CENTRO UNIVERSITARIO AMPARENSE – UNIFIA

CURSO DE DIREITO

OTACÍSIO FERREIRA DA SILVA

DIREITO DIGITAL: PRIVACIDADE E A INVIOLABILIDADE DOS DADOS NO CIBERESPAÇO

Amparo/SP

2023

OTACÍSIO FERREIRA DA SILVA

DIREITO DIGITAL: PRIVACIDADE E A INVIOLABILIDADE DOS DADOS NO CIBERESPAÇO

Trabalho de conclusão de curso, apresentado ao curso de Direito do Centro Universitário Amparense (UNIFIA) sob a orientação da Prof. Dra. Ana Silvia Marcatto Begalli, como requisito parcial para obtenção do título de Bacharel em Direito.

Amparo/SP
2023

Dedico este trabalho a quem colaborou diretamente comigo: minha esposa, minha orientadora Ana Silvia Marcatto Begalli, o coordenador Leandro Tomazi e a todos os professores que de alguma forma contribuíram, sem o qual eu não teria concluído este projeto.

AGRADECIMENTOS

Em primeiro lugar, a Deus, que fez com que meus objetivos fossem alcançados, durante todos os meus anos de estudos.

À minha esposa, por todo o apoio e pela ajuda, que em muito contribuíram para a realização deste trabalho.

Aos meus pais e irmãos, que me incentivaram nos momentos difíceis e compreenderam a minha ausência enquanto eu me dedicava à realização deste trabalho.

Aos amigos, que sempre estiveram ao meu lado, pela amizade incondicional e pelo apoio demonstrado ao longo de todo o período de tempo em que me dediquei a este trabalho.

Aos professores, pelas correções e ensinamentos que me permitiram apresentar um melhor desempenho no meu processo de formação profissional ao longo do curso.

“O advogado deve sugerir por forma tão discreta os argumentos que lhe dão razão, que deixe ao juiz a convicção de que foi ele próprio quem os descobriu”. (Piero Calamandrei)

RESUMO

São inegáveis os avanços provocados na internet ao redor do mundo. Todavia, também pode ser vislumbrado o aumento da prática de atos ilícitos no ciberespaço, devido a migração da sociedade para este âmbito. O vigente estudo tem como cerne analisar a insuficiência da proteção à privacidade e aos dados pessoais no ordenamento jurídico pátrio. Isto posto, serão abordados os conceitos de ciberespaço e cibersegurança, a fim de melhor analisar este novo contexto. Ademais, será investigado o direito à privacidade no ordenamento jurídico brasileiro, bem como seu progresso histórico e sua classificação. Além disso, será apurada a tutela dos dados pessoais no Direito pátrio, de forma a aprofundar o estudo sobre a definição de informação e dado, a relação entre os dados pessoais e a privacidade e o exame da legislação pertinente. Por fim, abordar-se-á o cometimento de atos ilícitos no ciberespaço, com o fito de explanar seus problemas, providências a serem tomadas e a importância do operador do Direito nesta conjuntura.

Palavras-chave: Op□r□dor do Dir□ito; dados p□sso□is; privacidade.

ABSTRACT

The advances made on the internet around the world are undeniable. However, an increase in the practice of illicit acts in cyberspace can also be seen, due to the migration of society to this area. The current study aims to analyze the lack of protection of privacy and personal data in the national legal system. That said, the concepts of cyberspace and cybersecurity will be addressed in order to better analyze this new context. In addition, the right to privacy in the Brazilian legal system will be investigated, as well as its historical progress and classification. In addition, the protection of personal data under national law will be investigated, in order to deepen the study on the definition of information and data, the relationship between personal data and privacy and the examination of the relevant legislation. Finally, the commission of illicit acts in cyberspace will be addressed, with the aim of explaining its problems, measures to be taken and the importance of the operator of the Law in this conjuncture.

Keywords: L□w Op□r□tor; p□rson□l d□t□; privacy.

SUMÁRIO

INTRODUÇÃO

Por intermédio do surgimento da vigilância do ciberespaço e em seu exterior, sobretudo em virtude da emersão da internet e da majoração exacerbada do valor de mercado dos dados das pessoas, adveio, nos tempos atuais, um novo padrão de desafios para o Direito. Em razão da otimização da tecnologia, emergem problemas anteriormente inexistentes, uma vez que com a técnica desponta, ainda, algo que sai do escopo do ser humano.

Guardando similaridades com as distopias literárias, cinematográficas e televisivas, nas quais a tecnologia, por meio da manipulação de dados, é hábil a viabilizar decisões automatizadas e elaborar perfis de consumidores e usuários, a realidade se torna cada vez mais ficcional. Ainda que se considere as diversas nuances positivas do tratamento das informações pessoais, é crucial que se volte a atenção para as viabilidades de cometimento de atos ilícitos no meio virtual, sobretudo no que tange ao direito à privacidade.

Isto posto, o presente trabalho tem o intento de demonstrar que o ordenamento jurídico pátrio não protege, de modo suficiente e eficaz, a privacidade e a inviolabilidade de dados no que cerne ao ciberespaço. Para tanto, o primeiro capítulo abordará os conceitos de ciberespaço e cibersegurança. Ulteriormente, o segundo capítulo tratará do direito à privacidade no Direito brasileiro. Em seguida, o terceiro capítulo será o responsável por expor a tutela dos dados pessoais, abordando o conceito de dado e informação, o vínculo entre estes e os dados pessoais e as legislações acerca do tema.

Por fim, o último capítulo versará acerca do cometimento de atos ilícitos no meio virtual, os problemas e providências a serem tomados de forma a sanar a questão e a importância do investimento em operadores do Direito no combate a ilícitos praticados nesta seara. Cuida-se de debate extremamente necessário na atualidade, eis o grande valor concedido a dados pessoais que, se correlacionados, podem ser depreendidas ingerências de monta econômica, social e política, incluindo-se predisposições às decisões íntimas dos usuários.

Desta feita, o presente trabalho se vale da abordagem qualitativa, haja vista que tem o intento de aprofundar a conjuntura analisada e a perspectiva interpretativa das informações viáveis para a realidade. Em que pese à finalidade almejada pelo atual trabalho, será empregado o método dedutivo, que será aplicado através de procedimentos técnicos, fundamentados na doutrina e na legislação vigente.

Nesta esteira, se vale da pesquisa bibliográfica com o fito de argumentar as teorias suscitadas. No que diz respeito aos objetivos, aplica-se a pesquisa exploratória, uma vez que o intento é possibilitar uma maior aproximação com o problema estudado.

1 CIBERESPAÇO E CIBERSEGURANÇA

1.1 Conceito de ciberespaço

Embora seja atual, a preocupação com a tutela dos dados dos indivíduos não é uma exclusividade dos tempos atuais. Desde a Antiguidade, o indivíduo registra seu cotidiano dos mais diversos modos para as atuais e futuras gerações. Todavia, em virtude do advento do ciberespaço e das redes de internet, a elaboração, armazenamento e transmissão de dados têm se aprofundado, e, em virtude disso, as vulnerabilidades são majoradas, tal como determina Machado (2019).

Desta feita, perante essas alterações, a seara da segurança da informação, incumbida de atribuir valores aos ativos de informação de Estados e empresas, além da instauração de políticas de segurança normas, procedimentos e diretrizes, que devem oportunizar confidencialidade, integridade e disponibilidade da informação, tem se debruçado sobre as temáticas que abarcam o ciberespaço, a segurança neste espaço e a tutela dos dados pessoais (MACHADO, 2019).

O nascedouro do termo ciberespaço se coaduna com a obra de ficção científica intitulada "Neuromancer", de autoria de William Gibson e surgida em 1984, que determina o ciberespaço como sendo uma simbolização gráfica de informações depreendidas de bancos de todos os computadores da organização humana (GIBSON, 2015).

Do ponto de vista científico, no entanto, Kuehl descreve o ciberespaço como sendo:

> [...] um domínio global dentro do ambiente informacional que se destaca pelo uso da eletrônica e do espectro eletromagnético a fim de criar, armazenar, modificar, trocar e explorar a informação através de redes interdependentes e interconectadas que utilizam tecnologias de comunicação e informação (KUEHL *in* STARR; WENTZ, 2009, p. 28).

Na visão de Lévy, ciberespaço é o meio de comunicação aberto por intermédio da interconexão global de computadores e dos dados armazenados nestes. Para o referido autor, o instituto em comento detém a vocação de pôr em harmonia e interfacear os dispositivos de elaboração de informação, de comunicação, de gravação e de simulação (LÉVY, 1999).

Além disso, Lévy fez a profecia de que partindo-se do início do século XXI, a perspectiva de digitalização geral dos dados transformará o ciberespaço o principal meio de comunicação e armazenamento de memória dos seres humanos (LÉVY, 1999).

De acordo com Guimarães Júnior, a expressão “ciberespaço” pode ser conceituada como o lugar virtual elaborado pelo compilado de variadas tecnologias de telemática e telecomunicação, sobretudo as intermediadas por computador, mas não somente por elas (GUIMARÃES JÚNIOR, 2000).

Na atualidade, a internet é a mais importante seara do ciberespaço, sobretudo em razão de que, atualmente, todas as redes que se valem de tecnologias da informação e comunicação se concentram na computação e nas plataformas localizadas no meio digital (GUIMARÃES JÚNIOR, 2000).

Logo, todos os dados e informações que circulam pelos notebooks, computadores, smartphones, smartvs, tablets, videogames e etc., transitam pelo ciberespaço (GUIMARÃES JÚNIOR, 2000).

1.2 Cibersegurança

A expressão cibersegurança, também denominada segurança cibernética, delineia todos os atos para tutelar computadores, dados e redes contra ataques a sua integridade, confidencialidade e disponibilidade, centrando-se sobretudo na tutela da informação no padrão digital e nos sistemas conectados que a transmitem, processam e armazenam (MENDOZA, 2017).

Nesta esteira, percebe-se que a cibersegurança é uma parcela da seara de segurança da informação, definição mais englobante que abarca a tutela de dados, não somente nos meios digitais, mas em qualquer forma que eles possam ser achados (meio digital, físico, no âmbito das ideias, entre outros) (MENDOZA, 2017).

Neste escopo, são relevantes os princípios fundamentais da segurança da informação e, por conseguinte, da cibersegurança, a saber: a disponibilidade, a integridade e a confidencialidade (POLESEL, 2021).

Em consonância com Machado, confidencialidade é a habilidade de assegurar que o estágio necessário de sigilo seja empregado em cada compilado de dados em processamento. Ademais, cuida-se de prevenção em detrimento da divulgação não permitida destes (MACHADO, 2019).

Assim sendo, técnicas de criptografia, além de procedimentos apropriados para o armazenamento, monitoramento, acesso e transferência de dados podem reduzir a atuação de usuários que não estejam autorizados a acessar determinada informação (MACHADO, 2019).

No que tange à integridade, Machado discorre ser a garantia de confiabilidade e rigor dos sistemas e informações e de que não existirão alterações não permitidas de dados. Em virtude deste princípio, a operabilidade e o processamento de dados exatos podem evitar modificações não desejadas ou ingerências hábeis a prejudicar a completude e plenitude das informações transmitidas ou armazenadas (MACHADO, 2019).

A disponibilidade, por seu turno, é a habilidade que as redes e os sistemas devem deter para realizar e disponibilizar as informações de modo adequado e previsível e, perante equívocos, se recuperarem de maneira segura e célere, a fim de que o acesso e processamento dos dados sejam impactados minimamente (MACHADO, 2019).

Diante disso, assegurar a confidencialidade, a disponibilidade e a integridade da informação no ciberespaço tem sido um desafio contínuo para a cibersegurança e, de modo geral, para a sociedade em sua totalidade, eis que, efetivamente, as testilhas provenientes da elaboração, transmissão, armazenamento e exploração de informação não são somente digitais, mas abarcam, sobretudo, a seara jurídica que tem se concentrado a normatizar e suprir as carências da coletividade digital (PINHEIRO, 2016).

Na acepção de Pinheiro, o Direito pátrio, ainda bastante embrionário nesta seara, tem progredido no equilíbrio de testilhas de interesse da sociedade digital, tais quais a privacidade, inclusão digital, liberdade de expressão, tutela de dados pessoais, armazenamento de provas eletrônicas, dentre outros (PINHEIRO, 2016).

2 DIREITO Á PRIVACIDADE

2.1 Evolução histórica

Primeiramente, é imprescindível entender o progresso histórico da definição de privacidade. No decorrer do século XIX, a fim de se atingir a privacidade, era preciso o desempenho do direito de propriedade, de forma que as definições se encontravam relacionadas (DONEDA, 2020).

Contudo, partindo-se do século XX, através do advento dos meios de comunicação de massa, existiu profunda alteração nos padrões de rotação do ordenamento jurídico, o que acarretou transformações na definição de privacidade e na forma de sua tutela (DONEDA, 2020).

> O recôndito mundo privado, antes garantido pelo chamado direito à privacidade, passou assim a demandar modelos jurídicos específicos para sua proteção – para a qual não bastam as ações individuais ressarcitórias, associadas à noção de privacidade como isolamento e reserva, na perspectiva tornada clássica por Warren e Brandeis no início do século XX (DONEDA, 2020, p. 13).

Nesta esteira, o artigo viabilizou que o direito à privacidade nos Estados Unidos da América fosse protegido pela seara constitucional. Em virtude disso, emergiu a necessidade de conceituação de um teor comum ao direito da privacidade, produto da massificação da transmissão de informações, eis que aumenta a necessidade de se robustecer os modos de proteção (DONEDA, 2020).

A partir dos anos 1970, o direito se relacionou cada vez mais com a acepção de privacidade e o problema do armazenamento de dados. De acordo com Robert Ellis Smith, atualmente, no que tange à privacidade, esta se conecta não somente ao direito de conservar a natureza sigilosa de fatos pessoais, mas também ao direito de ter ciência de quais informações sobre si são usadas e armazenadas por outrem, e, ainda, o direito de conservar essas informações verídicas e atualizadas (SMITH, 2000).

Várias teses emergiram com o fito de fracionar a acepção de privacidade. Neste panorama, cita-se a tese de Hubmann de 1953, também intitulada tese das esferas concêntricas, que sustentava a existência de diversos estágios de exteriorização do sentimento de privacidade. O estágio mais interno seria simbolizada pelo segredo ou intimidade, de forma que ao redor

dela se imiscuiria o estágio privado, e ao redor de ambas, a nuance pessoal, o que abrangeria a vida pública (HUBMANN, 1967).

Entretanto, esta tese também se tornou influente, tal como elucida Burket, como a tese da "pessoa enquanto cebola passiva", eis que não se demonstrava apropriada para a suficiente tutela da pessoa humana em virtude da separação de suas nuances de privacidade. Desta maneira, em virtude de ser enfoque de críticas, foi desprezada pelo Tribunal Constitucional Alemão no ano de 1983 (CHAVES, 2010).

Esta icônica decisão foi a incumbida de anular, de modo parcial, a lei de censo populacional da Alemanha que autorizava o rastreio dos dados do censo até os cidadãos, bem como que aqueles fossem aplicados para outros fins. Por conseguinte, firmou o entendimento de um direito constitucional de autodeterminação informativa, organizando as bases de tutela de dados à época (CHAVES, 2010).

Em consonância com a referida decisão, não se pode considerar apenas a natureza das informações, uma vez que são determinantes, ainda, a sua aplicação e sua necessidade. O fim para o qual a coleta de dados é voltada são importantes para o seu emprego e necessidade, de maneira que não existem dados sem relevância (CHAVES, 2010).

Nesta esteira, o progresso da própria personalidade, sem influências externas, é incumbido por evitar a sujeição do controle social impingido, este hábil a restringir a individualidade e limitar a autonomia privada da pessoa. Ademais, a tutela da privacidade não pode mais ser entendida somente a partir da dialética da exclusão, como amparo em detrimento do externo, mas, ainda, como um componente fomentador da cidadania (DONEDA, 2020).

O direito à privacidade, demonstra, assim, uma acepção coletiva, tendo em vista que a cidadania é premissa da sociedade democrática contemporânea e, ainda, incumbência promocional, eis que procura fomentar a tutela da pessoa humana (DONEDA, 2020).

A privacidade avoca, então, uma natureza relacional, já que se vincula à relação com outros indivíduos e com o mundo externo. Diante disso, se não se harmonizaria com a tese dos círculos concêntricos, eis que procura a elaboração de uma individualidade e o desenvolvimento livre da personalidade partindo-se de uma definição universal, sendo esta proteção basilar para a tutela da dignidade da pessoa humana (DONEDA, 2020).

2.2 Conceito e classificação

A privacidade consiste em um direito humano, tal como se pode depreender do artigo XII da Declaração Universal dos Direitos Humanos (DUDH). Esta Declaração foi prolatada

pela Assembleia Geral das Nações Unidas de Paris em 1948, através da Resolução nº 217 da Assembleia Geral, enquanto uma norma comum a ser atingida por todas as nações e povos (AGNU, 1948).

O referido artigo preleciona: “Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques” (AGNU, 1948).

No Brasil, o direito à privacidade está protegido pela Carta Magna por intermédio do artigo 5º, X, que declara: “São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação” (BRASIL, 1988).

Em virtude disso, a privacidade configura um princípio fundamental a ser respeitado no ordenamento jurídico pátrio. Desta maneira, se toda pessoa deve ter direito à tutela de suas propriedades e de sua privacidade, é fato que suas informações constituem um ativo da propriedade e, em virtude disso, são merecedoras de proteção (PINHEIRO, 2016).

Vale mencionar que a inviolabilidade do sigilo de dados, preconizada no artigo 5º, XII, da Constituição Federal, complementa, na visão de José Afonso da Silva, a previsão ao direito à vida privada e à intimidade, dispostos no artigo 5º, X, da Lei Maior (SILVA, 2016).

As referidas previsões de defesa da privacidade são regulamentadas pelo princípio da exclusividade, que procura garantir ao indivíduo, como sustenta Tercio Ferraz Júnior,

> [...] sua identidade diante dos riscos proporcionados pela niveladora pressão social e pela incontrastável impositividade do poder político. Aquilo que é exclusivo é o que passa pelas opções pessoais, afetadas pela subjetividade do indivíduo e que não é guiada nem por normas nem por padrões objetivos. No recôndito da privacidade se esconde, pois a intimidade. A intimidade não exige publicidade porque não envolve direitos de terceiros. No âmbito da privacidade, a intimidade é o mais exclusivo dos seus direitos (FERRAZ JÚNIOR, 1992, p. 441).

Isto posto, a defesa da privacidade deve tutelar o indivíduo em detrimento de: i) ingerência em sua vida familiar, privada e doméstica; ii) interferência em sua integridade mental ou física, em sua liberdade moral ou intelectual; iii) ataques à sua reputação (honra); iv) sua posição em ocupação falsa; v) utilização de sua identidade, retrato (nome); vi) espionagem; vii) interferência na correspondência; viii) mau emprego de informações orais

□scrit□s; ix) tr□nsf□rênci□ d□ inform□s conc□didos ou r□c□bidos □m virtud□ d□ s□gr□do profissional (SILVA, 2016).

3 A PROTEÇÃO DOS DADOS PESSOAIS NO DIREITO BRASILEIRO

3.1 Conceito de dado e informação

O debate acerca da privacidade cada vez mais retoma questionamentos vinculados a dados pessoais e, por conseguinte, acerca da informação. A tarefa da informação enquanto referência de uma grande quantidade de contextos jurídicos é latente. A sua relevância e visibilidade para a sociedade contemporânea também é flagrante (DONEDA, 2020).

Asseverar a importância da informação na qualidade de um dado moderno, não é, contudo, uma verdade plena, eis que é igualmente conjecturável a abstração de sua relevância em períodos precedentes (MENESINI, 1983).

No que tange ao emprego das expressões "informação" e "dado", é imprescindível perceber, a princípio, que o teor de ambos é priorizado em vários contextos, o que legitima uma determinada vulgaridade em seu emprego. As duas expressões operam como a representação de um fato, uma certa acepção de uma realidade (DONEDA, 2020).

Apesar disso, cada uma delas detêm suas particularidades a serem consideradas. Desta maneira, o "dado" explicita conotação mais fracionada e primitiva, tal como se depreende em um autor que o compreende como uma informação em estágio potencial, em momento anterior à sua transmissão. O dado, desta maneira, consistiria em um tipo de "pré-informação", precedente à interpretação e a um processo de confecção (WACKS, 1989).

A informação, por seu turno, se refere a algo para além da simbolização detida no dado, alcançando o patamar da cognição. Ainda que não aluda ao seu significado, no contexto da informação, já se presume a purificação de seu conteúdo, de forma que carrega uma acepção instrumental, de forma a minorar um estágio de dúvida. Todavia, deve-se ressaltar que a comunidade doutrinária e a legislação, por vezes, abordam estas duas expressões de maneira indistinta (DONEDA, 2020).

Efetivamente, o que atualmente salienta a informação de sua acepção histórica é a maior habilidade de sua manipulação, que pode se imiscuir desde o estágio de sua coleta e tratamento até à sua transmissão. Nota-se, também, que o condutor desta diferenciação é tecnológico, eis que fomenta a habilidade de comunicação e armazenamento, majorando, ainda, a diversidade de modos através dos quais a informação pode ser empregada ou apropriada (DONEDA, 2020).

À proporção em que se amplia a sua utilidade, mais a informação se torna um componente basilar para uma crescente quantidade de vínculos, como, ainda, majorando-se as suas viabilidades de influenciar no cotidiano das pessoas. Em consonância com o que percebeu

Rodotà, em 1973, a novidade precípua principiada pelos computadores é a alteração da dispersão da informação para a organização da mesma (RODOTÀ, 1973).

3.2 O vínculo entre os dados pessoais e a privacidade

A informação de monta pessoal se encontra vinculada à privacidade em virtude de uma lógica simplificada e básica que relaciona um maior estágio de privacidade à menor disseminação de informações de cunho pessoal e vice-versa (DONEDA, 2020).

Esta lógica não finaliza o complexo problema ao redor deste vínculo. Contudo, pode operar como ponto de partida para exemplificar a forma pela qual a tutela dos dados pessoais passou a achar amparo no ordenamento jurídico brasileiro, a saber: enquanto um produto da proteção do direito à privacidade (DONEDA, 2020).

Em razão da majoração da relevância da informação de maneira geral, é precisamente ao redor dela que o tema da privacidade passou a girar, sobretudo no que cerne aos dados pessoais (DONEDA, 2020).

Através da tutela dos dados pessoais, tutelas, a princípio vinculadas à privacidade, passam a ser encaradas em uma nuance mais englobante, por meio da qual outros interesses devem ser levados em consideração, compreendendo vários modos de controle tornadas viáveis com a manipulação de dados pessoais (DONEDA, 2020).

> A proteção de dados pessoais é uma disciplina que engloba, em grande parte, temas relacionados ao direito à privacidade. Ela é um instrumento para a construção da própria esfera privada e, portanto, para o livre desenvolvimento da personalidade. Essa passagem, da privacidade à proteção dos dados pessoais, obedece a critérios metodológicos que procuram promover a funcionalidade de alguns dos valores fundamentais do ordenamento. Essa transição, porém, sublinhou a necessidade do direito civil confrontar uma série de elementos com os quais não estava habituado, seja pela sua absoluta novidade ou então pelo fato de se estender a domínios dos quais era mantido afastado, devido a uma longa tradição patrimonialista (DONEDA, 2020, p. 313).

A fim de que seja realizada uma plena apreciação da problemática, estes interesses devem ser levados em consideração pelo operador do Direito devido ao que simbolizam, e não apenas pela sua nuance latente, qual seja: a ofensa da privacidade (DONEDA, 2020).

> O ponto fixo de referência neste processo é que, entre os novos prismas para visualizar a questão, mantém-se uma constante referência objetiva

> a uma disciplina para os dados pessoais, que manteve o nexo de continuidade com a disciplina da privacidade, da qual é uma espécie de herdeira, atualizando-a e impondo características próprias (DONEDA, 2020, p. 164).

Essa relação na abordagem dos dados pessoais com o controle foi particularizada pelo Ministro Ruy Rosado de Aguiar, em uma decisão prolatada no ano de 1995:

> A inserção de dados pessoais do cidadão em bancos de informações tem se constituído em uma das preocupações do Estado moderno, onde o uso da informática e a possibilidade de controle unificado das diversas atividades da pessoa, nas múltiplas situações de vida, permitem o conhecimento de sua conduta pública e privada, até nos mínimos detalhes, podendo chegar à devassa de atos pessoais, invadindo área que deveria ficar restrita à sua intimidade; ao mesmo tempo, o cidadão objeto dessa indiscriminada colheita de informações, muitas vezes, sequer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, retificá-lo ou cancelá-lo. E assim como o conjunto dessas informações pode ser usado para fins lícitos, públicos e privados, na prevenção ou repressão de delitos, ou habilitando o particular a celebrar contratos com pleno conhecimento de causa, também pode servir, ao Estado ou ao particular, para alcançar fins contrários à moral ou ao Direito, como instrumento de perseguição política ou opressão econômica. A importância do tema cresce de ponto quando se observa o número imenso de atos da vida humana praticados através da mídia eletrônica ou registrados nos disquetes de computador. (STJ, 1995).

A tutela dos dados pessoais, em resumo, sugere a temática da privacidade, sendo que, todavia, altera os seus componentes, intensifica suas diretrizes e atinge os pontos precípuos dos interesses em voga.

3.3 A Lei Geral de Proteção de Dados

O Brasil avocou para si uma tarefa de protagonista nos debates desde o ano de 2013, ocasião em que a Presidenta Dilma Rousseff abordou o tema da espionagem internacional executada pelos Estados Unidos da América e solicitou um novo padrão de governança global na internet, em um plenário realizado na Organização das Nações Unidas (ONU, 2013).

Portanto, o direito de tutelar suas informações privadas constitui um direito reivindicado pelo Estado brasileiro, principalmente no ciberespaço. A governança em múltiplos setores é, fundamentalmente, a asseguração da liberdade de expressão, da observância aos direitos

humanos, da privacidade das pessoas e uma governança multissetorial no ciberespaço (PINHEIRO, 2021).

Na situação da conjuntura brasileira, a legislação de tutela de dados pátria se originou com o Projeto de Lei Complementar nº 53 de 2018, sendo promulgada pelo então Presidente Michel Temer no mês de agosto do ano mencionado (BRASIL, 2018).

Em virtude da Lei nº 13.709 de 2018, foi iniciado o marco legal pátrio direcionado às instituições públicas e privadas, eis que a Lei Geral de Proteção de Dados, ou LGPD, assevera sobre a tutela dos dados pessoais das pessoas em qualquer vínculo que abarca o tratamento de informações que possam ser encaixadas enquanto dados pessoais, isto é, que estejam vinculadas a uma pessoa natural identificada ou passível de identificação e que sejam tratadas em qualquer amparo ou meio, quer por pessoa física ou jurídica (PINHEIRO, 2021).

Trata-se de regulamentação encarada como sendo técnica e que acarreta mais do que regramentos e norteamentos, já que carrega direitos, princípios e obrigações atinentes à utilização de bases de dados pessoais, um importante ativo na sociedade hodierna (PINHEIRO, 2021). É relevante salientar que a finalidade da lei em comento é tutelar os direitos fundamentais de privacidade, liberdade e livre desenvolvimento da personalidade do indivíduo, através do pressuposto de boa-fé para toda espécie de tratamento de dados pessoais (PINHEIRO, 2021).

O texto da lei carrega vários itens e princípios de controles técnicos para atingir a governança devida da segurança das informações, de forma a garantir o cumprimento dos direitos previstos, sendo o enfoque do progresso de seu teor da tutela dos direitos humanos (PINHEIRO, 2021). A norma tem visível inspiração no Regulamento Europeu de Proteção de Dados Pessoais, sendo fracionada em 10 capítulos e contendo 65 artigos. Em comparação à legislação europeia, a lei pátria é menor, já que aquela detém 11 capítulos e 99 artigos (PINHEIRO, 2021).

Em suma, tem-se: i) capítulo I – disposições preliminares, que compreende do artigo 1º ao artigo 6º; ii) capítulo II – do tratamento dos dados pessoais, que engloba o artigo 7º ao 16; iii) capítulo III – dos direitos do titular, que abrange dos artigos 17 ao 22; iv) capítulo IV – do tratamento dos dados pessoais pelo Poder Público, que elenca os artigos 23 ao 32; v) capítulo V - da transferência internacional de dados, que elenca o artigo 33 ao 36; vi) capítulo VI - dos agentes de tratamento de dados pessoais, que inclui o artigo 37 ao 45; vii) capítulo VII – da segurança e boas práticas, que abrange o artigo 46 ao 51; VIII) capítulo VIII – da fiscalização, que engloba o artigo 52 ao 54; ix) capítulo IX – Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, que envolve

□o □rtigo 55 □o 59; □x) c□pítulo X – das disposições finais e transitórias, que inclui o artigo 60 ao 65 (BRASIL, 2018).

Logo, a variante pátria é menor e em algumas partes concede uma interpretação mais abrangente, acarretando algumas acepções de insegurança jurídica, eis que autoriza espaço para sentido subjetivo em ocasiões que deveria ter mais objetividade. A título de exemplo, vale citar o que acontece no que cerne aos prazos: ao passo que o Regulamento Europeu de Proteção de Dados Pessoais determina prazos precisos, tais como 72, a lei brasileira fixa "prazo razoável" (PINHEIRO, 2021).

3.3.1 Autoridade Nacional de Proteção de Dados (ANPD)

Relevante verificar que a legislação ora comentada foi ulteriormente alterada pela Medida Provisória nº 869 de 2018, convertida na Lei nº 13.853/2019, que acarretava a elaboração da Autoridade Nacional de Proteção de Dados (ANPD), importantíssima no processo de acolhimento, uniformização e execução das normas (BRASIL, 2019). Sobre o tema, Danilo Doneda assevera:

> Assim, em 27 de dezembro de 2018, o Poder Executivo publicou a Medida Provisória n. 869/2018 166 , criando a Autoridade Nacional de Proteção de Dados (ANPD) e modificando uma série de outros pontos da lei. A estrutura proposta então era a da ANPD como um órgão público, formalmente localizado dentro da estrutura da Presidência da República (DONEDA, 2020, p. 312).

Cuida-se de um órgão pertencente à Administração Pública incumbido de zelar e instaurar a Lei Geral de Proteção de Dados em todo o Brasil. Neste sentido, detém a finalidade de tutelar os direitos fundamentais de privacidade e liberdade, bem como orientar, fiscalizar e propiciar a execução da LGPD, além de empregar punições em situações de ofensas ao tratamento de dados (PINHEIRO, 2019).

Sua organização foi fixada através do Decreto nº 10.474 de 26 de agosto de 2016. Em consonância com o determinado o órgão em comento fica sujeito à Casa Civil da Presidência da República, de forma que as nomeações ficam a cargo do presidente (BRASIL, 2020).

É salutar rememorar que a ANPD foi elaborada para auxiliar a tutelar o mercado e a instaurar a proteção de dados, em uma operacionalização de assegurar a execução e o proveito da lei, quer através de pareceres técnicos e normas complementares, quer por procedimentos relacionados à inspeção. Devido a isso, em um cenário ideal, haveria uma autoridade nacional

independente, com subsídios para atingir sustentabilidade e eficiência, tal como prevê o Regulamento Europeu de Proteção de Dados Pessoais (PINHEIRO, 2021).

Ademais, a lei em comento foi conjecturada com o intuito de conceder maior independência e robustecer a tutela da privacidade do titular dos dados. A garantia de transparência, segurança e respeito ao usuário foram os enfoques que orientaram as normas de regulamentação. Conceder funções de fiscalização e monitoramento a profissionais que não considerem a ótica da pessoa pode provocar decisões distantes e conflituosas ao objetivo da lei ora mencionada (PINHEIRO, 2021).

Noutro giro, existiu modificação pela Lei nº 14.010 de 2020, que procedeu à prorrogação do emprego das multas dispostas pelo artigo 52. Em virtude disso, salienta-se que, embora seja uma legislação recente, a Lei Geral de Proteção de Dados já passou por certas transformações importantes (BRASIL, 2020).

3.3.2 Adaptações

Através da sua entrada em vigor no ano de 2020, as organizações privadas, bem como as públicas precisaram rever processos e práticas para se harmonizarem com o tratamento e coleta de dados pessoais.

Em resumo, a Lei Geral de Proteção de Dados principia direitos aos titulares de dados (apropriação/modificação de dados, acesso à informação, revogação de consentimento, apagamento de dados), singulariza a ação e a incumbência dos agentes de tratamento (executar o tratamento dentro do objetivo e a adaptação necessária, com o conhecimento de que a desobediência acarreta punições que englobam advertências, multas simples limitadas a 50 milhões de reais por infração, multas diárias, extinção dos dados, bloqueio de dados, proibição plena da atividades concernentes ao tratamento de dados pessoais) e condições fundamentais para a execução do tratamento de dados de modo legítimo (consentimento informado do proprietário dos dados, objetivo adequado e indicado, minimização dos dados, acesso à informação, transparência das ações e garantias de privacidade e segurança dos dados (PINHEIRO, 2021).

A fim de instaurar o que está previsto na legislação, de forma a determinar uma governança de privacidade e tutela de dados sustentável, é imprescindível agir em três esferas: i) t□cnológic□(□mpr□go d□soluçõ□s); ii) gov□rn□nç□(r□v□li□ção d□polític□s □contr□tos); □ iii) educacional (treinamento e conscientização de equipes) (PINHEIRO, 2021). Nesse processo

de adaptações, em consonância com a ótica de Doneda, Mendes e Cueva, deve-se levar em consideração que:

> A LGPD, apesar de, como verificado, procurar sistematizar a problemática relacionada ao tratamento de dados pessoais e proporcionar um eixo em torno do qual a disciplina passa a se estruturar, não cumpre essa tarefa meramente com a absorção de elementos já presentes na nossa ordem jurídica. Na verdade, a lei apresenta diversos elementos novos que, por si sós, causaram certo impacto, o fato de consolidarem em uma normativa toda a matéria foi somente o primeiro deles: com a LGPD, passa a integrar o ordenamento toda uma nova série de institutos próprios da disciplina da proteção de dados, de direitos do titular, um enfoque novo de tutela dos titulares é proporcionado pelas regras de demonstração e prestação de contas (accountability), são considerados elementos que levam em conta o risco em atividades de tratamento de d□dos p□sso□is □muit□s outr□s (DONEDA; MENDES; CUEVA, 2020, p. 254-255).

Desta forma, a lei em estudo é encarada como sendo complexa e de elevado impacto, eis que determina vários procedimentos especiais, bem como reafirma princípios que já estiveram dispostos em outras leis, tais como o Marco Civil da Internet e a Constituição Federal vigente (BRASIL, 1988).

Outrossim, existe a necessidade de executar uma intensa compatibilização com legislações em vigência, tais como a Lei de Acesso à Informação, que exige um labor meticuloso de adaptação, sobretudo na seara pública. Além disso, na situação específica da Administração Pública, é importante que exista atenção com o capítulo IV, mormente a partir do artigo 23, na ocasião em que fica determinado que o tratamento de dados pessoais é disciplinado pelo princípio da transparência e o fundamento legal que legitima o emprego das informações pelas entidades públicas é o acossamento do interesse público, restrito ao objetivo público e consonante com as competências da entidade (PINHEIRO, 2021).

3.3.3 Controlador, operador e encarregado de dados

Outro ponto relevante da lei são as novas definições e atribuições determinadas no artigo 5º: i) controlador (pessoa jurídica, de direito privado ou público, ou natural, a quem incumbem □s d□cisõ□s □tin□nt□s □o tr□t□m□nto d□ d□dos p□sso□is); ii) op□r□dor (pessoa jurídica, de direito privado ou público, ou natural, que executa o tratamento de dados pessoais em nome do control□dor; □iii) □nc□rr□g□do de dados (pessoa apontada pelo operador e controlador para atuar

enquanto canal de comunicação entre os titulares dos dados, o controlador e a Autoridade Nacional de Proteção de Dados (BRASIL, 2018). O encarregado de dados, também intitulado DPO, deve, antes de tudo, ser um indivíduo com autonomia para desempenhar função fiscalizatória dentro da organização. Ademais, deve possuir prerrogativas na qualidade de interlocutor com a ANPD (PINHEIRO, 2021).

Isto posto, sugere-se que seja um profissional com formação dotada de maior interdisciplinaridade, com ciência da nova legislação, entendimento acerca da governança de dados pessoais e de segurança da informação e que, contudo, tenha competência para se vincular enquanto porta-voz da organização diante das autoridades e dos titulares de dados, sobretudo na situação de reportar cenários de incidentes de ofensas a dados pessoais (PINHEIRO, 2021).

Por obra da majoração da quantidade de países acolhendo leis de privacidade de dados, o encarregado de dados é um dos profissionais mais enaltecidos e destacados da atualidade. No entanto, trata-se de um perfil em construção, que, preferivelmente, deve compilar habilidades jurídicas, técnicas e interpessoais (PINHEIRO, 2021). Assim, não existe ninguém plenamente preparado para este cargo, que carrega grande responsabilidade e demanda várias competências. Devido a isso, foi majorada a oferta de cursos de preparações e certificações para encarregado de dados, o que é apontado às pessoas que querem se imiscuir nessa carreira (PINHEIRO, 2021).

Na visão da autora, recomenda-se que tenha ciência sobre regulamentação, bem como experiência na execução de atividades que a norma particulariza como sendo particulares da função de encarregado, tais quais: i) receber comunicações e reclamações de clientes; ii) oportunizar esclarecimentos e validar providências; iii) recebar comunicação da Autoridade Nacional (ANPD); iv) ser interlocutor e porta-voz da entidade para resposta a incidentes concernentes à privacidade de dados; v) estruturar mecanismos de que modo e onde são empregados os dados dos clientes nas empresas; vi) executar auditorias para garantir que a utilização dos dados se coadune com os mandamentos legais; vii) nortear contratados e funcionários da organização no que tange às práticas de tutela de dados pessoais, sendo um propagador da temática; e viii) realizar outras atribuições fixadas pelo controlador ou determinadas em regras complementares (PINHEIRO, 2021).

A figura do encarregado de dados é efetivamente indispensável enquanto um profissional que concentra o debate acerca da harmonia à nova legislação e orienta a instauração de otimizações, bem como acompanha o progresso da temática junto à entidade, à sociedade e ao mercado (PINHEIRO, 2021).

Cuida-se de uma atuação importante no estágio de adequação e nas atualizações ulteriores, eis que a regulamentação necessitará progredir e se sujeitará a contextualizações em consonâncias com o cenário de cada setor (PINHEIRO, 2021). Uma nova conjuntura demanda uma nova posição e uma grande alteração de cultura, com consequências econômicas e sociais que exigem o amparo e a mediação de um encarregado nas entidades (PINHEIRO, 2021).

Além disso, as entidades devem estar preparadas para o emprego das tarefas de operador e controlador, dois papéis que acarretam responsabilidades particulares dentro da gestão. Catalogados enquanto agentes de tratamento, o controlador é o incumbido de tomar decisões concernentes ao tratamento de dados pessoais, ao passo que o operador é encarregado da execução do tratamento dos dados pessoais a mando do controlador (PINHEIRO 2021). Nas ocasiões em que existe o enquadramento de controlador, os que atuam na organização se sujeitam a essa ligação. Semelhantemente ocorre com o profissional liberal que, no desempenho de suas funções (na qualidade de pessoa física), cuida de dados pessoais e necessita respeitar as normas legais (PINHEIRO, 2021).

Todos os que detêm controle acerca dos dados pessoais no decorrer do seu ciclo de vida, que procedem ao tratamento de dados pessoais com autonomia, através de relacionamento autônomo com o titular, são encarados como controladores (PINHEIRO, 2021). Em situações de incidentes, para fins de exemplificação, é obrigação da entidade reportar os acontecimentos que abarquem ofensa a dados pessoais pelos usuários. O encargo da demonstração das evidências é da entidade que executa o tratamento dos dados pessoais, incidindo, a princípio, sobre o controlador dos dados, incluindo o tempo em que ficou armazenado e a ocasião do descarte (PINHEIRO, 2021).

O operador, por seu turno, presume um novo vínculo, não determinado com o titular, mas com o controlador, comumente através de terceirização, subcontratação ou transferência de atividade. A atuação do operador se sujeita ao controlador e acarreta incumbências específicas que incidirão sobre ele de modo direto, incluindo por meio de solidariedade, tal como prevê o artigo 42 da LGPD (BRASIL, 2018).

Constitui uma efetiva jornada de adequações em favor de se assegurar uma maior tutela dos dados pessoais. Desta maneira, as entidades privadas e públicas detêm a responsabilidade de informar ao usuário, de modo acessível e simplificado, a ocasião em que o dado pessoal é angariado, o seu objetivo e o tempo em que será utilizado (PINHEIRO, 2021).

É imprescindível que se parta de um programa de harmonização para executar as adequações indispensáveis que detenham quatro sustentáculos: gestão, controle, transparência,

administração de aquiescência (ou sua realização) e segurança dos dados pessoais (PINHEIRO, 2021).

Nesta esteira, deve-se conjecturar a gestão de dados de forma a elaborar um ambiente benéfico à compreensão do cidadão, a fim de que não se tenha obstáculos caso se almeje ter ciência das informações coletadas, suas finalidades e os meios para que sejam consolidados os direitos preconizados nos artigos 18 e 19 da Lei Geral de Proteção de Dados (BRASIL, 2018).

Neste diapasão, é de suma importância que o usuário compreenda quais dados a entidade possui, a forma pela qual eles são utilizados e atua para tutelá-los. No cotidiano das pessoas, estes regramentos, empregos e desvios abarcando bases de dados pessoais, que podem se dar na forma de perfis falsos em redes sociais ou delitos cometidos no meio digital (BRASIL, 2018).

4 DOS ATOS ILÍCITOS COMETIDOS NO CIBERESPAÇO E SEU COMBATE

Pode-se asseverar que o Brasil é o segundo país com maior quantidade de casos de delitos cibernéticos, impactando aproximadamente 62 milhões de indivíduos e acarretando um prejuízo de US$ 22 bilhões, tal como verificou um relatório emitido pela Norton Cyber Security no ano de 2017 (TILT, 2018). Todavia, esse exacerbado problema não sobrevive apenas em alguns países, eis que a tecnologia é mundialmente aplicada para emprego de comportamentos delituosos. Nesta seara, vários são os crimes praticados no ciberespaço (MÁXIMO, 2015).

Isto posto, essa facilidade no cometimento de crimes no meio virtual se deve ao fato de que se trata de uma ferramenta de simples acesso e utilização descomplicada, em que o autor do delito não se expõe fisicamente, falseando sua identidade por intermédio de um computador ou celular (MÁXIMO, 2015). Acerca da temática:

> A informatização crescente das várias atividades desenvolvidas individual ou coletivamente na sociedade veio colocar novos instrumentos nas mãos dos criminosos, cujo alcance ainda não foi corretamente avaliado, pois surgem a cada dia novas modalidades de lesões aos mais variados bens e interesses que incumbe ao Estado tutelar, propiciando a formação de uma criminalidade específica da informática, cuja tendência é aumentar quantitativamente e, qualitativamente, aperfeiçoar os seus métodos de execução (FERREIRA, 2000, p. 129).

No que tange aos crimes passiveis de prática no ciberespaço, Ramos elucida que são: i) homicídio, em que o delinquente invade o computador da Unidade de Terapia Intensiva de um hospital e modifica os remédios de um determinado paciente, de forma que o profissional da saúde pode mata-lo em razão da dosagem equivocad□; ii) d□litos contr□□honr□: c□lúni□, injúri□ ou dif□m□ção com□tidos por int□rmédio d□ sit□s □r□d□s soci□is; iii) instig□ção □ suicídio realizado por intermédio de mensagens instantâneas ou e-m□ils; iv) furto: subtr□ção d□dinh□iro por m□io d□□plic□tivos □sit□s d□instituiçõ□s fin□nc□ir□s; v) □st□lion□to: utiliz□ção d□C□d□stros d□P□sso□s Físic□s □c□rtõ□s d□créditos f□lsos □fim d□□x□cut□r compr□s p□lo m□io virtu□l; vi) violação de direito autoral por intermédio da cópia de músicas, fotos, livros, softwares, dentre outros; vii) divulg□ção d□pornogr□fi□inf□ntil; viii) f□vor□cim□nto d□prostituição; ix) tráfico de armas e drogas através do meio virtual (RAMOS, 2009).

Para além da detecção do crime, é necessário que as autoridades e operadores do Direito em geral estejam habilitados a apurar e punir os delitos cometidos no ciberespaço. Neste sentido, é indispensável a cooperação dos provedores na apuração, primando pela ética e

interesse público. Desta maneira, este capítulo tratará do conceito de cibercrimes, da legislação a eles aplicada, das providências ineficientes atualmente empregadas para a sua solução e, posteriormente, o que deve ser realizado no que cerne aos operadores do Direito para que a diminuição de sua incidência.

4.1 Conceito e legislação aplicada aos crimes cibernéticos

Vários foram os termos elaborados com o fito de acarretar tipicidade aos atos ilícitos realizados no meio virtual. Pode-se citar as seguintes nomenclaturas: crimes virtuais, crimes digitais, delitos cibernéticos, crimes de alta tecnologia, crimes informatizados, etc.

> O crime eletrônico é, em princípio, um crime de meio, isto é, utiliza-se de um meio virtual. Não é um crime de fim, por natureza, ou seja, o crime cuja modalidade só ocorra em ambiente virtual, à exceção dos crimes cometidos por hackers, que de algum modo podem ser enquadrados na categoria de estelionato, extorsão, falsidade ideológica, fraude, entre outros. Isso quer dizer que o meio de materialização da condut□ criminos□ pod□ s□r virtu□l; contudo, □m c□rtos c□sos, o crim□ não (PINHEIRO, 2021, p. 223).

Rossini (2004, p. 125) esclarece que delitos informáticos seria a melhor nomenclatura:

> Ouso denominá-los “delitos informáticos”, pois dessa singela maneira abarcam-se não somente aquelas condutas praticadas no âmbito da internet, mas toda e qualquer conduta em que haja relação com sistemas informáticos, quer de meio, quer de fim, de modo que essa denominação abrangeria, inclusive, delitos em que o computador seria uma mera ferramenta, sem a imprescindível “conexão” à Rede Mundial de Computadores

Nesta esteira, o referido autor explana que os delitos informáticos seriam gênero, de maneira que crime cibernético ou crime telemático seriam espécies, se aludindo apenas aos crimes executados especialmente na seara da internet (ROSSINI, 2004). Resolvida questão da conceituação, vislumbra-se que no Brasil, similarmente ao que ocorre em outros países, o ordenamento jurídico perpassa por contínua atualização, ocasionada pela alteração e progresso da sociedade. Emergem novas situações, novos comportamentos e valores, o que acarreta uma dinâmica logica do Direito, a fim de que se conserve acolhedor à conjuntura socioeconômica de cada época (PINHEIRO, 2021).

Desta forma, a lei n° 12.737 de 2012 é a incumbida de regulamentar os delitos cibernéticos (BRASIL, 2012). De acordo com Pinheiro, a referida lei ainda é intitulada “Lei Carolina Dieckmann”, eis que foi em virtude de um vazamento de fotos armazenadas no computador da atriz que a legislação foi aprovada.

> Desde 1999 o Brasil discutia o Projeto de Lei de Crimes Eletrônicos71, e nem os ataques das quadrilhas fizeram o projeto andar, como fez o efeito “Carolina Dieckmann”, em que o vazamento de fotos íntimas de uma celebridade trouxe à tona novamente a importância de se aprovar uma lei como esta. Isso porque a liberdade de um vai até onde não fira o direito de outro (PINHEIRO, 2021, p. 78).

No âmbito da lei em comento, foi tipificado o delito de utilização de dados de cartões de débito ou crédito angariados de modo indevido ou sem aquiescência do seu titular legítimo, equiparando essa conduta ao crime de falsificação de documento particular (PINHEIRO, 2021). Ademais, a mesma legislação elevou ao status de delito a invasão a dispositivos eletrônicos de outrem conectados ou não à internet, tais quais notebooks, computadores, celulares, caixas eletrônicos ou tablets, com a finalidade de angariar ou modificar dados no sistema e obter uma vantagem ilícita (PINHEIRO, 2021).

Além disso, foi determinada a mesma pena do delito de invasão ao crime de produzir, oferecer ou vender programas de computadores que possibilitem a invasão. Outrossim, a pessoa que angariar informações sigilosas ou ofender segredos comerciais ou comunicações eletrônicas privadas, tais quais conteúdos de e-mails ou senhas, obterá uma pena maior (PINHEIRO, 2021). Outra alteração foi a criminalização do comportamento de interromper, de maneira intencional, o serviço de internet de utilidade pública, que constituiria o ato de tirar do ar sites de serviços públicos ou semelhantes, comumente praticado por hackers (PINHEIRO, 2021).

Na visão de Ramos Júnior, a inexistência de conceituação legal de várias expressões e termos empregados na norma penal é um grande desafio a ser confrontado no emprego da lei, eis que há a necessidade de elucidar o que se compreende por dispositivo informático, ferramenta de segurança, invasão, fragilidades, autorização tácita, dentre outros (RAMOS JÚNIOR, 2013). Ao passo que isso não acontece, a fim de resolver essa temática, reflete-se que é possível a sua dimensão aos dispositivos que operam por computação em nuvem. No que cerne à ferramenta de segurança, leva-se em consideração que sua definição não pode ser limitada a somente alguns modos de tutela, devendo abranger toda ferramenta computacional,

englobando antivírus, senhas e a tecnologia moderna de vislumbre de invasões, intrusões e ataques de cunho cibernético (RAMOS JÚNIOR, 2013).

Nesta esteira, também se pôde vislumbrar outras atualizações da legislação no que cerne à internet, tendo em vista que foram modificados o Código de Processo Civil (utilização de assinatura através de certificado digital), o Código de Processo Penal (delitos digitais em detrimento da Administração Pública), o Estatuto da Criança e do Adolescente (delito de pedofilia), bem como foram elaboradas leis concernentes a lan houses e ciber cafés (PINHEIRO, 2021).

Contudo, percebe-se que o Brasil é mais deficiente no que cerne à capacitação das autoridades e operadores do Direito atinentes à investigação (ferramentas técnicas, agilidade, treinamento, dentre outras) (PINHEIRO, 2021).

4.2 Problemas e providências a serem tomadas no combate a delitos cibernéticos

Se valendo de um exame entre o anseio que o indivíduo tem em realizar condutas delituosas na seara virtual, é imprescindível que as formas de amparar e represar a ciber criminalidade se mostra insuficiente. Hodiernamente, é relevante vislumbrar no Brasil o baixo número de delegacias específicas em delitos virtuais. Não há delegacias especializadas em boa parcela do país, ao passo que é crucial existir uma delegacia desta espécie em cada estado federativo. Um estudo executado pela BandNews FM dá conta de que 34% das capitais pátrias não detêm delegacias especializadas em delitos cibernéticos (BANDNEWS FM, 2021).

O combate a esses delitos também se torna bastante complexo por duas razões: i) a ausência de conhecimento do usuário, que, desta maneira, não repassa às autoridades dados pr□cisos □ import□nt□s; □ ii) □usênci□ d□ r□cursos □m g□r□l d□s □utorid□d□s polici□is (PINHEIRO, 2021).

O maior incentivo aos delitos virtuais se baseia na crença de que o ciberespaço é um âmbito marginal, onde a ilegalidade é soberana. Essa conduta é efetiva porque a sociedade não crê que a seara é vigiada de maneira eficaz, bem como que os crimes nela cometidos são devidamente punidos (PINHEIRO, 2021). O compilado lei e punição é indispensável na seara digital, tal como ocorre na conjuntura real. Se existir essa ausência de crédito na habilidade punitiva da coletividade digital, os delitos serão majorados e os negócios pactuados neste meio serão desestimulados (PINHEIRO, 2021).

Compreende-se que existem três motivos para a majoração de delitos digitais: i) majoração dos usuários de internet e demais formas eletrônicas, sobretudo no que tange às

classes sociais menos abastadas, que são vítimas fáceis, eis que ainda não detêm conhecimento d□ utiliz□ção m□is s□gur□; ii) qu□nto m□is indivíduos no m□io digit□l, os d□linqu□nt□s profissionais também se deslocam, e, assim, existe um maior acontecimento d□ d□litos; iii) ausência de conscientização em segurança da informação, o que acarreta que a maior parcela dos indivíduos crê que nunca ocorrerá com ela, deixa o computador ligado e desprotegido, empresta senhas, não se preocupa em utilizar mecanismos de segurança e, ainda, aliado a uma dose de inocência que intensifica as ocorrências (PINHEIRO, 2021).

Ao se executar uma análise sobre as deficiências relacionadas às medidas preventivas e de repressão aos atos criminosos no ciberespaço, é viável notar as mais importantes, que serão tratadas a seguir.

Em nível emergencial, a fim de otimizar o estágio de tutela dos dados dos indivíduos brasileiros, bem como do ente público, são: i) revisar o estágio de segurança das informações dos sites governamentais, otimizando a programação de códigos-fonte, além da criptografia de b□s□ d□d□dos; ii) inst□ur□ção do pl□no d□ continuid□d□ □contingênci□ □outr□s m□did□s, d□ m□n□ir□□□ vit□r int□rrupçõ□s; iii) □x□cut□r monitor□m□nto p□r□ n□no □mbi□nt□ virtu□l, pod□ndo se valer de estratégias para capturar o ataque em seu princípio □id□ntific□r □□utori□; □l□bor□r polici□m□nto onlin□(não som□nt□ inst□l□r m□is d□l□g□ci□s □sp□ci□liz□d□s); iv) □prov□ção d□ leis que otimizem a tipificação e armazenamento de provas, devendo acarretar novas espécies de delito eletrônico, guerr□ cib□rnétic□ □cib□rt□rrorismo; v) d□t□rmin□r p□drão d□ id□ntid□d□ digital imposto e prazo mínimo de armazenamento de dados de tráfego e conexão por prov□dor□s d□ int□rn□t; págin□s d□ cont□údo, □-m□il □r□d□s soci□is; vi) inst□ur□r c□mp□nh□ d□ conscientização de segurança da informação pública, destinada a cidadãos e servidores, norteando acerca da tutela da senha, necessidade de desligar o equipamento fora dos momentos de uso, bloqueio da estação de labor e de conservar atualizados os softwares de antivírus (PINHEIRO, 2021).

4.3 A importância do investimento em operadores do Direito no combate a ilícitos cometidos no meio virtual

A investigação de delitos mais comuns na sociedade, tais quais tráfico de entorpecentes, roubo e homicídios, já é bastante complexa de se realizar, mesmo que se verse de ofensa comum e há muito tempo impacta a realidade brasileira (NASCIMENTO, 2022). Devido a este contexto, deve-se fomentar a educação dos operadores do Direito. Em consonância com Patrícia Pinheiro, deve-se investir em capacitação e mecanismos tecnológicos que autorizem,

efetivamente, a executar investigações indispensáveis na solução dos delitos digitais e na sanção dos autores (PINHEIRO, 2021).

Apenas com campanhas de conscientização robustas, treinamento e acolhimento de aulas de "ética e cidadania digital" enquanto disciplina obrigatória na grade da graduação em Direito, pode-se criar um operador dotado de maior ética e hábil a combater significativamente, o delito eletrônico em seu nascedouro, eis que em vários contextos há determinado desconhecimento, negligência e desatenção do operador enquanto simplificador do comportamento, ou, ainda, existe uma despreocupação com as normas, fomentando o delinquente cibernético (PINHEIRO, 2021).

Ademais, há o tema da territorialidade dos delitos digitais, o que pode acarretar grandes controvérsias. Como é sabido, o Direito Penal está sujeito a certo território nacional, o que extrapola ultrapassa o referido território está submetido à existência ou não de pactos entre os Estados soberanos envolvidos (PINHEIRO, 2021). Por isso,

> são submetidos à lei brasileira os crimes cometidos dentro da área terrestre, do espaço aéreo, e das águas fluviais e marítimas, sobre as quais o Estado brasileiro exerce sua soberania, pouco importando a nacionalidade do agente. Porém, nos dias atuais, o conceito de território para fins de aplicação da jurisdição deve englobar também o espaço virtual, com todos os serviços de Internet prestados no Brasil. (TOLEDO, 1991, p, 45)

Uma apuração bem realizada pode não alcançar a sanção do delito e realização do cumprimento de pena nas situações em que for constatado que o delinquente age de outro país e não for deferida a extradição dele ou seu julgamento no país em que ocorreu o delito. Já acontecem movimentações entre as várias diplomacias a fim de que sejam determinados regramentos internacionais de sanção de delitos pela internet (PINHEIRO, 2021). Domingos e Röder (2018, p. 35) chamam a atenção para a mesma possibilidade em se tratando de empresas que armazenam dados pessoais de indivíduos:

> Uma vez que tais empresas podem possuir sede física em um país, mas armazenar suas informações em servidores em qualquer local do planeta, os operadores do Direito depararam-se com a perplexidade de não saber qual local teria jurisdição para decidir acerca do fornecimento de tais dados. Além disso, cada país possui uma percepção peculiar acerca da proteção da privacidade, o que se reflete nas diferenças legislativas sobre requisitos para fornecimento de dados e conteúdo. Some-se a isso a volatilidade da prova digital, pois a enorme quantidade de informações em circulação no mundo faz com que a sua manutenção

> pelas empresas seja a menor possível, ditada pelos custos que o armazenamento de dados gera.

Neste sentido, percebe-se, ainda, que o operador do Direito no que tange aos crimes cibernéticos, deve, ainda, deter conhecimentos acerca de Direito Internacional, de maneira a saber o melhor modo de agir diante da prática de delitos que envolvem mais de um país.

No que diz respeito à origem da ação criminosa, esta será melhor descoberta nas ocasiões em que se otimizarem as ferramentas de identificação dos usuários. Contudo, esta é uma temática bastante polêmica, eis que a predisposição global é a determinação de um parâmetro de identidade digital obrigatória, eis que isso acarreta uma testilha direta com o anonimato provocado pela própria internet (PINHEIRO, 2021).

Neste diapasão, pode-se inferir que os indivíduos a riqueza e as empresas estão se mudando para a seara virtual, e é natural que os atos ilícitos também. Portanto, o estudo interdisciplinar dos delitos cibernéticos é fundamental para o profissional do Direito, tendo em vista que cada vez mais será exigida a sua compreensão sobre a realização de atos ilícitos no ciberespaço.

CONSIDERAÇÕES FINAIS

A internet é encarada por vários como a grande incumbida pelas alterações sociais nos últimos anos. Isso ocorre porque, em virtude da sua popularização, possibilitou a transformação de padrões em todos os estágios sociais, de forma que as informações correm o mundo todo de maneira célere. O mesmo ocorre com os dados pessoais dos indivíduos.

É sabido que a Constituição Federal pátria protege os dados pessoais por intermédio do direito à privacidade, à intimidade e à vida privada. Todavia, essa proteção se torna mais complexa devido ao fluxo de informações e à inserção dos dados dos indivíduos no ciberespaço.

Nesta esteira, o presente trabalho tencionou demonstrar que o direito à privacidade e a tutela dos dados pessoais no ciberespaço ainda é insuficiente na atualidade em função de vários fatores, tais quais: legislação apropriada, treinamento de operadores do Direito, investimento em ferramentas tecnológicas de investigação, monitoramento e controle, dentre outros, o que acarreta a majoração dos delitos cibernéticos.

As mais importantes leis acerca do tema não são suficientes para a prevenção desta espécie de crimes, além de que a repressão, em várias situações, é inexistente, dado os fatos e razões anteriormente esposados.

Isto posto, a esfera digital demanda uma regulamentação apropriada a fim de que a convivência nesta seara se dê de modo lícito e saudável a todos os indivíduos por ela alcançados. É imprescindível que exista confecção legislativa específica, clara, exata e objetivo acerca da temática, de modo que não é útil, nem almejável que se legisle acerca de tudo o que a lei não satisfaça aos objetivos que se tenciona.

Ademais, é imprescindível que os órgãos de investigação sejam regularmente equipados com equipe técnica devidamente atualizada e qualificada e material moderno, bem como deve existir fomento de forma a se prevenir o acontecimento de crimes, não somente se represar o mau acarretado.

É indubitável os progressos provocados pela internet e pelo aparato técnico que possibilita a sua aplicação. No entanto, as problemáticas enfrentadas não aparentam achar soluções no modo em que se tem aplicado empenho. Continuadamente, direitos são ofendidos com a divulgação de dados no meio virtual, e o ordenamento jurídico pátrio não traz a solução ao problema, o que explicita a necessidade de emprego das medidas já salientadas no decorrer do presente estudo, conclui-se que o mais importante a que se chega é a de que o tema precisa continuar a ser enfrentado, diante da imensa problemática que o envolve (os avanços tecnológicos) e que embora tenha havido avanços, ainda há muito a ser feito.

REFERÊNCIAS

AGNU. Assembleia Geral das Nações Unidas**. Declaração Universal dos Direitos Humanos de 1948**. Paris, 1948. Disponível em: <https://www.oas.org/dil/port/1948%20Declaração%20Universal%20dos%20Direitos%20Humanos.pdf>. Acesso em: 20 fev. 2023.

BANDNEWS FM. **34% das capitais brasileiras não possuem delegacias especializadas em crimes digitais**. 11/11/2021. Disponível em: <https://www.band.uol.com.br/bandnews-fm/noticias/34-das-capitais-brasileiras-nao-possuem-delegacias-especializadas-em-crimes-digitais-16459684>. Acesso em: 25 fev. 2023.

REPÚBLICA FEDERATIVA DO BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 21 fev. 2023.

_____. **Decreto nº 10.474, de 26 de agosto de 2020**. Disponível em: < https://legislacao.presidencia.gov.br/atos/?tipo=DEC&numero=10474&ano=2020&ato=433gXSU1UMZpWTbae>. Acesso em: 23 fev. 2023.

_____. **Lei nº 12.737, de 30 de novembro de 2012**. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 25 fev. 2023.

_____. **Lei nª 13.709, de 14 de agosto de 2018**. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 22 fev. 2023.

BRASIL. **Lei nº 13.853, de 8 de julho de 2019**. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm>. Acesso em: 22 fev. 2023.

_____. **Lei nº 14.010, de 10 de junho de 2020**. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14010.htm>. Acesso em: 23 fev. 2023.

_____. **Projeto de Lei da Câmara n° 53, de 2018**. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/133486#:~:text=Projeto%20de%20Lei%20da%20Câmara%20n°%2053%2C%20de%202018&text=Ementa%3A,23%20de%20abril%20de%202014.>. Acesso em: 22 fev. 2023.

CHAVES, C. F. O. A luta contra o terrorismo e a proteção de dados pessoais: Análise crítica de um precedente do Tribunal Constitucional Alemão (bundesverfassungsgericht). **Revista Brasileira De Direitos Fundamentais & Justiça**, 4(12), 284–293, 2010.

DOMINGOS, F□rn□nd□ T□ix□ir□ Souz□; RÖDER, Priscil□ Cost□ Schr□in□r. Obt□nção d□ prov□s digitais e jurisdição na internet. **Crimes cibernéticos**. 2ª Câmara de Coordenação e Revisão, Criminal. – Brasília: MPF, 2018. 275 p. – (Col□tân□□ d□□rtigos ; v. 3).

DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. -- 2. ed. -- São Paulo: Thomson Reuters Brasil, 2020.

DONEDA, D□nilo; MENDES, L□ur□ Sch□rt□; CUEVA, Ric□rdo V. B. **Lei Geral de Proteção de Dados**. São Paulo: Revista dos Tribunais, 2020.

FERRAZ JÚNIOR, Tercio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. Cadernos de Direito Constitucional e Ciência Política. São Paulo, **Revista dos Tribunais**, nº 1, 1992, p. 441.

FERREIRA, Iv□t□ S□nis□. A crimin□lid□d□ informátic□. In: D□ LUCCA, N□wton; SIMÃO FILHO, Adalberto (Coord.). **Direito e Internet**: aspectos jurídicos relevantes. Bauru: Edipro, 2000.

GIBSON, William. **Neuromancer**. São Paulo: Ed. Aleph, 2015.

GUIMARÃES JÚNIOR, Mário José Lopes. O ciberespaço como cenário para as Ciências Sociais. **Ilha Revista de Antropologia**, Florianópolis, v. 2, n. 1, p. 139-154, jan. 2000.

HUBMANN, Heinrich. **Das Persönlichkeitsrecht**, 2a. ed., Köln/Graz, 1967.

KUEHL, Daniel T. From cyberspace to cyberpower: defining the problem. In: KRAMER, Fr□nklin D.; STARR, Stu□rt H.; WENTZ, L□rry K. (□d.) **Cyberpower and national security**. Washington, DC, USA: National Defense University Press, 2009.

LÉVY, Pierre. **Cibercultura**. Trad. de Carlos Irineu da Costa. São Paulo: Ed. 34, 1999.

MACHADO, Felipe Nery Rodrigues. **Segurança da informação**: princípios e controle de ameaças. São Paulo: Editora Saraiva, 2019.

MARCONI, M. A; LAKATOS, E. V.. **Metodologia científica**. São Paulo: Editora Atlas, 2004.

MÁXIMO, Érica. A criminalidade aliada à tecnologia: uma abordagem acerca dos meios insuficientes para prevenção e repressão no ciberespaço. **Revista Juris Rationis**, Ano 8, n.2, p. 17-28, abr./set. 2015.

MENDOZA, Miguel Ángel. Cibersegurança ou segurança da informação? Explicando a diferença. Welivesecurity. 17 jan. 2017. Disponível em: <https://www.welivesecurity.com/br/2017/01/17/ciberseguranca-ou-seguranca-da-informacao/>. Acesso em: 20 fev. 2023.

MENESINI, Vittorio. Il problema giuridico dell'informazione, in: **Il diritto di autore**. ano LIV, n. 4, out.- dez. 1983.

NASCIMENTO, Stefalyne Pereira do. Direito à privacidade e crimes digitais: uma análise da proteção jurídica no ambiente virtual na legislação brasileira. **Conteúdo Jurídico**, Brasilia-DF: 01 jun 2022. Disponível em: <https://conteudojuridico.com.br/consulta/artigos/58546/direito-privacidade-e-crimes-digitais-uma-anlise-da-proteo-jurdica-no-ambiente-virtual-na-legislao-brasileira>. Acesso em: 25 fev. 2023.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Organização das Nações Unidas. **Dilma pede à ONU criação de marco internacional para regular internet**. 24/09/2013. Disponível em: < https://news.un.org/pt/story/2013/09/1450541>. Acesso em: 22 fev. 2023.

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

_____. **Direito digital**. – 7. ed. – São Paulo: Saraiva Educação, 2021.

POLESEL, Jussara de Oliveira Machado. **Cibersegurança, privacidade e proteção de dados pessoais no Brasil, à luz do direito comparado e dos standards internacionais de regulamentação** [recurso eletrônico]. Caxias do Sul, RS: Educs, 2021.

RAMOS, José Sérgio. **Responsabilidade civil dos provedores de internet**. 90 f. 2009. Monografia (graduação em Direito) submetida à Universidade do Vale do Itajaí – UNIVALI. Itajaí, 2009.

RAMOS JÚNIOR, Hélio Santiago. Invasão de dispositivo informático não é crime impossível. **Revista Consultor Jurídico**, 16 de novembro de 2013. Disponível em: <https://www.conjur.com.br/2013-nov-16/helio-junior-invasao-dispositivo-informatico-nao-crime-impossivel>. Acesso em: 25 fev. 2023.

RODOTÀ, Stefano. **Elaboratori elettronici e controllo sociale**. Bologna: Il Mulino, 1973.

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

SILVA, José Afonso da. **Curso de direito constitucional positivo**. - 39. ed., rev. e atual. até a Emenda Constitucional n. 90, de 15.9.2015. São Paulo: Malheiros, 2016.

SMITH, Robert Ellis. **Ben Franklin's web site**. Providence: Privacy Journal, 2000.

SUPERIOR TRIBUNAL DE JUSTIÇA. **Recurso Especial n° 22.337/RS**, rel. Min. Ruy Rosado de Aguiar, DJ 20/03/1995.

TILT. **Brasil é o segundo país no mundo com maior número de crimes cibernéticos. Uol. São Paulo:** 15/02/2018. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2018/02/15/brasil-e-o-segundo-pais-no-mundo-com-maior-numero-de-crimes-ciberneticos.htm>. Acesso em: 25 fev. 2023.

TOLEDO, Francisco de Assis. **Princípios Básicos de Direito Penal.** São Paulo: Ed. Saraiva, 1991.

WACKS, Raymond. **Personal information**. Oxford: Clarendon Press, 1989.