sem este trabalho coletivo não há como atuar contra o cibercrime de forma efetiva, dado que ele habita o ciberespaço, um local em que não existem fronteiras e as pessoas podem interagir sem presença física.(DE SIMAS, 2014).

Embora assinada em território europeu, a Convenção conta com países de outros continentes em sua lista de signatários. Na América do Sul, o Chile aderiu ao documento em 2017, seguido da Argentina em 2018. Ambos antes do Brasil, que se juntou ao grupo somente em 2021 por meio do Decreto Legislativo nº 37/2021.(SANTOS, 2022)

Com a aderência federativa e a devida aprovação do Congresso Nacional, o Brasil internalizou a Convenção, de fato, em abril de 2023 por meio do decreto nº 11.491/2023. Desde então além de contar com a rede de signatários para investigações e capacitações, o Estado brasileiro deve adotar medidas legislativas e outras providências compatíveis a norma internacional.(GARCIA, 2023)

Uma possível justificativa para a adesão brasileira 20 anos após a assinatura do documento é a fragilidade da disposição estrutural e legislativa atual do país, principalmente quando há o envolvimento de dados pessoais. Para que a atuação do Brasil seja mais efetiva, faz-se necessário o fortalecimento de um arcabouço jurídico nacional direcionado à harmonização de um sistema de proteção de dados

com salvaguardas e limites para a atuação estatal.(EILBERG et al., 2021) Além de garantir uma segurança maior em relação aos cibercriminosos, cabe ao Estado também estabelecer balizas concretas sobre a utilização de dados pessoais por parte de órgãos policiais, investigativos e judiciais.

A LGPD nada fala sobre sanções penais, tampouco sobre o tratamento de dados no âmbito da segurança pública e de atividades de persecução e repressão de infrações penais. Da mesma forma a jurisprudência ainda não é concisa sobre os limites dos poderes de vigilância e acesso do Estado aos dados pessoais.(FERNANDES; MEGGIOLARO; PRATES, 2022)

Infelizmente não se percebe grandes avanços no meio legislativo sobre o anteprojeto de “LGPD Penal”, que é a proposta de texto que aborda sobre: direitos e garantias dos cidadãos, a definição de autoridades competentes, e os limites para o momento e o formato da atuação estatal.(FERNANDES; MEGGIOLARO; PRATES, 2022) O que se observa atualmente é uma lacuna na proteção dos cidadãos, não só em questões legislativas, mas também em questões estruturais para investigação e repressão.

Tendo em vista esse contexto, é preciso que se faça uma análise sobre a ocorrência dos cibercrimes no Brasil, suas consequências e medidas coercitivas, mantendo o foco naqueles que envolvem dados pessoais.

3.3 O CIBERCRIME APLICADO NO CENÁRIO BRASILEIRO

Em 2020, a *Akamai Technologies*[49] reportou mais de 3 bilhões de tentativas de roubos de credenciais[50] no Brasil, com um recorde diário de 55 milhões de tentativas. No ano seguinte, o país ocupou o 5º lugar na lista de países que mais sofreram com crimes cibernéticos segundo a consultoria alemã Roland Berger[51]. Na mesma tendência, a Kaspersky, empresa russa de cibersegurança, classificou o Brasil como o país mais envolvido em cibercrimes realizados por meio do *WhatsApp*[52].

[49]Empresa americana no ramo de computação em nuvem, segurança e entrega de conteúdo.
[50] Informações ou dados utilizados como meio de acessar sistemas, dispositivos ou banco de dados.
[51] Empresa alemã, de atuação global, voltada para consultoria de gestão, incluindo estratégia de negócios, transformação digital, fusões e aquisições, gestão de talentos, marketing e vendas, operações, finanças corporativas e sustentabilidade.
[52] https://securelist.lat/spam-phishing-scam-report-2022/97582/

A presença brasileira no topo dessas pesquisas e relatórios cresce consideravelmente e a tendência não aponta para notícias melhores. Especialistas da área da segurança cibernética consideram que esses ataques estão entre as principais ameaças voltadas a empresas e pessoas, sobretudo quando se analisa a sofisticação e a atualização dos vários tipos de armadilhas, como *phishing, deepfake*[53]*, ransomware.*(BARBOSA, 2022) Além desses, não são raros os casos de repercussões midiáticas sobre o acesso e compartilhamento ilegal de dados pessoais através de dispositivo como computadores e celulares.

Seguindo a lista divulgada em 2022 pela revista Forbes[54] com as principais ameaças no ciberespaço brasileiro, inicia-se uma análise sobre os tipos de cibercrimes relacionados aos dados pessoais e com maiores níveis de repercussão na mídia; os casos de *phishing* e os de *ransomware*. Além disso, abordar-se-á os casos em que dispositivos como computadores e celulares particulares foram invadidos ou acessados de forma irregular, gerando impacto midiático, investigativo e legislativo.

3.3.1 Phishing na prática

A palavra *phising* deriva do verbo em inglês “*to fish*” e denota justamente a ideia de usar uma isca para obter alguma recompensa. No mundo digital essa prática costuma ser encontrada em e-mails, sites e redes sociais onde os *crackers* criam armadilhas para enganar a vítima e acessar diferentes tipos de informações.(SHANKAR; SHETTY; NATH K, 2019)

Geralmente, tal prática se relaciona com o crime de fraude eletrônica previsto no Art 171 § 2º-A do CP tendo em vista que o cibercriminoso utiliza de meios fraudulentos para obter dados pessoais, credenciais de acesso, recursos financeiros entre outros tipos de dados. Para isso, o *cracker* cria e-mails ou páginas da internet falsas, porém com aspecto visual muito próximo da versão verdadeira, inserindo *links* ou formulários que induzem a vítima ao erro. (DE SIMAS, 2014)

Nesses casos, ao clicar nos falsos links a vítima pode estar autorizando um *download* com arquivos maliciosos em seu dispositivo ou então ser direcionada para

[53] Deepfake usa inteligência artificial para trocar o rosto de pessoas em vídeos, sincronizar movimentos labiais, expressões e demais detalhes para imitar imagem e voz de pessoas reais
[54] https://forbes.com.br/forbes-tech/2022/02/os-principais-ataques-ciberneticos-previstos-para-2022/

uma falsa página de pagamento. Os formulários enganosos também são meios para a captura de dados pessoais ou dados de credenciais de acesso, atingindo assim a confidencialidade do bem jurídico informático.

Quando a ação é direcionada para uma pessoa física, o foco tende a ser a obtenção de (i) recursos financeiros ou (ii) credenciais de acesso, sobretudo contas bancárias. Exemplificando o primeiro caso, encontramos os crimes envolvendo o sistema PIX[55] e o comércio *online* em sites ou redes sociais.[56]Ainda que a ação criminosa costume ter como alvo o dinheiro, um bem patrimonial, o criminoso tende a ter acesso aos dados pessoais como as chaves PIX (CPF, número de telefone, e-mail) além de dados de pagamento (dados de cartão ou conta bancária).

No segundo exemplo, o infrator busca diretamente dados pessoais para acessar uma conta, e posteriormente obter algum tipo de vantagem. Na prática, além dos delitos envolvendo o setor bancário[57], visualiza-se as ações em redes sociais onde o usuário original perde o acesso da sua conta enquanto o cibercriminoso utiliza-a para outra finalidade.

O *phishing* acaba alcançando uma larga escala quando é direcionado para pessoas jurídicas por meio dos seus funcionários. O acesso de algum colaborador a conteúdo fraudulento pode comprometer a base de dados e sistemas da organização privada, permitindo o *cracker* acessar informações confidenciais. Como consequência, esses acessos ilegais afetam a confidencialidade e, às vezes, a integridade de dados pessoais de diversos cidadãos.

3.3.2 Ransomware na prática

Ransomware é um *software* malicioso que atinge dispositivos e exige um pagamento para o reestabelecimento do sistema ou acesso aos dados envolvidos.

---

[55] https://g1.globo.com/economia/noticia/2023/02/09/novo-golpe-do-pix-tem-invasao-fake-de-conta-bancaria-acesso-a-dados-sigilosos-e-ate-musica-de-banco-veja-relato-de-vitima.ghtml

[56] COMPRA POR MEIO DE SITE FRAUDULENTO – PAGAMENTO DE BOLETO FRAUDULENTO – CULPA EXCLUSIVA DO CONSUMIDOR – AFASTAMENTO DA RESPONSABILIDADE DO FORNECEDOR DO PRODUTO - SENTENÇA MANTIDA. (TJSP; Recurso Inominado Cível 1003809-46.2020.8.26.0271; Relator (a): Patricia de Assis Ferreira Braguini; Órgão Julgador: 2ª Turma Cível, Criminal e Fazenda - Itapecerica da Serra; Foro de Itapevi - Juizado Especial Cível e Criminal; Data do Julgamento: 05/04/2021;

[57] Dados da Federação Brasileira de Bancos (Febraban) mostram que o Brasil registrou um aumento de 80% nas tentativas de ataques de phishing com intuito de roubo financeiro em 2021. Disponível em: https://valor.globo.com/patrocinado/mercado-bitcoin/noticia/2022/07/07/brasil-registra-aumento-de-80percent-nas-tentativas-de-ataques-de-phishing.ghtml acesso em 20/04/2023

De certa forma há um “sequestro” do sistema e/ou das informações nele inseridas.(ZANIOLO, 2021) A contrapartida financeira costuma ser cobrada via criptomoedas[58], com o intuito de dificultar o rastreamento desse pagamento e a identificação do *cracker* envolvido.(VOLPI; VOLPI, 2021)

Essa prática vem gerando um mercado bastante lucrativo, com certa facilidade para o criminoso pois ele não precisa se movimentar ou correr o risco para negociar com terceiros. Nesse cenário as vendas são diretamente para os próprios titulares dos sistemas ou dados, que se sentem obrigados a pagar a exigência para que não ocorra a perda definitiva dos elementos envolvidos.(FORNASIER; SPINATO; RIBEIRO, 2020)

Ainda que o *cracker* possa ameaçar a divulgação das informações, os principais elementos atingido aqui são a disponibilidade e a integridade do bem jurídico. Os impactos dessas ações vão além da posse de dados e outros tipos de arquivos, alcançando também sistemas vitais como por exemplos os sistemas hospitalares. Com isso, além de comprometer exames, prontuários e demais documentos relacionados aos pacientes o ataque pode afetar equipamentos médicos importantes que operam com uso da internet.

Na atual disposição do Código Penal não há um dispositivo que cumpra de forma integral com o princípio da legalidade para englobar a prática do *ransomware* como tipo penal. Não há motivos para a aplicação do crime de sequestro e cárcere privado (Art 148 do CP) tendo em vista sua definição de crime contra a liberdade pessoal e a ideia de ser um delito relacionado a liberdade de movimento, o direito de ir e vir.(PRADO, 2019)

Ainda que a ação remeta a ideia da extorsão (Art 158 do CP) não se encaixa integralmente no contexto do *ransomware* pois nesses casos o *cracker* já está com a posse e alguma vantagem indevida em relação ao sujeito. Mesmo que ainda não seja uma vantagem patrimonial, já há um acesso ilegal de dados, informações e sistemas.(ESTEFAM, 2022)

3.3.3 Acesso não autorizado em dispositivos e sistemas informáticos

[58] “Moedas virtuais, de circulação na internet e operada via tecnologia chamada *blockchain.”*(RODRIGUES AFONSO; RIOS DA NÓBREGA; NETTE ALVES OLIVEIRA DE CASTILHOS, 2022)

Diferentemente dos casos relatados anteriormente, em que as ações eram realizadas no meio virtual, existem também as ações realizadas no meio físico, em contato direto com o dispositivo eletrônico. Na prática, trata-se de uma ação realizada por um sujeito ativo comum, sem exigência de grandes conhecimentos informáticos no nível de um *hacker* ou *cracker.*

De forma concreta, podemos visualizar dois cenários principais: (i) conserto técnico de dispositivos, e (ii) relacionamento amoroso.

No primeiro exemplo, a vítima deixa seu dispositivo informático com um profissional, e na ausência do proprietário, o responsável pelo conserto acessa e visualiza informações desnecessárias para o trabalho e/ou não autorizadas pelo titular. Neste exemplo, não há de fato uma invasão ao dispositivo, uma vez que o profissional está autorizado para o serviço, mas há um acesso não autorizado a informações, que por sua vez, contraria os princípios da finalidade[59] e da necessidade[60]. Além de ferir a confidencialidade, tal acesso pode ainda comprometer a integridade das informações e do próprio dispositivo.(DEMARTINI, 2022)

No segundo caso, como visto na jurisprudência[61], o sujeito ativo acessa o dispositivo alheio ou instala algum componente para monitorar arquivos, trocas de mensagens e senhas do seu parceiro. Mesmo o início da ação sendo relacionado ao dispositivo e o acesso das informações, abre-se a possibilidade para a incidência de outros delitos como extorsão (Art 158 do CP) e constrangimento ilegal (Art 146 do CP). De forma similar ao tópico anterior, não há um artigo no Código Penal que atenda todos os elementos de ponta a ponta da ação para que seja definido como crime efetivamente.

---

[59] realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

[60] limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

[61] “III - Pratica a conduta tipificada no art. 154-A, § 3º, do CP aquele que, sem o conhecimento de sua então namorada, instala programa espião no notebook dela, com o fim de monitorar as conversas e atividades e, diante dessa vulnerabilidade, consegue violar os dispositivos de segurança e, com isso, ter acesso ao conteúdo das comunicações eletrônicas privadas e outras informações pessoais, inclusive diversas senhas.” (TJ-DF 20160110635069 DF 0009088-86.2016.8.07.0016, Relator: NILSONI DE FREITAS CUSTODIO, Data de Julgamento: 19/09/2019, 3ª TURMA CRIMINAL, Data de Publicação: Publicado no DJE : 24/09/2019 . Pág.: 88/89)

3.4 CASOS EMBLEMÁTICOS NO CENÁRIO BRASILEIRO

O território cibernético brasileiro é marcado por grandes e constantes violações. Tais ações ainda que sejam direcionados contra empresas privadas e órgãos governamentais, atingem a privacidade e a segurança jurídica individual de muitos cidadãos.

Nesta linha, abordar-se-á brevemente sobre alguns casos de ataques virtuais com impacto relevante no Brasil.

- **Ministério da Saúde**

Em plena pandemia da Covid-19, o site do Ministério da Saúde (www.saude.gov.br/) foi atacado por *crackers* que tiraram do ar não só o site principal, mas também outros endereços eletrônicos relacionados e aplicativos para celular. O Lapsus$ Group[62] assumiu a autoria do ataque que comprometeu 50 terabytes de informações e deixou a população sem acesso a dados de saúde por mais de dez dias.(“Ataque hacker tira do ar site do Ministério da Saúde e o ConecteSUS”, 2020)

O portal sofreu um *ransomware* que atingiu a disponibilidade e a integridade do site em si e dos dados pessoais envolvidos, sobretudo os dados pessoais sensíveis relacionados à saúde. Sabe-se que os sujeitos ativos realizaram a cobrança de um valor financeiro pela liberação do sistema, mas não há informações concretas sobre como se deu o reestabelecimento do mesmo.(TORTELLA, 2021)

- **Hospital Universitário da USP**

Também em uma ação de *ransomware,* o site e alguns sistemas internos do Hospital Universitário da USP ficaram fora do ar em março de 2023. A ação impactou a operação do hospital que precisou reagendar exames, consultas, e até realizar ações de forma manual em papel[63].

---

[62] Grupo conhecido por ataques cibernéticos a grandes empresas de tecnologia.

[63] Disponível em: https://g1.globo.com/sp/sao-paulo/noticia/2023/03/30/hospital-universitario-da-usp-sofre-ataque-de-hackers-e-deixa-de-atender-ao-menos-700-pacientes-em-uma-semana.ghtml acessado em: 21/04/2023.

Tendo em vista a impossibilidade de acessar prontuários, exames e outros documentos médicos, reforça-se a ideia de que não poder tratar os dados pessoais pode equivaler a perda deles.(VIANNA; MACHADO, 2013) No caso concreto, constata-se um impacto direto na integridade e na disponibilidade dos bens jurídicos, com alta probabilidade de comprometimento da confidencialidade também.

- **Vazamento da Netshoes**

Diferentemente dos exemplos anteriores onde o envolvimento de dados pessoais sensíveis chama a atenção, o caso da Netshoes, empresa de comércio eletrônico voltada para o nicho esportivo, caracteriza-se pela grande base de clientes envolvidos e pelo acordo com o Ministério Público.

Vazamentos de dados das operações da empresa no Brasil ocorreram entre 2017 e 2018, comprometendo dados pessoais como nome, CPF, e-mail, data de nascimento e histórico de compras de aproximadamente 2 milhões de contas. Os fatos ocorreram antes da LGPD entrar em vigor, mas teve o envolvimento do Ministério Público do Distrito Federal que assinou um termo de ajustamento de conduta com a empresa.[64]

A Netshoes se comprometeu a pagar R$ 500 mil de indenização, a título de danos morais, em depósitos para o Fundo de Defesa de Direitos Difusos (FDD) vinculado ao Ministério da Justiça, além de diversas medidas internas para aprimoramento da segurança informática.[65]

No caso em tela, nota-se que as sanções tendem a ser direcionadas para a pessoa com a posse dos dados e sua responsabilidade de cuidado. Por outro lado, as correções penais voltadas aos criminosos de fato ainda são frágeis e de aplicação prática complexa. Dentre as causas dessa lacuna penal estão os aspectos legislativos, tendo em vista a construção dos tipos penais marcadas por imediatismo, incompreensão e insuficiência técnica.(SYDOW, 2023)

Os exemplos descritos anteriormente demonstram um o uso desenfreado do Direito Penal com a esperança de que este atenda todos os anseios sociais de forma autônoma e exclusiva. Por consequência, o Direito Penal Informático se

[64] Disponível em: https://www.tecmundo.com.br/seguranca/129428-vazamento-netshoes-continua-totaliza-dados-2-5-milhoes-clientes.htm. Acessado em: 21/04/2023.
[65] Disponível em: https://g1.globo.com/df/distrito-federal/noticia/2019/02/05/netshoes-tera-de-pagar-r-500-mil-por-vazamento-de-dados-de-2-milhoes-de-clientes.ghtml. Acessado em: 21/04/2023

arquiteta repleto de Leis penais em branco; normas imperfeitas, com conteúdo incompleto, vago, impreciso e que dependem de complementação jurídica.(BITENCOURT, 2011)

Nesta linha, parte-se para análise do cibercrime em espécie com foco nas ações envolvendo dados pessoais, nas propostas do PL 879 de 2022 e nas possíveis ações sistêmicas para a prevenção de cibercrimes.

4 PROJETO DE LEI 879/2022: HISTÓRICO, SITUAÇÃO E FUTURO

Em processo de tramitação, o Projeto de Lei 879 de 2022, de autoria do Senador Carlos Viana (PL/MG) almeja modificar o Código Penal alterando e criando dispositivos legais relacionados ao cibercrime. Em suas justificativas, o político reforça a ideia de que os novos paradigmas comportamentais da sociedade geram a necessidade de um legislativo mais atento para reprimir e combater os crimes cometidos em ambiente digital.(BRASIL, 2022)

As inovações constitucionais com a inclusão da proteção de dados pessoais como direito fundamental e os ataques realizados contra entidades privadas e órgãos governamentais também são fundamentos para as alterações penais proposta. Na mesma linha, o compromisso do Estado brasileiro em relação à Convenção de Budapeste tem movimentado o meio jurídico e legislativo para um maior alinhamento com a norma internacional.

Para uma análise mais aprofundada do texto atual e suas implicações práticas, faz-se necessário uma compreensão inicial sobre o histórico legislativo brasileiro relacionado ao tema proposto pelo projeto, para que as novas propostas no PL possam ser analisadas com maior eficiência posteriormente.

4.1 A CONSTRUÇÃO LEGISLATIVA RELACIONADA AO PL 879/2022

Embora um dos pontos focais do PL seja a inclusão de um novo tipo penal (sequestro de dados informáticos), há também a proposta de alteração do Art 154-A, já presente no Código Penal. Considerando que tal dispositivo foi incluído no CP por meio da Lei nº 12.737/2012, e posteriormente modificado pela Lei nº 14.155/2021, é importante compreender o contexto em que se deu está construção e analisar suas modificações.

4.1.1 A Lei nº 12.737 de 2012 e suas propostas

Originária do Projeto de Lei nº 2793/2011, apresentado em 29 de novembro de 2011, pelo Deputado Paulo Teixeira (PT-SP), tramitou no Congresso Nacional em regime de urgência e atingiu o status de Lei nº 12.737/2012 no tempo recorde de aproximadamente um ano. Apelidada de “Lei Carolina Dieckmann”, já ganhava notoriedade antes mesmo de publicada e sancionada, tendo em vista sua forte relação com o episódio envolvendo a atriz que teve fotos intimas divulgadas na internet.(DE ARAÚJO, 2019)

A situação de Dieckmann mobilizou a imprensa nacional que por sua vez pressionou o legislativo para que fossem criados mecanismos de defesa mais eficientes no meio digital.(SOUZA, 2021) A mesma mídia veiculava notícias[66] conectando o fato com os crimes de difamação, furto e extorsão, todavia observava-se, na época, uma certa afronta ao princípio da legalidade, visto que o contexto fático possuía divergências em relação aos tipos penais relacionados.

Toda essa situação de urgência, pressão e imprecisão, resultou em uma Lei considerada pela doutrina como açodada, enxuta, imprecisa, ambígua, e tecnicamente defasada.(SOUZA, 2021)

Ainda que anuncie tratar sobre a tipificação penal de delitos informáticos, no plural, o que se visualiza na prática é a criação de apenas um novo delito e o alargamento da incidência de outros tipos como a interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública, e a falsificação de documento particular. No caso, os artigos 266[67] e 298[68] passaram por uma atualização para que estes não ferissem o princípio da legalidade.(SYDOW, 2023)

Ultrapassado o contexto e justificativas da sua promulgação, parte-se para a análise do Art 154-A, tipo penal inaugurado integralmente pela Lei em questão.

---

[66] Disponível em https://g1.globo.com/fantastico/noticia/2012/05/policia-encontra-hackers-que-roubaram-fotos-de-carolina-dieckmann.html acessado em 05/05/2023

[67] § 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento. § 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública.” (NR)

[68] Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito.” (NR)

> 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:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.”

Em relação ao tipo penal, BITENCOURT (2020) o considerava como semiaberto, ou seja, nem aberto nem fechado. Se por um lado o trecho “mediante violação indevida” abria a locução, sua complementação “de mecanismo de segurança” fechava e limitava a atuação penal. Com isso, pelo princípio da legalidade, dispositivos que não tivessem mecanismo de segurança, ou se ele tivesse desligado, ou ainda, quando o sujeito ativo conhecesse e utilizasse a senha, não seria possível aplicar o Art 154-A do CP. De forma comparativa, seria equivalente exigir que a porta de uma residência esteja chaveada ou que o alarme do veículo esteja funcionado para a aplicação do crime de furto (Art 155 CP).(SYDOW, 2023)

Ainda sobre a invasão, nota-se uma certa contradição ao utilizar o tipo penal “invadir” atrelado com a autorização ou não do titular do dispositivo. O núcleo do tipo penal, utilizado com o sentido de violar, acessar, ingressar de forma arbitrária ou hostil, sem o consentimento de quem é de direito, por si só não ocorreria se existisse uma autorização. Afinal, o que justificaria alguem invadir um dispositivo que possui autorização? Em outras palavras, invasão já implica em uma ação realizada sem a autorização do titular. (BITENCOURT, 2020; SYDOW, 2023)

Acrescenta-se ao debate a subjetividade da autorização expressa ou tácita, seu formato e sua validade temporal. Como definir uma correta autorização? Uma autorização realizada hoje, mesmo sem efeito de revogação, terá validade permanente? Pode o titular de direito autorizar de forma parcial ou apenas integralmente no formato “tudo ou nada”? São alguns dos questionamentos gerados pela imprecisão de uma lei com traços marcantes de normal penal em branco.(BITENCOURT, 2011; SYDOW, 2023)

Ressalta-se que uma vez concedido o acesso, não seria possível atender o tipo objetivo, tendo em vista que uma plausível revogação da autorização não surtiria efeito penal algum.(CUNHA, 2017) O artigo pune apenas a conduta de invadir o dispositivo sem autorização, mas não contempla os atos cometidos após um cancelamento da autorização. O cibercrime em foco não habilita o mecanismo da revogação tal qual se constata no crime de violação de domicílio (Art 150 do CP), que pune a entrada ou a permanência não autorizada, ou a importunação sexual (Art 215-A do CP) que pode retratar uma relação inicialmente consentida que se transforma em ato sem anuência.(ESTEFAM, 2022)

A doutrina também contrariava a utilização do conceito “titular do dispositivo”, uma vez que tal personagem poderia ou não ser o real detentor das informações ali armazenadas. O termo escolhido inicialmente pelo legislador mostrava-se ser algo cinzento e perigoso, pensando no contexto de uso compartilhado de dispositivo no círculo familiar, empréstimo de equipamentos e modelo de trabalho remoto no mundo corporativo.(SYDOW, 2023)

Além do verbo “invadir”, o texto também requer que a finalidade do agente seja a de obter (alcançar, adquirir), adulterar (alterar, modificar) ou destruir (inutilizar, extinguir) dados ou informações.(PRADO, 2019) Tal redação limita a abrangência do tipo penal, uma vez que pelo princípio da legalidade e pela impossibilidade do entendimento *in malam partem*, são enquadradas no Art 154-A somente aquelas invasões em que se comprove algum dos tipos subjetivos do dispositivo.(GRECO, 2019)

Mesmo que se note apenas um núcleo (“invadir”), a utilização intensa da conjunção “ou” e a disposição deste instrumento gramatical ao longo da redação, sustentam a rotulação do crime como tipo misto cumulativo. Dessa maneira, o delito seria consumado com a mera invasão do dispositivo informático com alguma das finalidades já listadas, ou com a instalação de vulnerabilidades, uma vez que

decorrem de ações distintas que podem ser realizadas separadamente.(PRADO, 2019)

Como argumenta PRADO (2019): “É possível invadir um dispositivo e realizar algo sem instalar nenhuma vulnerabilidade. De outro lado, a instalação de vulnerabilidade depende da ação de invadir.”. Assim, aquele que invadisse o dispositivo e instalasse vulnerabilidades responderia pelos dois crimes em concurso material, previsto no Art 69 do CP.

Finalizando a análise sobre o *caput*, cabe ressaltar que a ausência de uma definição concreta sobre “dispositivo informático”, abre margem para dois entendimentos distintos: (i) mais restrito, que contempla apenas o *hardware* que trata informações, excluindo assim o conceito de sistemas totalmente on-line, ou (ii) mais amplo, como sustentando por ESTEFAM (2022) que considera tanto o *hardware* como o *software*, argumentando que o conceito trata de “mecanismo físico ou virtual capaz de reunir informações ou dados digitalizados em ambiente eletrônico, por meio da linguagem característica dos computadores e mecanismos equivalentes”.(SYDOW, 2023)

Olhando para a Convenção da Budapeste, que separa “sistema” e “dispositivo” nos Art 4º e 5º respectivamente, e considerando mais uma vez a impossibilidade da analogia *in malam partem*, a ideia de que o artigo penal apenas protege as ações contra elementos físicos demonstra ser a mais coerente. Além disso, caso o objetivo fosse apenas de danificar o dispositivo, sem intenção de atingir os dados e informações ali armazenados, seria possível considerar o crime de dano (Art 163 do CP) voltado para coisas alheias de perfil patrimonial.(PACHECO; COSTA, 2018)

Seguindo para o primeiro parágrafo do Art 154-A, contempla-se a figura equiparada punindo também aquele que oferece (mostrar, dar), distribui (repartir ou entregar a diversas pessoas), vende (negociar, alienar, trocar por dinheiro ou outro valor, comercializar); ou difunde (propagar ou expor) dispositivo ou programa de computador com o objetivo de permitir a ação prevista no caput. Na redação original, a pena base era de detenção, de 3 (três) meses a 1 (um) ano, e multa.(BITENCOURT, 2020)

Com isso, o legislador estabelece um crime vinculado que busca também punir os intermediários da ação. Trata-se de um crime de ação múltipla ou de

conteúdo variado, pois ainda que o agente perpetre mais de uma ação prevista no texto, tem-se apenas um único delito.(BITENCOURT, 2020; PRADO, 2019)

Novamente, há um critério subjetivo que avalia a finalidade da ação. Amparado pela Convenção de Budapeste[69], SYDOW (2023) alerta, que aqueles que não demonstrem o caráter prejudicial da conduta, não devem ser responsabilizados, considerando que o erro de tipo exclui o dolo.

Em sua primeira majorante (§ 2º), a Lei apresenta, de forma reiterada, uma escrita genérica e abstrata. Por um lado, BITENCOURT (2020) entende e concorda com a limitação da lesão, uma que vez que só se majora a pena quando há "prejuízo econômico", afastando assim questões morais, íntimas e afetivas. Todavia, SYDOW (2023) considera que a valoração econômica neste contexto é algo "demasiadamente genérico", considerando que dados e informações possuem um valor diferente a depender do seu contexto e utilidade.

Tal delimitação imposta pelo legislador desperta atenção pois o vazamento de fotos íntimas de uma atriz foi fator preponderante para a criação do dispositivo. Todavia, no caso concreto, a principal lesão não era patrimonial, mas sim algo íntimo e moral, que acabou ficando de fora da majorante.

O legislador aplicou também uma qualificadora (§ 3º) duplicando as penas mínima e máxima para as invasões de dispositivos que resultarem na obtenção de "conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido.". Ainda que se desenhe uma limitação nos dados e informações envolvidos, há novamente elementos de uma norma penal em branco, com regras imperfeitas, que necessitam do apoio legal oriundo de outras fontes do Direito. Assim, para seu entendimento completo, o parágrafo quarto recorre a outras leis como Lei 12.527 de 2011[70] e Lei 9.279 de 1996[71].(GRECO, 2019)

---

[69] "Este Artigo não deve ser interpretado para estabelecer responsabilidade criminal quando a produção, venda, aquisição para uso, importação, distribuição ou disponibilização por qualquer meio ou a posse referida no parágrafo 1 deste Artigo não se destine à prática de qualquer dos crimes tipificados de acordo com os artigos 2 a 5 desta Convenção, como para, por exemplo, a realização de testes autorizados ou a proteção de um sistema de computador."

[70] Lei de Acesso à Informação: Art 4º, III - informação sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado;

[71] Código da Propriedade Industrial: Regula direitos e obrigações relativos à propriedade industrial.

De modo geral, a ausência de menções mais diretas a “dados pessoais” pode ser explicada pela diferença temporal entre a construção da Lei Carolina Dieckmann e os debates sobre proteção de dados pessoais. Todavia, compreende-se a ideia de que é indiferente a relevância da informação violada, pois a importância está na violação em si e não em seu conteúdo. No mais, as fotos da atriz, que no contexto fático foram violadas por meio de “comunicações eletrônicas privadas”, não estariam aptas à qualificadora do § 3º se fossem violadas de um dispositivo com finalidade única de armazenamento, mas não de comunicação.(BITENCOURT, 2020)

Vinculado a este último parágrafo, o § 4º majora a “divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas”, colocando assim um delito do tipo misto como aumento específico para o delito qualificado. Ainda que se compreenda de forma relativamente simples o significado de cada elemento do tipo[72], a majorante possui subjetividade e carrega algumas indagações: (i) a transmissão a terceiro ou a divulgação precisam ser solicitadas por quem recebe as informações? (ii) a invasão e as ações elencadas no § 4º precisam ser realizadas por um mesmo sujeito para a majoração?(SYDOW, 2023)

A primeira questão relaciona-se com o erro de tipo, visto que uma pessoa pode receber uma informação que fora obtida por meio de uma violação, e divulgar a mesma sem saber que a obtenção inicial se deu por meio ilegal. Sobre o segundo tópico, aquele que comercializa as informações, ainda que não seja enquadrado no Art 154-A, poderia se tornar réu pelo crime de receptação, previsto no Art 180 do CP[73].

Por fim, na mesma tendência dos crimes conta a honra, o § 5º prevê causa de aumento especial pelo perfil do sujeito passivo. No caso, considerou-se uma maior desvalorização da ação, pela qualidade ou condição funcional da vítima, haja vista que tais personagens possuem acesso a dados de enorme valor e importância para o Estado brasileiro.(PRADO, 2019; SYDOW, 2023)

De modo geral, em relação à classificação informática, o Art 154-A pode ser considerado como puro (no *caput*) e impuro (no parágrafo primeiro). Na divisão

[72] Divulgação: Abrir para todos. Comercializar: Colocar no mercado mediante preço. Transmissão a terceiro: passar de forma individual (SYDOW, 2023)

[73] Adquirir, receber, transportar, conduzir ou ocultar, em proveito próprio ou alheio, coisa que sabe ser produto de crime, ou influir para que terceiro, de boa-fé, a adquira, receba ou oculte.

tradicional do Direito Penal, trata-se de um crime doloso comum e formal, que pode ser unissubjetivo ou de concurso eventual, porém sempre comissivo.(PRADO, 2019; SYDOW, 2023)

No que tange os elementos processuais, a Lei utiliza do Art 154-B para definir que, em regra, a ação penal será condicionada à representação da vítima, salvo se o crime for 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.”. Como foi visto anteriormente, a dúvida sobre a caracterização do “titular do dispositivo” afeta o entendimento sobre o conceito de “vítima” e a definição do direito de representação.

De qualquer forma, para o prazo de representação, prevalece o tempo de 6 (seis) meses, a contar do momento que se identifica o autor do crime. É um tempo aceitável para a representação, porém a maior dificuldade prática é a de identificar o autor do crime. No mais, tendo em vista sua pena mínima e as possibilidades de qualificadoras e majorantes, crimes como estes não deveriam ser afastados da competência dos Juizados Especiais Criminais.(BITENCOURT, 2020)

Diante do exposto, pode-se compreender melhor a redação original do dispositivo, seus pontos contraditórios e sua imprecisão prática. Reconhecendo isto, novas propostas legislativas foram trabalhadas e lapidas, resultando em ações como a promulgação da Lei nº 14.155 de 2021, a qual se propõe analisar no capítulo seguinte.

4.1.2 A Lei nº 14.155 de 2021 e suas alterações

A redação de 2012 mostrava-se inoperante em aspectos jurídicos e legislativos. Como analisado por SYDOW (2023), o Tribunal de Justiça de São Paulo registrou apenas dois casos[74] relacionados ao Art 154-A no período entre 2012 e 2020. Também na visão do autor, o tipo penal foi aplicado de forma incorreta nesses raros episódios, concedendo vantagem para os condenados que foram enquadrados em dispositivo com pena mais branda do que deveriam.

Esse número baixo de casos em um TJ relevante no país mostra que o Direito Penal informático não alcançou sua função de proteger bens essenciais ao

[74] Apelação nº 3003607-07.2013.8.26.0586 SP 3003607-07.2013.8.26.0586 e Apelação nº 0005468-51.2014.8.26.0196 SP 0005468-51.2014.8.26.0196, ambas do TJ/SP.

indivíduo e à comunidade. Por outro lado, como visto em capítulos anteriores, os casos e projeções de ameaças e violações a dados pessoais no mundo virtual aumentam de forma significante no país.(PRADO, 2019)

Buscando aprimorar a eficiência jurídica, o PL 4554/2020, de iniciativa do Senador Izalci Lucas (PSDB/DF), resultou na Lei 14.155 de 2021, também chamada de Lei do Cibercrime. Suas principais justificativas relacionam-se ao aumento dos cibercrimes no Brasil, sobretudo aqueles que impactam em fatores econômicos, gerando "perda do poder aquisitivo e perdas emocionais por parte das vítimas.".(BRASIL, 2021b)

Ainda que o texto inicial do PL contemplasse apenas alterações no Art 155 do CP (furto), sua tramitação bicameral resultou em alterações em três artigos do Código Penal. No crime de furto, foram inseridos os § 4º-B e § 4º-C[75] para qualificar os furtos cometidos mediante fraude por meio de dispositivo eletrônico ou informático, enquanto no estelionato (Art 171) foi inaugurado o crime de fraude eletrônica, por meio dos parágrafos 2-A, 2-B e 3-A[76]. Tais alterações refletem os cibercrimes impróprios tendo em vista que os artigos já existiam, e foram ajustados para refletir melhor o novo contexto social.(SYDOW, 2023)

Observando-se o cibercrime próprio, a Lei também transformou o Art 154-A, resultando em uma nova redação do seu caput:

> Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.

Embora se reconheça as modificações com intuito de expandir o alcance da modalidade fundamental e elevar o rigor punitivo, a nova composição não se

[75] § 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é 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. § 4º-C. A pena prevista no § 4º-B deste artigo, considerada a relevância do resultado gravoso: I – aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional; II – aumenta-se de 1/3 (um terço) ao dobro, se o crime é praticado contra idoso ou vulnerável.

[76] § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.§ 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional. § 3º - A pena aumenta-se de um terço, se o crime é cometido em detrimento de entidade de direito público ou de instituto de economia popular, assistência social ou beneficência.

esquivou de críticas doutrinárias e imprecisões práticas.(ESTEFAM, 2022) De imediato, percebe-se a manutenção do núcleo “invadir”, cultivando as críticas anteriores sobre a incompatibilidade do verbo com o elemento da autorização e a inaplicabilidade da revogação.

SYDOW (2023) considera que o Brasil diverge da prática internacional ao não utilizar o tipo “intrusão” com o significado de estar em uma situação de desacordo e não autorização, optando por considerar como crime apenas o ingresso ilegal no dispositivo. Com isso, a permanência desautorizada no equipamento informático segue sendo fato atípico.

Por outro lado, a nova versão do artigo tornou este mais aberto em razão de não existir mais a necessidade da violação de mecanismo de segurança. Tal exclusão é vista com bons olhos na doutrina pois não existia, e ainda não existe, uma definição concisa sobre “mecanismo de segurança”. Além do que, como foi demonstrado no tópico anterior, a ausência de senhas nos dispositivos, ou o conhecimento delas pelo sujeito ativo seriam situações não enquadradas neste tipo penal.(SYDOW, 2023)

Dentre as alterações, destaca-se a troca de “dispositivo informático alheio” no texto de 2012, para “dispositivo informático de uso alheio” na redação vigente. Antes, apenas o titular do dispositivo ocupava o papel jurídico de vítima, função esta que foi expandida na nova descrição. Embora a expansão seja comemorada pela doutrina, nota-se agora novos debates por duas razões principais: (i) o uso compartilhado dos dispositivos; (ii) a diferença entre ser o usuário de um dispositivo e o titular dos dados e informações vinculados.(SYDOW, 2023)

No primeiro ponto, ao considerar o ambiente familiar e corporativo, é comum que um mesmo dispositivo seja utilizado por pessoas diferentes. Cada uma delas pode acessar sistemas distintos com contas individuais e armazenar tipos variados de informações. Nesses casos, quem, de fato, pode conceder a autorização de acesso? A autorização realizada por um dos usuários interfere nos sistemas e informações utilizados por um outro usuário? São respostas que, na prática, ficam a critério da interpretação do juiz em cada caso concreto.(SYDOW, 2023)

O segundo fator também é observado no contexto familiar e empresarial, sendo igualmente abstrato. Com a nova redação, não está claro se aquele que almeja obter, adulterar ou destruir dados ou informações, por meio de um dispositivo que já utiliza, será ou não enquadrado no Art 154-A do CP. Se considerarmos o *in*

dubio, pro reo, o exemplo tende a ser fato atípico, mas neste pensamento, o titular dos dados e informações fica penalmente desprotegido.(SYDOW, 2023)

Continuando com a comparação, a proposta original do artigo permitia a interpretação de incidência do concurso material entre os verbos 'invadir' e 'instalar vulnerabilidades', devido à forma como estes foram posicionados ao longo do texto.(PRADO, 2019) No entanto, a partir de 2021, com um simples acréscimo da preposição “de”, a redação foi modificada, alterando o entendimento e incluindo a instalação de vulnerabilidades como mais uma das finalidades possíveis para a tipificação do crime. Tal desígnio passa a integrar os elementos subjetivos específicos do artigo junto de obter, adulterar e destruir dados ou informações.(ESTEFAM, 2022)

Por outro lado, a manutenção da redação com “vulnerabilidades”, no plural, restringe a aplicação do crime. Além de comprovar a finalidade, faz-se necessário também demonstrar a multiplicidade de vulnerabilidades como forma de atender ao princípio da legalidade. (BITENCOURT, 2011; SYDOW, 2023)

Em relação a pena, passou a vigorar, no *caput*, a reclusão, de 1 (um) a 4 (quatro) anos, e multa. Com isso, os delitos cometidos a partir 28 de maio de 2021 deixaram de ser considerados como infração de menor potencial ofensivo, não podendo mais se valer de medida despenalizadora da transação penal, prevista na Lei n. 9.099/95. Por outro lado, ainda pode-se aplicar o acordo de não persecução penal, com fundamento no art. 28-A do Código de Processo Penal[77].(ESTEFAM, 2022)

Os demais parágrafos com majorantes e qualificadoras do delito não tiveram qualquer alteração em sua descrição, e por isso, todos aqueles impasses abordados anteriormente seguem desde 2012. Permanecem as (i) imprecisões sobre a aplicação e a eficiência da “autorização”, (ii) indefinições sobre o conceito de “dispositivo informático”, e (iii) lacunas sobre a valoração do prejuízo econômico. Assim sendo, o tipo penal continua dependendo da comprovação de finalidades específicas do agente, ao passo que o § 2º e o § 3º possuem uma compreensão embaraçada.

[77] Art. 28-A. Não sendo caso de arquivamento e tendo o investigado confessado formal e circunstancialmente a prática de infração penal sem violência ou grave ameaça e com pena mínima inferior a 4 (quatro) anos, o Ministério Público poderá propor acordo de não persecução penal, desde que necessário e suficiente para reprovação e prevenção do crime, mediante as seguintes condições ajustadas cumulativa e alternativamente

Na mesma tendência do *caput*, houve um agravamento da pena em relação ao § 2º e o § 3º. Enquanto a majorante foi elevada para 1/3 (um terço) a 2/3 (dois terços) se da invasão resultar prejuízo econômico, a qualificadora passou a adotar a pena de reclusão, de 2 (dois) a 5 (cinco) anos, e multa.

Com essa situação, percebe-se que o legislador priorizou a dosimetria e o aspecto penalizador do direito, deixando de lado as necessárias correções na descrição do tipo penal. Sobre isso, SYDOW (2023) alerta para a possibilidade de ter-se iniciado um relevante problema social, pois enquanto a compreensão da lei segue turbulenta, as medidas coercitivas se tornaram mais rigorosas e ferem o princípio da proporcionalidade.(PRADO, 2019)

Na disposição atual, a pena máxima no caso concreto pode chegar a 8 anos e 4 meses, considerando as qualificadoras e majorantes em grau máximo. Nesse cenário, além de não mais se permitir transformações em penas restritivas de direito, o início do cumprimento da pena se dará em regime fechado, em estabelecimento de segurança máxima ou média. (SYDOW, 2023)

Com todas as modificações, o dispositivo legal ainda se mostra fragilizado na garantia da tutela penal dos dados pessoais. Os incidentes cibernéticos aumentam em quantidade e complexidade, enquanto a máquina estatal ainda enfrenta dificuldades para prevenir, legislar e punir sobre o tema.(BARRETO; KUFA; SILVA, 2022)

No Brasil, nota-se construções legislativas que almejam deixar as normas mais fortes e atualizadas no combate ao cibercrime. Nessa esteira, os dados pessoais, comumente relacionados ao Direito Civil e Constitucional, começam a ganhar espaço na área penal por meio de inovações e projetos legislativos como o PL 879/2022 que será mais bem detalhado a seguir.

4.2 O PROJETO DE LEI Nº 879 DE 2022 E SUA TENTATIVA DE EVOLUÇÃO

De autoria do Senador Carlos Viana (PL/MG), o PL ainda em tramitação conta com a participação de alguns especialistas na área de cibercrime em sua elaboração. De forma repetitiva, verifica-se o objetivo de atingir uma maior segurança jurídica para as relações entre indivíduos e instituições, e, especialmente, para reprimir e combater o crime no meio digital.(BRASIL, 2022)

Ao longo das justificativas, o legislador argumenta sobre a necessidade de tipificar ações não previstas no Direito Penal, além de valorar os ataques envolvendo dados pessoais, seguindo a linha de outras ações legislativas e constitucionais. No mais, o autor também relembra sobre a Convenção de Budapeste e a adesão brasileira, que requer ajustes e aprimoramentos legais.

No texto inicial, embora proponha-se uma sutil alteração no Art 154-A do CP, o destaque é direcionado para a criação do crime de sequestro de dados informáticos, pensando em ações de *ransomware* e casos como o do Ministério da Saúde do Hospital da USP, abordados no capítulo anterior. Para melhor compreensão faz-se necessário realizar a análise da proposta.

4.2.1 Alteração no 154-A do CP

A única proposta inicial de alteração no Art 154-A impacta apenas o § 3º propondo a seguinte redação: “Se da invasão resultar a obtenção de dados pessoais, conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, ou informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido”. Nas mudanças impostas pela Lei 14.155/2021, o parágrafo em análise também já havia sido alterado, porém na época limitou-se a tratar sobre o aumento da pena.(BRASIL, 2022)

Agora, influenciado pela maior consolidação da LGPD e pelas alterações constitucionais impostas pela EC/115[78], o legislador preocupou-se em inserir “dados pessoais” na categoria de dados dignos de um caráter especial no dispositivo penal. De fato, convergindo com os direitos fundamentais, tal inclusão aumenta a proteção da privacidade individual, mas mantém expostas todas as imprecisões legislativas que foram detalhadas outrora neste trabalho.(SOUZA; ACHA, 2022)

Percebe-se também um desalinhamento da proposta com outras normativa nacionais, como LGPD e Lei do Cadastro Positivo (Lei nº12.414/2011), e internacionais como o GDPR, que classificam alguns dados e informações como “sensíveis”, observando a diferença pragmática entre a potencialidade lesiva dos considerados sensíveis e os demais dados e informações. Na prática, caso o texto

[78] Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

inicial seja oficializado, invadir um dispositivo para obter uma lista de e-mails terá o mesmo valor penal que invadir um banco de dados de um hospital com exames, prontuários e demais documentos.(KORKMAZ, 2019)

Dessa forma, os movimentos legislativos em relação ao Art 154- A seguem incompletos e ineficientes, pois ainda que as penas sejam aumentadas e os textos incrementados e atualizados, as lacunas e imprecisões se conservam por mais de dez anos.

4.2.2 Criação do sequestro de dados informáticos

A inauguração do crime de sequestro de dados informáticos é a protagonista do projeto assinado pelo Senador Carlos Viana. Nas justificativa da proposta, menciona-se um clamor da sociedade e a existência de uma espécie de ataque cibernético sem perfeita subsunção à norma penal vigente no Brasil. Como dito, a proposta se baseia nos casos concretos de *ransomware* em que sistemas e informações tornam-se inacessíveis aos seus legítimos usuários.

Com essa brecha legislativa, MENDONÇA (2020) destaca que ao longo do tempo foram ocorrendo tentativas de inserir os casos concretos em tipos penais já existentes, sobretudo no crime de furto. Todavia, tais analogias forçadas acabam gerando discussões na doutrina sob o olhar do princípio da reserva legal e da impossibilidade da analogia *in malan partem*.

Nesse contexto, o projeto de lei apresenta o seguinte texto inicial:

> Art. 154-C. Tornar inutilizáveis ou inacessíveis, por qualquer meio, e com o fim de causar constrangimento, transtorno ou dano, sistemas ou dados informáticos alheios:
> Pena – reclusão, de três a seis anos, e multa.
> § 1º Incorre na mesma pena quem oferece, distribui, vende ou dissemina códigos maliciosos ou programas de computador, com o intuito de permitir a prática da conduta definida no caput deste artigo.
> Forma qualificada:
> § 2º Se o agente pratica a conduta prevista no caput deste artigo, com o fim de obter, para si ou para outrem, qualquer vantagem como condição ou preço do resgate: Pena – reclusão, de quatro a oito anos, e multa.
> § 3º Aumenta-se a pena de um terço à metade se o crime for praticado contra: I - Presidente da República, governadores e prefeitos; II - Presidente do Supremo Tribunal Federal; III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

> § 4º Aumenta-se a pena de metade a dois terços se o crime atingir dados ou sistemas informáticos de qualquer dos poderes da União, Estado, Distrito Federal ou Município, ou de autarquia, fundação pública, empresa pública, sociedade de economia mista ou empresa concessionária de serviços públicos.

O núcleo do tipo tem ligação direta com o elemento da disponibilidade e assim como o Art 154-A apresenta a subjetividade da finalidade do agente. Dessa maneira, aquele que tornar os dados informáticos inutilizáveis ou inacessíveis por algum ato de imprudência, negligência ou imperícia, poderá ter sua culpabilidade eximida.

Seguindo no dispositivo, a proposta da redação “sistemas ou dados informáticos alheios”, reforça a ideia de que o tipo penal do Art 154-A tutela apenas dispositivos, no sentido físico do elemento, deixando de lado sistemas e dados compreendidos no aspecto virtual e digital. Por outro olhar comparativo, o legislador pretende aplicar o novo delito com uma pena superior ao crime de invasão de dispositivo informático, considerando que a limitação da disponibilidade possui uma reprovação maior do que a confidencialidade e a integridade.(ESTEFAM, 2022)

No mais, como mencionado por PEREIRA (2023), o parágrafo primeiro do Art 154-C, copia a redação do §1º do Art 154-A, com exceção de que não se utilizou o termo “produz” e, trocou “difunde dispositivo ou programa de computador”, por “dissemina códigos maliciosos ou programas de computador”. Em caminho idêntico, os mesmos personagens elencados na majorante do § 5º do 154-A estão na proposta do § 3º do 154-C.

Em relação ao § 2º, a ideia central de obtenção de qualquer vantagem como condição ou preço do resgate se assemelha com o delito de extorsão, estabelecido no Art 158 do Código Penal[79](PEREIRA, 2023). Todavia, PRADO (2019) defende que na extorsão o agente faz com que a coisa pretendida lhe seja entregue ou colocada à sua disposição. Dessa maneira, além de debater-se a inclusão ou não de dados e informações na definição de “coisa”, no caso concreto de *ransomware*¸ o cibercriminoso já tem a posse dos sistemas e informações, utilizando-se disso para constranger a vítima. Portanto, não poderia ser aplicado a ideia de extorsão já tipificada.

[79] Art. 158 - Constranger alguém, mediante violência ou grave ameaça, e com o intuito de obter para si ou para outrem indevida vantagem econômica, a fazer, tolerar que se faça ou deixar de fazer alguma coisa

Por fim, diferentemente do crime de invasão de dispositivo, não há na proposta qualquer menção ou diferenciação para certas categorias de dados e informações como visto no Art 154-A §3º. É algo contraditório visto que no mesmo PL o legislador insere “dados pessoais” como elemento de qualificadora para o crime já existente, mas é omisso sobre o assunto quando se refere a criação do novo dispositivo. Caso essa situação persista, qualquer sistema ou dado informático que se torne inutilizável ou inacessível terá o mesmo valor, independentemente da sua natureza, seja uma lista de contato, código fonte[80], contratos de negócios ou registros sindicais.

Nota-se ainda algumas lacunas em relação a garantia da privacidade individual e proteção dos dados pessoais no meio virtual. Partindo deste ponto, o final deste trabalho será destinado para a sugestão de ajustes e lapidações legislativas e sociais em prol de uma maior proteção dos dados pessoais contra cibercrimes.

4.3 CRÍTICAS AO PL 879/2022 E AÇÕES POSSÍVEIS PARA A PROTEÇÃO DE DADOS PESSOAIS

Mesmo reconhecendo os movimentos em prol de uma maior segurança no mundo informático, não se observa a eficiência prática de tais construções tanto no meio legislativo como também no jurídico e informático. Na visão de PEREIRA (2023), se o PL 879/2022 for aprovado com seu texto inicial, nascerão inúmeros problemas de ordem material e processual, sem atingir a finalidade principal de prevenir cibercrimes.

Tal situação remete a ideia do Direito Penal simbólico, que como posto por BARCELOS (2021) em referência a Claus Roxin, constitui-se de tipos penais que não geram efeitos protetivos concretos, mas se relacionam com as manifestações políticas, midiáticas e ideológicas ao declarar determinados valores como bens jurídicos ou repudiar atitudes tratadas como lesivas. Mesmo que se fundamentem em desejos de segurança coletiva, as excessivas mudanças legislativas e a falta de

[80] O código-fonte é a origem de um programa de computador. É constituído por declarações, instruções, funções, loops e outras definições, que atuam como guias para o *software* saber como operar.

técnica sobre os novos conteúdos das redações causam uma enorme incerteza jurídica.

Analisando de forma direta o PL 879/2022, a inclusão do novo crime se conecta com a ideia de Direito Penal do risco pois além de ser uma matéria afastada do seu caráter de última *ratio*, adota um perfil expansivo, com novos tipos, bens jurídicos e sujeitos. Por outro lado, essas novidades são apenas simbólicas e teóricas uma vez que abordam pontos já contemplados no Código. Em resumo, a construção Penal não pode confundir novidade e adaptação com repetição legal.(BARCELLOS, 2021)

No contexto do Art 154-A, SYDOW (2023) argumenta que a ofensa principal está nos dados e informações, e não nos dispositivos informáticos. Dessa forma, é irrelevante aprofundar-se sobre o usuário ou titular de um dispositivo tendo em vista que o que se pretende tutelar são as informações e dados tratados por meio de um sistema ou equipamento. Manter o foco no instrumento e não no objetivo da ação deixará o delito “invasão de dispositivo informático” sempre em conflito com o princípio da consunção, que se define pela absorção do crime meio pelo crime fim.(BITENCOURT, 2011; SYDOW, 2023)

Diante disso, sugere-se uma adaptação textual do Art 154-A: Acessar ou permanecer indevidamente em dispositivo ou sistema informático, conectado ou não à rede de computadores, com o fim de realizar tratamento ilegal de dado ou informação alheia e/ou de instalar vulnerabilidade para obter vantagem ilícita.

A sugestão de caput, que poderia ser aproveitada inclusive no PL 879, tem o objetivo de: (i) contemplar a revogação da permissão e a permanência não autorizada; (ii) resolver a discussão entre a definição e abrangência de dispositivos e sistemas informáticos; (iii) expandir a lista de finalidades e elementos subjetivos; (iv) conectar o Código Penal com as definições expostas pela LGPD[81], visualizando o aspecto de normal penal em branco do Art 154-A; e (v) não exigir a instalação de vulnerabilidades no plural.

Em relação ao § 3º que também compõe o conteúdo do PL, pode-se manter a ideia do texto inicial, mas há margem para o acréscimo de uma outra majorante específica para os “dados pessoais sensíveis”, seguindo a tendência de outras

[81] Art 5º, X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

normas abordadas neste trabalho que já reconhecem o caráter especial desse tipo de dado.

Outro caminho legislativo, seria adaptar a LGPD com tipos penais específicos para a proteção de dados pessoais, na mesma linha dos crimes envolvendo crianças e adolescentes no ECA, e aqueles ligados ao trânsito no Código de Trânsito Brasileiro (CTB). Nessa possibilidade, a unificação de termos e a centralização de ideias em um só documento tende a facilitar a compreensão dos tipos penais, reduzindo a ambiguidade e a generalidade dos dispositivos.

De qualquer forma, direcionar todos os esforços para a esfera penal não pode ser compreendido como sinônimo de um nível aceitável de segurança para a sociedade, tampouco considerar a diminuição da prática delitiva como algo garantido. Para uma proteção efetiva, faz-se necessário ajustes investigativos e processuais, considerando o atual cenário ilustrado pela facilidade de encobrir provas, dificuldade de identificar e encontrar cibercriminosos, aliado à lentidão investigativa.(PACHECO; COSTA, 2018)

Pensando no aprimoramento da máquina estatal, além de uma aproximação maior com outros países signatários da Convenção de Budapeste, pode-se considerar a parceria público-privada voltada a cibersegurança, unindo o Ministério Público e órgãos policiais com empresas nacionais e internacionais que atuam no combate ao cibercrime. Os agentes estatais e não-estatais não possuem capacidade e/ou competência para atuar com qualidade de forma individual, entretanto, tal fusão pode estabelecer um ganho mútuo com fluxos de conhecimento entre as partes, além da criação de novas ferramentas e metodologias de segurança.(MOREIRA, 2019)

SANTOS (2011) defende um outro trabalho coletivo unindo Estado, empresas e cidadãos, com foco na formação de uma cultura de segurança. Na prática, o autor propõe uma atuação mais proativa, dividida em quatro planos de capacitação e conscientização: organizacional (empresas visualizando a segurança como vantagem competitiva e não como um custo); sociopolítico (legisladores e juristas com capacidade técnica sobre o tema); ética (indústria tecnológica mobilizada e sensibilizada); e educacional (inserção da cibersegurança em currículos de diferentes níveis educacionais).

Por fim, centralizando o assunto em dados pessoais, é relevante frisar sobre a margem de aprimoramento da prevenção administrativa, com o intuito de frear a

expansão penal.(BARCELLOS, 2021) Justifica-se isso com o fato de que tanto a LGPD como o MCI possuem a previsão de sanções marcadas por um perfil administrativo e reativo, com a aplicação de multas e suspensões, principalmente contra pessoas jurídicas. São medidas reativas direcionadas para aqueles que por omissão ou alta exigência técnica e financeira não satisfazem as expectavas estatais de segurança no mundo virtual.(DERBLI, 2019)

Assim, o Estado que não apresenta êxito nem na prevenção conscientizadora e nem na aplicação da pena no aspecto positivista de defesa social, compensa suas fragilidades impondo sanções em personagens que não são os criminosos de fato. Em alguns casos, os agentes sancionados sofrem uma dupla penalização tendo em vista que além da cobrança estatal são também vítimas dos cibercrimes.(CUNHA, 2017)

Nesse enredo, a ANPD, espelhando-se no Instituto Brasileiro do Meio Ambiente e dos Recursos Naturais Renováveis (IBAMA) e na Agência nacional de Vigilância Sanitária (ANVISA,) pode-se valer da previsão legal de competência fiscalizadora[82] em relação aos dados pessoais e estabelecer melhores procedimentos, quer seja pela atuação do poder de polícia ou pelo emprego de meios de inspeção ou vigilância. Assim, aplica-se um controle administrativo preventivo, liberando o Direito Penal para sua função de atuação como última *ratio*.(BARCELLOS, 2021)

Não obstante que o Direito Penal remeta à uma ideia de maior rigorosidade, esta matéria não deve ser utilizada de maneira figurativa, com tipos penais vagos e desproporção na aplicação da pena.(BARCELLOS, 2021) Na mesma linha, não deve o legislador utilizar de suas atribuições funcionais para satisfazer o clamor midiático com a criação indiscriminada de leis que além de não atingirem seu objetivo prático, causam uma sobrecarga legislativa.(NASCIMENTO JUNIOR, 2016) Em outras palavras, a norma penal não deve ser utilizada apenas com a missão de passar uma imagem de autoridades dedicadas, atentas e preocupadas com certo tema.(FLORES, 2017)

---

[82] Art 55-J, IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso; XVI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público;

Portanto, ao longo do presente tópico, que não objetivava prover uma solução única e final para o problema, buscou-se apresentar algumas possibilidades sistêmicas para reduzir a incidência e os efeitos do cibercrime contra os dados pessoais. Como bem mencionado na Convenção de Budapeste, a cooperação entre Estados, indústrias e sociedade é elemento vital para a repressão ao cibercrime. De forma equivalente, é fundamental que as diferentes disciplinas do direito se conectem e respeitem cada um seu espaço para uma proteção jurídica mais eficiente.(ARAUJO, 2022)

Verifica-se, portanto, que há espaços e possibilidades para ações preventivas, unindo os órgãos públicos com entes privados em prol de uma maior conscientização e melhores estruturas de defesa. Da mesma forma, há exemplos e previsões legais para uma atuação estatal mais fiscalizadora, orientativa e capacitadora.

Ainda assim, caso seja necessária uma atitude repressiva, pode-se valer primeiro de instrumentos administrativos, para que somente depois - se preciso for - seja aplicado o Direito Penal, na sua condição de intervenção mínima e aplicação indispensável para a manutenção da ordem jurídica. Por fim, vale reafirmar que a efetiva aplicação da matéria penal é proporcional ao seu distanciamento de normas vagas, limitantes, imprecisas e contraditórias.(BITENCOURT, 2011)

5 CONCLUSÃO

A tecnologia impacta as transformações sociais de forma acelerada e contundente, alterando as relações, as necessidades e as preocupações dos indivíduos. Como consequência, o Estado busca se adaptar a essas novas realidades e garantir ferramentas de regulamentação, proteção e repressão no ambiente virtual.

Para atingir o objetivo central deste trabalho, foram analisados os anseios e perigos sociais em diferentes recortes temporais, partindo da ideia de privacidade da burguesia americana, passando pela relação da privacidade com a internet e a inexistência de fronteiras, até atingir a especificidade dos dados pessoais, marcados pela sua alta valorização atual. Além disso, foram observadas as mudanças e

aplicações do Direito, principalmente o Direito Penal, quanto à sua tutela, divisão e atuação.

Em um primeiro momento, compreendeu-se a ideia de privacidade, ligada ao anseio social de ser deixado só, e sua materialização por meio de normativas como a Declaração dos Direitos Humanos. Percebeu-se que com o tempo houve uma mudança no conceito de privacidade, afastando-se da ideia de ser deixado sozinho, sem o envolvimento de terceiros em suas informações, para uma ideia de direito de controle, em que cada pessoa tenha o poder de controlar para onde, como e para quem suas informações serão direcionadas.

Parte considerável dessa alteração conceitual se justifica pelo impacto da internet e dos meios digitais na vida dos indivíduos, possibilitando uma troca de informações mais ágil e de maior alcance. A regularização desse “novo” ambiente de relações também é um dos enfoques deste trabalho, que se propôs a analisar a construção e os efeitos de normas como o Marco Civil da Internet.

Posteriormente, observou-se que a disciplina da privacidade passou a ser estruturada especialmente em torno dos dados pessoais, dando origem a uma nova ramificação de estudos. Os dados pessoais são muito valorizados para órgãos públicos e para o mundo corporativo, justificando a criação de legislações mais centralizadas no tema, a exemplo da Lei Geral de Proteção de Dados do Estado alemão de Hesse, em 1970, do GDPR em 2018, e da LGPD em 2020. Além dessas normativas, ao longo do trabalho foram também expostas alterações constitucionais, como a que elevou os dados pessoais para o grupo de direitos fundamentais na Constituição brasileira.

De modo geral, pode-se extrair alguns resultados do primeiro capítulo: (i) a ideia de privacidade depende do recorte sociocultural; (ii) a internet impactou, e impacta, fortemente nas relações sociais; (iii) os dados pessoais derivam do conceito de privacidade, sendo mais específicos e conectados com a vida privada; (iv) o Direito, por meio da sua função social, busca se adaptar as novas realidades e criar mecanismos para atender anseios dos indivíduos e (v) em relação a proteção de dados pessoais e internet, a Lei brasileira é altamente impactada pela norma internacional.

Na segunda seção, o intuito era averiguar sobre as adaptações no Direito Penal em relação as mudanças da sociedade, novos bens jurídicos e novas ações lesivas, além de abordar conceitos relevantes para o entendimento do assunto.

Observou-se que a expansão do Direito Penal decorre de uma série de fatores, como o surgimento de novos interesses e riscos, a sensação social de insegurança, além do descrédito de outras instâncias de proteção.

Toda essa situação desagua no Direito Penal Informático, uma vertente atual do Direito Penal, voltada a tutela de bens jurídicos no meio informático. Como foi visto, a nova matéria dedica-se a integridade, confidencialidade e disponibilidade de sistemas informáticos, redes e dados informáticos, agrupados em um único bem jurídico, denominado segurança informática.

Em relação aos perigos dessa nova realidade, foi possível perceber que há alguns desalinhamentos sobre a conceituação de termos relevantes para a compreensão da matéria, principalmente no que se refere à criminalidade no contexto informático e seus sujeitos ativos. Na análise dos tipos em espécies, observou-se tanto a corrente tripartidária como a bipartidária, considerando seus fatores de classificação e exemplos concretos.

Após a compreensão dos elementos gerais do Direito Penal Informático, o presente trabalho dedicou-se a expor sobre a Convenção de Budapeste, contemplando sua construção, seus objetivos e princípios, mas especialmente sua implicação no Brasil. Comparou-se as tipificações previstas no documento internacional com o Código Penal brasileiro e constatou-se a necessidade de ajustes legislativos, investigativos, processuais e estruturais por parte estatal, para uma tutela mais efetiva para os dados pessoais.

Ao final do capítulo, foram apresentados exemplos de ataques no meio informático, expondo situações concretas já ocorridas no Brasil. Apoiado por notícias, pesquisas e outros tipos de estudos, a presente monografia demostrou que o país é um dos principais cenários para a incidência de cibercrimes, gerando efeitos nocivos para órgãos públicos, empresas e, principalmente, para os indivíduos.

Com tudo isso, o segundo tópico constata que: (i) recorre-se ao Direito Penal com a ideia de que seja a área do direito mais rigorosa e relevante para a proteção da sociedade; (ii) o Direito Penal Informático é uma divisão mais específica do Direito Penal, derivada dos perigos atuais, (iii) não há alinhamento conciso sobre os conceitos do Direito Penal Informático, (iv) nesta temática, a legislação brasileira se molda com base na Convenção de Budapeste, mas apresenta lacunas consideráveis para sua aplicação em aspectos legislativos, investigativos e processuais, (v) o território brasileiro é um local com alta incidência de cibercrimes.

No último capítulo, por sua vez, partiu-se para a análise específica do Projeto de Lei 879/2022 e os crimes em espécie relacionados. Inicialmente, apontou-se para a construção legislativa, contemplando as Leis anteriores que se relacionam com o PL central do trabalho.

Quantos aos crimes em espécie, examinou-se os elementos do tipo, suas aplicações práticas, entendimentos doutrinários e pontos debatidos na doutrina. Com isso, observou-se traços marcantes de Leis penais em branco; normas imperfeitas, com conteúdo incompleto, vago, impreciso e que dependem de complementação jurídica. Na mesma linha, constatou-se a dificuldade de aplicação da norma, visto a sua incompatibilidade com o princípio da legalidade e a impossibilidade da analogia *in malam partem.*

Mesmo com novas construções legislativas, a atual configuração do Direito Penal não demonstra total coerência com a realidade concreta e ainda expõe limitações para garantir a tutela dos dados pessoais contra os cibercrimes. Em outras palavras, as medidas teóricas não se efetivam com sucesso na prática.

Quanto à pergunta problema, “O Projeto de Lei 879/2022 garante a tutela penal dos dados pessoais contra cibercrimes?”, resta confirmar a hipótese inicial de caráter negativo, visto que o PL possui lacunas legislativas com termos ambíguos e genéricos, além de questões práticas de difícil aplicação.

Com isso em mente, a finalização do trabalho foi direcionada para a exposição de possíveis ajustes legais, por meio da revisão legislativa e da utilização de outras matérias do direito. Além disso, também foram sugeridas ações sistêmicas, que envolvam diferentes personagens da sociedade, objetivando um aprimoramento das estruturas de conscientização, fiscalização e investigação.

Como comentado ao longo do desenvolvimento, os avanços tecnológicos proporcionam variados benefícios para a sociedade, todavia, em um efeito colateral facilitam o surgimento de novos riscos e perigos. Ainda que o Estado seja demandando por mais segurança em relação aos dados pessoais, deve-se buscar por ferramentas conscientizadoras, fiscalizadoras e penalizadoras em outras áreas do Direito, antes de recorrer ao Direito Penal.

Este por sua vez deve ser acionado no seu papel de última *ratio,* atendendo os seus princípios basilares e afastando-se da ideia de ação estatal simbólica. Novamente, reitera-se a ideia de que a efetiva aplicação da matéria penal é

proporcional ao seu distanciamento de normas vagas, limitantes, imprecisas e contraditórias.

REFERÊNCIAS

ALMEIDA, Jéssica de Jesus e colab. **Crimes Cibernéticos**. Ciências Humanas e Sociais Unit, v. 2, n. 3, p. 215–236, 2015.

ANANIAS, Amanda Silvestre Patrus e colab. **O Bem Jurídico nos Crimes Informáticos**. Revista do CAAP, v. 22, n. 1, p. 34–54, 2017.

ARAUJO, Clayton Vinicius Pegorarode. **Os Aspectos Gerais Dos Tratados Internacionais e a Convenção de Budapeste Sobre Crimes Cibernéticos**. Revista Da Faculdade De Direito Da Universidade Federal De Uberlândia, v. 50, n. 1, p. 146–165, 2022.

Ataque hacker tira do ar site do Ministério da Saúde e o ConecteSUS. Disponível em: <https://g1.globo.com/jornal-nacional/noticia/2021/12/10/ataque-hacker-ao-site-do-ministerio-da-saude-tira-do-ar-o-conectesus.ghtml>. Acesso em: 20 abr 2023.

Audiência Pública: mais 15 expositores participam do debate sobre Marco Civil da Internet. Disponível em: <https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=504828&ori=1>. Acesso em: 14 maio 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado**. [S.l: s.n.]. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_agentes_de_tratamento_e_encarregado___defeso_eleitoral.pdf>. Acesso em: 3 abr 2023. 2022

BARBOSA, Andresa. **Especialistas alertam para os principais ataques cibernéticos de 2022**. Disponível em: <https://forbes.com.br/forbes-tech/2022/02/os-principais-ataques-ciberneticos-previstos-para-2022/ Acesso em: 20 abr 2023.

BARCELLOS, Eduardo Rodrigues. **O caráter simbólico da tutela penal, seus efeitos na sociedade contemporânea e as possíveis soluções sistêmicas**. 2021. Tese de mestrado – Pontifícia Universidade Católica de São Paulo, São Paulo, 2021.

BARRETO, Alessandro Gonçalves e KUFA, Karina e SILVA, Marcelo Mesquita. **Cibercrimes e seus reflexos no direito brasileiro**. 3. ed. São Paulo: Juspodivim, 2022.

BBC NEWS BRASIL. **Entenda as polêmicas sobre o Marco Civil da Internet**. Disponível em: <https://www.bbc.com/portuguese/noticias/2014/03/140219_marco_civil_internet_mm>. Acesso em: 21 mar 2023.

BECHARA, Ana Elisa Liberatore S. **O RENDIMENTO DA TEORIA DO BEM JURÍDICO NO DIREITO PENAL ATUAL**. Revista Liberdades, n. 1, p. 16–29, 2009.

BIONI, Bruno Ricardo. **Compreendendo o conceito de anonimização e dado anonimizado**. Cadernos Jurídicos, n. 53, p. 191–201, 2020. Acesso em: 3 abr 2023.

BIONI, Bruno Ricardo e RIELLI, Mariana Marques. **A construção multissetorial da LGPD: História e aprendizados**. Proteção de dados [livro eletrônico]: contexto, narrativas e elementos fundantes, p. 15–58, 2021. Disponível em: <https://observatoriolgpd.com/wp-content/uploads/2021/08/1629122407livro-LGPD-Bruno-Bioni-completo-internet-v2.pdf>. Acesso em: 3 abr 2023.

BITENCOURT, Cezar Roberto. **Parte especial: crimes contra a pessoa**. 20. ed. [S.l.]: Saraiva, 2020. v. 2.

BITENCOURT, Cezar Roberto. **Tratado de direito penal: parte geral**. 17. ed. rev. ed. São Paulo: Saraiva, 2011.

BRASIL. **ATO DECLARATÓRIO DO PRESIDENTE DA MESA DO CONGRESSO NACIONAL Nº 58, DE 2021**. 2021 a.

BRASIL. **Constituição (1988)**.1988.

BRASIL. **Lei n° 12.965, de 23 de abril 2014**. 2014.

BRASIL. 13709. **Lei Nº 13.709, de 14 de agosto de 2018**. 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 1 fev 2023.

BRASIL. **Lei Nº 14.155, de 27 de maio de 2021**. 2021 b.

BRASIL. **Projeto de Lei Nº 879, de 2022**. 2022.

BRITO, José Sousa. **O CIBERCRIME**. 2014. Universidade Lusófona de Humanidades e Tecnologias, Lisboa, 2014.

BRUNO, MARCOS GOMES DA SILVA. **SEÇÃO III – DA RESPONSABILIDADE E DO RESSARCIMENTO DE DANOS**. MALDONADO, V. N.; BLUM, R. O. (Org.). LGPD: Lei Geral de Proteção de Dados comentada [livro eletrônico]. 2. ed. rev. ed. São Paulo: São Paulo: Thomson Reuters Brasil, 2020.

CALLEGARI, André Luís e ANDRADE, Roberta Lofrano. **Sociedade do risco e direito penal**. Revista da Defensoria Pública do Estado do Rio Grande do Sul, n. 26, p. 115–140, 2020.

CANCELIER, Mikhail Vieira de Lorenzi. **O Direito à Privacidade hoje: perspectiva histórica e o cenário brasileiro**. Seqüência studos Jurídicos Políticos, p. 213–240, 2017.

CONSELHO DA UNIÃO EUROPEIA. **Diretiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de outubro de 1995**. 1995. Disponível em: <https://www.conjur.com.br/dl/diretiva-europeia.pdf>. Acesso em: 17 mar 2023.

CUNHA, Rogério Sanches. **Manual de Direito Penal - Parte Especial (Arts 121 ao 361)**. 9. ed. [S.l.]: JusPODIVIM, 2017.

D'AVILA, Fabio Roberto e DOS SANTOS, Daniel Leonhardt. **Derecho Penal y ciberdelitos. Breves aproximaciones dogmáticas.** REVISTA PENSAMIENTO PENAL, v. 1, n. 1, p. 1–14, 2016.

DE ARAÚJO, Fábio Lucena. **Aspectos Jurídicos no Combate e Prevenção ao Ransomware**. Revista do Ministério Público do Estado do Rio de Janeiro, n. 71, p. 93–118, 2019. Disponível em: <http://brasil.elpais.com/brasil/2017/05/14/>.

DE SIMAS, Diana Viveiros. **O cibercime**. 2014. Universidade Lusófona de Humanidades e Tecnologias, Lisboa, 2014.

Declaração Universal dos Direitos Humanos. 1948. Disponível em: <https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos>. Acesso em: 17 mar 2023.

DEMARTINI, Felipe. **Em testes, metade das assistências técnicas acessaram dados dos PCs de clientes**. Disponível em: <https://canaltech.com.br/seguranca/em-testes-metade-das-assistencias-tecnicas-acessaram-dados-dos-pcs-de-clientes-231301/>. Acesso em: 20 abr 2023.

DERBLI, Ludimila Santos. **O transplante jurídico do Regulamento Geral de Proteção de Dados da União Européia ("GDPR") para o Direito Brasileiro**. E-Legis - Revista Eletrônica do Programa de Pós-Graduação da Câmara dos Deputados, v. 12, n. 30, p. 181–193, 1 Nov 2019.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados**. 3. ed. São Paulo: Thomson Reuters Brasil, 2021.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados**. 2. ed. São Paulo: Revista dos Tribunais, 2019.

DOS SANTOS, Gabrielly Daianne Alves. **Crimes Virtuais: tratamento legal e limitações no combate aos crimes cibernéticos.** Monografia. Anápolis. UniEVANGÉLICA, 2021.

EILBERG, Daniela Dora e colab. **Os cuidados com a Convenção de Budapeste**. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/os-cuidados-com-a-convencao-de-budapeste-08072021>. Acesso em: 20 abr 2023.

ESTEFAM, André. **Direito Penal: Parte Especial – Arts. 121 a 234-C –**. 9. ed. São Paulo: SaraivaJur, 2022. v. 2.

EUGENIA FINKELSTEIN, Maria e FINKELSTEIN, Claudio. **Privacidade e Lei Geral de Proteção de Dados Pessoais**. Revista de Direito Brasileira, Florianópolis, 2019. p. 284–301.

FAVORITO, FERNANDA. **Uma análise do primeiro mês de vigência do Marco Civil na Internet**. Disponível em: <https://fernandafav.jusbrasil.com.br/noticias/129525513/uma-analise-do-primeiro-mes-de-vigencia-do-marco-civil-na-internet>. Acesso em: 21 mar 2023.

FERNANDES, Maíra e MEGGIOLARO, Daniella e PRATES, Fernanda. **Lei de Proteção de Dados para segurança pública e persecução penal**. Disponível em: <https://www.conjur.com.br/2022-out-28/escritos-mulher-lei-protecao-dados-seguranca-publica-persecucao-penal>. Acesso em: 20 abr 2023.

FILHO, Paulo Roberto Aguiar de Lima. **O DIREITO PENAL NA QUARTA REVOLUÇÃO INDUSTRIAL: A EXPANSÃO RAZOÁVEL FRENTE AOS CRIMES CIBERNÉTICOS**. Delictae, v. 6, n. 10, p. 215–304, 2021.

FLORES, Karina Sartori. **A ilusão da sociedade de risco alimentada pelo Direito Penal simbólico**. Revista Da Faculdade De Direito Da FMP, v. 12, n. 2, p. 85–105, 2017.

FORNASIER, Mateus de Oliveira e SPINATO, Tiago Protti e RIBEIRO, Fernanda Lencina. **RANSOMWARE E CIBERSEGURANÇA: A INFORMAÇÃO AMEAÇADA POR ATAQUES A DADOS**. Revista Thesis Juris – RTJ, v. 9, n. 1, p. 208–236, 2020.

GARCIA, Amanda. **Entenda o que muda após a promulgação da Convenção sobre o Crime Cibernético**. Disponível em: <https://www.cnnbrasil.com.br/tecnologia/entenda-o-que-muda-apos-a-promulgacao-da-convencao-sobre-o-crime-cibernetico/>. Acesso em: 4 mai 2023.

GIACCHETTA, André Zonaro e MENEGUETTI, Pamela Gabrielle. **Marco Civil da Internet: A garantia constitucional à inviolabilidade da intimidade e da vida privada como direito dos usuários no marco civil da internet.** São Paulo: Atlas, 2014.

GOMES, Évelyn Vieira e BITTENCOURT, Izabella Alves Jorge. **A era do algoritmo: Os impactos na atual sociedade informacional**. 2º Simpósio Internacional Subjetividade e Cultura Digital, Belo Horizonte, 2019. p. 109–105.

GRECO, Rogério. **Direito Penal Estruturado**. São Paulo: Método, 2019.

JORNAL NACIONAL. **PL das Fake News: entenda o que diz o projeto que criminaliza divulgação de notícias falsas na internet**. Brasil: Rede Globo. 2 maio 2023

KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. **Dados Sensíveis na Lei Geral de Proteção de Dados Pessoais: mecanismos de tutela para o livre desenvolvimento da personalidade.** 2019. Tese de mestrado – Universidade Federal de Juiz de Fora, Juiz de Fora, 2019.

LÓSSIO, Claudio Joel Brito. **Manual descomplicado de direito digital**. 3. ed. São Paulo: Juspodivm, 2022.

LUGATI, Lys Nunes e ALMEIDA, Juliana Evangelista De. **A LGPD e a construção de uma cultura de proteção de dados**. Revista de Direito, v. 14, n. 01, p. 01–20, 29 jun 2022.

MACRI JÚNIOR, José Roberto e MACRI, Bianka Jaquetti. **EXPANSÃO DO DIREITO PENAL: ABORDAGEM SOCIOLÓGICA**. Revista Reflexão E Crítica Do Direito, v. 5, n. 1, p. 185–203, 2017.

MALDONADO, Viviane Nóbrega e BLUM, Renato Opice. **LGPD: Lei Geral de Proteção de Dados comentada**. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

MARQUES, Garcia e MARTINS, Lourenço. **Direito da Informática**. 2. ed. Coimbra: Almedina, 2006.

MATSUYAMA, Keniche Guimarães e LIMA, João Ademar de Andrade. **CRIMES CIBERNÉTICOS: ATIPICIDADE DOS DELITOS**. [S.d.].

MENDONÇA, Júlia Fernandes De. **A RESPONSABILIDADE CIVIL E PENAL DOS ENVOLVIDOS EM SEQUESTROS DIGITAIS EM FACE DA LEGISLAÇÃO BRASILEIRA DE PROTEÇÃO DE DADOS PESSOAIS**. Revista do CEPEJ, v. 22, p. 156–173, 2020.

MOREIRA, Maria Cristina de Castro. **A parceria público-privada na ciberestratégia norte-americana: uma análise comparativa entre as ações dos governos Bush e Obama (2001-2017)**. 2019. Trabalho de conclusão de graduação – Universidade Federal do Rio Grande do Sul., Porto Alegre, 2019.

MULCAHY, Nick. **DLA Piper Counts €2.9bn GDPR Fines In 2022**. Disponível em: <https://businessplus.ie/news/gdpr-fines-dla-piper/>. Acesso em: 3 abr 2023.

NADER, Paulo. **Introdução ao Estudo do Direito**. Rio de Janeiro: Forense, 2014.

NASCIMENTO JUNIOR, Aguinaldo Ferreira Do. **DIREITO PENAL SIMBÓLICO: a ineficiência do sistema penal contemporâneo**. Revista JurES, v. 8, n. 17, 2016.

OLIVEIRA, Camila Fiamoncini. **Dados pessoais disponíveis publicamente e a prática de data scraping: uma análise dos parâmetros legais impostos pela Lei Geral de Proteção de Dados Pessoais**. 2022. Universidade Federal de Santa Catarina, Florianópolis, 2022.

ORLOWSKI, Jeff. **O dilema das redes**. Estados Unidos da América: Netflix. 2020

PACHECO, Gisele Freitas e COSTA, Renato Lopes. **CRIMES VIRTUAIS E A LEGISLAÇÃO PENAL BRASILEIRA**. Revista Eletrônica de Ciências Jurídicas, v. 1, n. 1, 2018. Disponível em: <http://fadipa.educacao.ws/ojs-2.3.3-3/index.php/cjuridicas/article/view/269>. Acesso em: 4 maio 2023.

PARLAMENTO EUROPEU. **Direito da União Europeia: Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016**. 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680&from=HU>. Acesso em: 3 abr 2023.

PEREIRA, Emanuela de Araújo. **Reflexões sobre o crime de invasão de dispositivo informático e o PL 879/2022**. Disponível em: <https://www.jornaljurid.com.br/doutrina/penal/reflexoes-sobre-o-crime-de-invasao-de-dispositivo-informatico-e-o-pl-8792022>. Acesso em: 4 maio 2023.

PESTANA, Marcio. **Os princípios no tratamento de dados na LGPD (Lei Geral da Proteção de Dados Pessoais)**. Disponível em: <https://www.conjur.com.br/dl/artigo-marcio-pestana-lgpd.pdf>. Acesso em: 5 abr 2023.

PRADO, Luiz Regis. **Curso de Direito Penal Brasileiro**. 17. ed. Rio de Janeiro: Forense, 2019.

RODOTÀ, Stefano. **A vida na sociedade da vigilância – privacidade hoje [Tradução de Danilo Doneda e Luciana Cabral Doneda]**. Rio de Janeiro: Renovar, 2008.

RODRIGUES AFONSO, José Roberto e RIOS DA NÓBREGA, Marcos Antônio e NETTE ALVES OLIVEIRA DE CASTILHOS, Núbia. **Criptomoedas e Moedas Digitais dos Bancos Centrais – Desafios e Perspectivas da Tributação no Brasil**. Direito Público, v. 19, n. 102, 6 Set 2022.

RODRIGUES, Laura Secfém. **Linha do tempo da Lei Geral de Proteção de Dados (LGPD)**. Disponível em: <https://laurasecfem.jusbrasil.com.br/artigos/1149830826/linha-do-tempo-da-lei-geral-de-protecao-de-dados-lgpd>. Acesso em: 3 abr 2023.

ROSSINI, Augusto Eduardo de Souza. **A informática e a telemática ante o direito penal**. 2003. Pontifícia Universidade Católica de São Paulo, São Paulo, 2003.

SANTOS, Ana Felícia Canilho. **O CIBERCRIME: DESAFIOS E RESPOSTAS DO DIREITO**. 2015. Universidade Autónoma de Lisboa, Lisboa, 2015.

SANTOS, Bruna Martins Dos. **Convenção de Budapeste Sobre o Cibercrime na América Latina: uma breve análise sobre adesão e implementação na Argentina, Brasil, Chile, Colômbia e México**. [S.l: s.n.], 2022.

SANTOS, José Lino Alves Dos. **Contributos para uma melhor governação da cibersegurança em Portugal**. 2011. Mestrado – Universidade Nova de Lisboa, Lisboa, 2011.

SANTOS, Rahellen. **O que é o Marco Civil da Internet?** Disponível em: <https://www.politize.com.br/marco-civil-da-internet/>. Acesso em: 21 mar 2023.

SCHREIBER, Anderson. **PEC 17/19: Uma Análise Crítica**. Disponível em: <https://genjuridico.jusbrasil.com.br/artigos/734618692/pec-17-19-uma-analise-critica>. Acesso em: 5 abr 2023.

SENADO FEDERAL. **Proposta de Emenda à Constituição Nº 17, de 2019**. 2019. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=7925004&ts=1647518557360&disposition=inline>. Acesso em: 17 mar 2023.

SHAHUL, Ameer. **Data is the New Oil. Right?** Disponível em: <https://www.ibm.com/blogs/digital-transformation/in-en/blog/data-is-the-new-oil-right/>. Acesso em: 3 abr 2023.

SHANKAR, Akarshita e SHETTY, Ramesh e NATH K, Badari. **A Review on Phishing Attacks**. nternational Journal of Applied Engineering Research, v. 14, n. 9, p. 2171–2175, 2019.

SILVA, Orlando. **PARECER PROFERIDO EM PLENÁRIO AO PROJETO DE LEI Nº 2.630, DE 2020, E APENSADOS**. Brasília: [s.n.], 2023.

SIQUEIRA, EDUARDO RODRIGO BARBOSA. **Marco Civil da Internet**. Disponível em: <https://adv-siqueirabr349120.jusbrasil.com.br/artigos/1775140412/marco-civil-da-internet>. Acesso em: 21 mar 2023.

SOBRINHO, Jéssica Rafaela Nunes e GROTT, Sergio. **OS SUJEITOS ATIVOS NO CIBERCRIME E A RESPONSABILIDADE PENAL DO OFENSOR**. REVISTA CIENTÍFICA MULTIDISCIPLINAR DO CEAP, v. 4, n. 2, p. 1–10, 2022.

SOUZA, Nicolle Bêtta De e ACHA, Fernanda Rosa. **A Proteção de dados como direito fundamental: Uma análise a partir da Emenda Constitucional 115/2022**. Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 8, n. 9, p. 666–684, 30 Set 2022.

SOUZA, Mykaelly. **Cibercrimes e os reflexos no Direito brasileiro**. Goiânia: [s.n.], 2021.

SYDOW, Spencer Toth. **Curso de Direito Penal Informático - Parte geral e especial**. 4. ed. São Paulo: Juspodivm, 2023.

TOMASEVICIUS FILHO, EDUARDO. **Marco civil da internet: Uma lei sem conteúdo normativo**. Estudos Avançados, v. 30, n. 86, p. 269–285, 1 jan 2016.

TORTELLA, Tiago. **Após 13 dias fora do ar, ConecteSUS volta a funcionar, diz Ministério da Saúde**. Disponível em: <Após 13 dias fora do ar, ConecteSUS volta a funcionar, diz Ministério da Saúde>. Acesso em: 20 abr 2023.

UNIÃO EUROPÉIA. **Carta dos Direitos Fundamentais da União Europeia**. 2000. Disponível em: <https://www.europarl.europa.eu/charter/pdf/text_pt.pdf>. Acesso em: 17 mar 2023.

UNIÃO EUROPÉIA. **Regulamento Geral sobre a Proteção de Dados - GDPR (2016/679)**. 2016.

VAINZOF, Rony. CAPÍTULO I – Disposições Preliminares. OPICE BLUM, R.; MALDONADO, V. N. (Org.). LGPD: Lei Geral de Proteção de Dados comentada [livro eletrônico]. 2. ed. rev. ed. São Paulo: Thomson Reuters Brasil, 2020.

VIANNA, Túlio e MACHADO, Felipe. **Crimes informáticos**. Belo Horizonte: Fórum, 2013.

VOLPI, Matheus Tauan e VOLPI, Murilo Alan. **Ransomware no ordenamento jurídico brasileiro**. Revista Judiciária do Paraná, v. 19, n. 22, p. 79–98, 2021.

WARREN, Samuel D. e BRANDEIS, Louis D. **The Right to Privacy**. Harvard Law Review, v. 4, n. 5, 1890.

ZANIOLO, Pedro Augusto. **Crimes modernos: o impacto da tecnologia do direito**. 4. ed. [S.l: s.n.], 2021.