REVISTA BRASILEIRA DE FILOSOFIA E HISTÓRIA
ISSN:2447-5076

A efetivação dos direitos fundamentais no uso da inteligência artificial

The realization of fundamental rights in the use of artificial intelligence

Aurislene Olegario de Morais Barros [1]

Aceito para publicação em: 03/04/2024

Área do conhecimento: Direito

DOI: 10.18378/rbfh.v13i2.10452

RESUMO: A Inteligência Artificial está transformando rapidamente vários aspectos de nossas vidas, desde saúde até finanças, educação e entretenimento, mas também pode representar riscos significativos para os nossos direitos fundamentais. Os direitos fundamentais são os direitos e liberdades básicos a que cada indivíduo tem direito, independentemente da sua raça, gênero ou posição social, sendo essenciais para proteger a dignidade humana e promover a justiça social. Estão consagrados em leis nacionais e internacionais, como a Declaração Universal dos Direitos Humanos e a Convenção Europeia dos Direitos Humanos. A relação entre os direitos fundamentais e a inteligência artificial é complexa, uma vez que os sistemas podem reforçar e ameaçar os direitos fundamentais. É importante salientar que a aplicação dos direitos fundamentais na utilização é crucial para garantir que a inteligência artificial beneficia todos e não perpetua os preconceitos e a discriminação existentes. Os desafios na aplicação dos direitos fundamentais na utilização exigem uma abordagem multifacetada que inclua o reforço dos quadros jurídicos, o desenvolvimento de orientações éticas e a incorporação de mecanismos humanos de supervisão e responsabilização. Ao fazê-lo, podemos garantir que a inteligência artificial é desenvolvida e utilizada de forma responsável e ética, respeitando os direitos fundamentais. Por isso, o objetivo do estudo é explorar o conceito de direitos fundamentais no contexto da inteligência artificial, demonstrar os desafios na sua aplicação e analisar as abordagens para aplicá-los no uso da inteligência artificial.

Palavras-chave: Dignidade humana; Direitos fundamentais; Inteligência artificial.

ABSTRACT: Artificial Intelligence is rapidly transforming many aspects of our lives, from health to finance, education and entertainment, but it can also pose significant risks to our fundamental rights. Fundamental rights are the basic rights and freedoms to which every individual is entitled, regardless of their race, gender or social position, and are essential for protecting human dignity and promoting social justice. They are enshrined in national and international laws, such as the Universal Declaration of Human Rights and the European Convention on Human Rights. The relationship between fundamental rights and artificial intelligence is complex, since systems can both reinforce and threaten fundamental rights. It is important to stress that the application of fundamental rights in use is crucial to ensure that artificial intelligence benefits everyone and does not perpetuate existing prejudices and discrimination. The challenges in enforcing fundamental rights in use require a multi-faceted approach that includes strengthening legal frameworks, developing ethical guidelines and incorporating human oversight and accountability mechanisms. In doing so, we can ensure that artificial intelligence is developed and used responsibly and ethically, respecting fundamental rights. Therefore, the aim of the study is to explore the concept of fundamental rights in the context of artificial intelligence, demonstrate the challenges in applying them and analyze approaches to applying them in the use of artificial intelligence.

Keywords: Human dignity; Fundamental rights; Artificial intelligence.

[1] Graduada em Direito pela Faculdade Integrada de Patos, Paraíba; Especialista em Ciências Criminais e Segurança Pública pela Faculdade Integrada de Patos, Paraíba; Mestranda em Direito Constitucional pela UniBrasil; Procuradora de Carreira do Município de Carpina-PE.

INTRODUÇÃO

Nos últimos anos, tem-se observado que os dados pessoais estão cada vez mais valiosos e, consequentemente, mais difíceis de serem protegidos. Em especial, após o surgimento da pandemia, houve um grande aumento da utilização de serviços digitais como as redes sociais, lojas virtuais, *internet banking* etc., fazendo parte do cotidiano de milhares de pessoas a navegação na *internet.* É de suma importância ressaltar que, uma vez que aumentou o número de usuários na rede virtual, expandiu-se também, em contrapartida, o número de dados armazenados pelos sistemas[2].

Com tantos novos integrantes e dados expostos na *web*, verifica-se a vulnerabilidade perante os diversos riscos de ataques e vazamento de dados pessoais no âmbito digital. Em um debate feito por Carloto[3], analisando dois grandes vazamentos de dados ocorridos pelas redes sociais, no caso do *Facebook* e *Twitter*, o autor salienta que em ambos os casos, os vazamentos se deram em virtude do uso indevido das informações pessoais dos usuários, rompendo a privacidade, além de concentrar o poder de controle dos dados pessoais a terceiros, função que deveria ser exercida pela própria empresa.

Como se verifica, a *internet* é um extenso ramo digital que propicia diversas facilidades e recursos para a realização das mais diversas atividades, contudo, necessita de um órgão protetor que seja uma autarquia independente, a fim de que os usuários presentes nela possam ser protegidos e resguardados em casos de ataques aos dados pessoais, abrangendo o próprio usuário e até mesmo grandes empresas e órgãos. Em meio a constante insegurança que há no espaço digital, resta claro a importância da criação da LGPD para dispor sobre condutas e normas a despeito do tema. Contudo, apesar das melhorias dos dispositivos de proteção instaurados pela lei, se observa que ainda não foi atingido todo o potencial que a lei tem a oferecer, seja através de dispositivos mais claros e precisos e órgãos independentes para atuar na proteção direta dos dados pessoais[4].

A inteligência artificial (IA) é uma tecnologia de processamento de linguagem natural que utiliza algoritmos avançados de aprendizado de máquina para gerar respostas coerentes e

[2] LIETZ, Bruna. O uso da inteligência artificial e a fiscalização dos contribuintes na perspectiva dos direitos e deveres da relação tributária. 2021.
[3] CARLOTO, Selma et al. Lei Geral da Proteção de Dados Comentada: Com enfoque nas relações de trabalho. LTr Editora, 2021.
[4] SOARES, Marcelo Negri; MEDINA, Valéria Julião Silva. A inteligência artificial como instrumento de acesso à justiça e seus impactos no direito da personalidade do jurisdicionado. Revista de Direito Brasileira, v. 26, n. 10, p. 277-291, 2020.

relevantes em conversas com humanos. No entanto, a utilização da inteligência artificial na coleta e tratamento de dados pessoais pode trazer implicações éticas e legais que devem ser avaliadas com cuidado. Analisar as implicações éticas e legais do uso da inteligência artificial na coleta e tratamento de dados pessoais no contexto do Direito Civil brasileiro, identificando desafios e oportunidades e propondo soluções e diretrizes para garantir a proteção dos direitos fundamentais dos indivíduos, como a privacidade e a segurança dos dados pessoais[5].

A IMPLEMENTAÇÃO DA TECNOLOGIA NA SOCIEDADE HUMANA E A CRIAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) PARA A EFETIVAÇÃO DOS DIREITOS FUNDAMENTAIS

Com decorrer dos anos, criou-se mecanismos que facilitaram a acessibilidade a um vasto recurso informacional, decorrentes da implementação da tecnologia na sociedade humana, a qual vem proporcionando atividades em apenas um clique. Com isso, nota-se que em países mais desenvolvidos essas inovações emergiram mais cedo do que em outros lugares ao redor do mundo, levando, consequentemente, num primeiro momento, a busca para solucionar os problemas advindos dessa era digital. Apesar do meio digital facilitar o cotidiano de muitas pessoas, é considerável dizer que trouxe riscos consigo, pois, quando utilizado armazena informações pessoais de cada um que faz seu uso, e para assegurar a inviolabilidade dessas informações pessoais e coletivas.

Criou se mecanismos para resguardar todos os dados memorizados nele, dando início a projetos, regulamentos e leis, com o objetivo de proteger os direitos fundamentais de liberdade, de privacidade e o livre desenvolvimento da personalidade da pessoa natural. E um dos sistemas utilizados e atualmente aperfeiçoado foi inserção da Lei Geral de Proteção de Dados no ordenamento jurídico. A elaboração desta lei em âmbito nacional sofreu grande influência de regulamentos e tratados estrangeiros. Segundo Mendes e Doneda[6], a proteção de dados pessoais foi regulada primeiramente em regiões já desenvolvidas, como no caso dos Estados Unidos da America (EUA) e da União Europeia (UE), em razão dos grandes avanços informáticos terem se iniciado mais cedo nestes locais com a introdução da economia digital, consequentemente, houve a necessidade de se regulamentar a matéria para garantir a privacidade dos titulares,

[5] LIETZ, Bruna. O uso da inteligência artificial e a fiscalização dos contribuintes na perspectiva dos direitos e deveres da relação tributária. 2021.

[6] MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, 2020.

decorrente das possibilidade e dos primeiros riscos encontrados que pudessem atingir a dignidade e liberdade das pessoas.

Os Estados Unidos tiveram grande participação no contexto histórico global, sendo um dos primeiros países a dispor de normas sobre a proteção de dados. Conforme Mendes[7], o precursor do direito à privacidade foi o artigo intitulado de *The Right To Privacy*, escrito por Samuel Warren e Louis Brandeis publicado em 1890. Tal artigo iniciou a discussão sobre a proteção da privacidade dos indivíduos nos EUA e ganhou força em outros países com o passar dos anos, conforme novas demandas de mecanismos iam surgindo para proteger as informações das pessoas, diante das inovações dos meios de veiculação e armazenamento de dados.

Em razão do progresso tecnológico, os EUA objetivaram readequar o seu ordenamento jurídico de modo que passou a delimitar normas quanto a proteção da privacidade. Em 1973, esclarece Mendes e Doneda[8] que devido ao relatório gerado pelo Departamento de Saúde, Educação e Bem-Estar verificou-se a necessidade da criação de uma lei específica para tratar sobre a segurança dos dados, onde foram instituídos princípios que prevaleceram até a atualidade em diversos modelos de leis que regulam as informações pelo mundo.

No ano de 2016 foi criado na União Europeia o Regulamento Geral de Proteção de Dados (RGPD), com o objetivo de regulamentar as práticas e condutas dos responsáveis pelo tratamento de dados dos europeus para assegurar a proteção da privacidade das informações. Este regulamento em especial serviu de forte inspiração na construção da lei brasileira acerca do tema, abarcando direitos fundamentais já existentes desde a Declaração Universal Dos Direitos Humanos de 1948, reforçando a importância da inviolabilidade das garantias individuais.

A primeira lei sobre proteção de dados a ser constituída de fato, se deu na época de 1970 na Alemanha. Conhecida por lei do Estado alemão de Hesse, passou a tratar a matéria de forma autônoma e criteriosa. Partindo da lei alemã, os demais países começaram a preparar seus próprios regimentos quanto ao tema. No Brasil, antes de haver a presença de uma legislação própria, a garantia dos dados pessoais era regulamentada pelo código civil, código de defesa do consumidor, código penal e a Constituição Federal que prevê o princípio da dignidade da pessoa humana bem como a inviolabilidade de suas informações.

Em conformidade com Mendes e Doneda[9], é recente o uso do termo proteção de dados pessoais no âmbito brasileiro, o qual surgiu através de debates que antecederam a promulgação

---

[7] MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, 2020.
[8] Ibid.
[9] MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. Revista de Direito do Consumidor, 2020.

da LGPD. Este assunto, por muito tempo, foi associado ao direito do consumidor, da privacidade, liberdade individual e outros. A primeira iniciativa nacional que fez menção diretamente a proteção de dados, o qual assegurava o acesso à informação dos bancos de dados aos cidadãos e retificação, resultou no que se conhece hoje como *habeas data*.

No entanto, apesar de introduzir o *habeas data* na Constituição Federal de 1988, ele não prosperou no sentido de representar o direito de proteção de dados pessoais. A partir de então, muitos debates foram feitos acerca da matéria em busca de novas normativas. Neste sentido, se observa que alguns dispositivos posteriores já continham normativas genéricas que abrangiam o assunto, como no caso do código de defesa do consumidor que assegura as informações contidas dos clientes em bancos de dados, conforme disposto no art. 43 do referido código, mas, não preveu expressamente sobre a conduta dos responsáveis pelos tratamentos de dados.

Posteriormente, foi aprovado o Marco Civil da Internet, Lei nº 12.965/2014 que implementou vários direitos e procedimentos relacionados ao uso de dados pessoais, resultando em seguida, na elaboração da Lei Geral de Proteção de Dados. A Lei n. 13.709/2018 foi criada em 14 de agosto de 2018, composta por 65 artigos, e alterada pela Medida Provisória 869/2018 e pela Lei n. 13.853/2019. A elaboração da lei brasileira sobre a proteção de dados pessoais passou por todos estes marcos históricos contidos ao longo de experiencias de diversos países, tendo como principal fonte de influencia o regulamento europeu, contendo algumas semelhanças. Além do contexto internacional, a LGPG se consolidou também através de leis e normativas esparsas que já existiam no ordenamento brasileiro, realizando a junção delas em um único texto com um objetivo que é a proteção dos dados pessoais[10].

Compreende-se sobre proteção de dados todos os meios utilizados para resguardar a privacidade, a liberdade e o livre desenvolvimento da personalidade da pessoa natural, em face da pessoa jurídica. Em conformidade com Violla (2020), a terminologia proteção de dados parte do pressuposto de que todo dado pessoal é importante e possui valor definido por informações de pessoa natural identificável ou identificada.

Ressalta Lima[11], que a de proteção de dados nada mais é que a proteção da pessoa humana, visto que são conjuntos de informações que compõem os perfis ou as identidades digitais, aponta ainda que os dados pessoais possui caráter personalismo, pois é

[10] ____ Lei nº 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 06 de maio de 2023.

[11] LIMA, Cíntia Rosa Pereira de. Autoridade Nacional de Proteção de Dados e a Efetividade da Lei Geral de Proteção de Dados. São Paulo: Grupo Almedina, 2020.

regido pela identificabilidade e pela determinabilidade do seu titular, enquanto os dados sensíveis correspondem a origem racial e étnica, as convicções políticas, ideológicas, religiosas, as preferências sexuais, os dados genéticos e os biométricos.

Com criação da lei n. 13.709/2018 veio uma diversificação de elementos que passaram a fazer parte do ordenamento jurídico, com uma série de institutos próprios, os quais levam em conta o risco em atividades de tratamento de dados pessoais. E para garantir e proteger as relações sociais no âmbito digital, a LGPD apresenta em sua estruturação onze princípios fundamentais no seu artigo 6º, sendo eles: finalidade; adequação; necessidade; livre acesso; qualidade dos dados; transparência; segurança; prevenção; não discriminação; responsabilização e prestação de contas. Embora a lei apresente uma vasta concepção principiológica, verifica-se que para a segurança das relações sociais no âmbito digital de forma transparente e clara, nenhum dos princípios apontado, poderá de forma isolada garantir a proteção dos usuários e nem ao menos regulamentar aqueles que realizam a coleta de dados no Brasil[12].

Os direitos fundamentais são direitos humanos básicos essenciais para a proteção e preservação da dignidade humana. Esses direitos incluem o direito à privacidade, a liberdade de expressão e o direito à não discriminação. No contexto da IA, os direitos fundamentais são cruciais para garantir que a utilização da tecnologia não viola os direitos dos indivíduos. A relação entre os direitos fundamentais e a IA é complexa, uma vez que a IA pode tanto melhorar como prejudicar a proteção destes direitos. Por exemplo, a IA pode ser utilizada para melhorar os resultados dos cuidados de saúde e reduzir o preconceito nos processos de contratação, mas também pode perpetuar os preconceitos e a discriminação existentes[13].

Um desafio significativo na aplicação dos direitos fundamentais na utilização da IA é a falta de quadros jurídicos claros. O panorama jurídico da IA ainda está em evolução e há falta de clareza relativamente às responsabilidades jurídicas dos sistemas de IA e dos seus criadores. Além disso, responsabilizar os sistemas de IA por violações dos direitos fundamentais é um desafio, uma vez que os sistemas de IA podem ser complexos e difíceis de compreender. Além disso, a IA tem o potencial de perpetuar os preconceitos e a discriminação existentes, uma vez que pode aprender com conjuntos de dados e algoritmos tendenciosos[14].

---

[12] ____ Lei nº 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 06 de maio de 2023.

[13] SOARES, Marcelo Negri; MEDINA, Valéria Julião Silva. A inteligência artificial como instrumento de acesso à justiça e seus impactos no direito da personalidade do jurisdicionado. Revista de Direito Brasileira, v. 26, n. 10, p. 277-291, 2020.

[14] COSTA, Ramon Silva; KREMER, Bianca. Inteligência artificial e discriminação: Desafios e perspectivas para a proteção de grupos vulneráveis frente às tecnologias de reconhecimento facial. Revista Brasileira de Direitos Fundamentais & Justiça, v. 16, n. 1, 2022.

Para enfrentar os desafios da aplicação dos direitos fundamentais na utilização da IA, podem ser adotadas diversas abordagens. Uma abordagem consiste em reforçar os quadros jurídicos para a IA e os direitos fundamentais. Isto poderia envolver a criação de novas leis ou a alteração das existentes para garantir que os sistemas de IA sejam concebidos e utilizados de uma forma que respeite os direitos fundamentais. Outra abordagem é desenvolver diretrizes éticas para o uso da IA. Estas orientações poderiam delinear as melhores práticas para o desenvolvimento e implantação de sistemas de IA incluindo a necessidade de transparência, responsabilização e supervisão humana. Por último, a incorporação de mecanismos humanos de supervisão e responsabilização nos sistemas de IA pode ajudar a garantir o cumprimento dos direitos fundamentais. Isto poderia envolver a criação de sistemas humanos que permitam aos humanos monitorar e intervir nos processos de tomada de decisão da IA[15].

O TRATAMENTO DE DADOS E A INTELIGÊNCIA ARTIFICIAL

A Lei n° 13.709/2018 dispõe sobre os 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, de privacidade e o livre desenvolvimento da personalidade da pessoa natural. A disciplina da proteção de dados pessoais possui como fundamento o respeito à privacidade, a autodeterminação informativa, a liberação de expressão, de informação, de comunicação e de opinião, a inviolabilidade da intimidade, da honra e da imagem, o desenvolvimento econômico e tecnológico e a inovação, a livre iniciativa, a livre concorrência e a defesa do consumidor e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais[16].

Preceitua o art. 7° as modalidades em que o tratamento de dados pessoais será realizado, o quais serão: mediante o fornecimento de consentimento pelo titular; para cumprimento de obrigação legal ou regulatória pelo controlador; pela administração pública; para realização de estudos por órgãos de pesquisa; quando necessário para execução de contrato; para a proteção da vida; para tutela da saúde; quando necessário para atender aos interesses legítimos do controlador ou de terceiros; para proteção de crédito[17].

---

[15] BASSAN, Richard; DE SOUSA TROVÃO, Lidiana Costa. Gestão e eficiência na recuperação do crédito tributário no âmbito da execução fiscal municipal através do uso da automação e da inteligência artificial. **Revista de Direitos Fundamentais e Tributação**, v. 1, n. 3, p. 165-187, 2020.

[16] ____ Lei nº 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD).

[17] KIRCHNER, Isabel Luiza. O uso de inteligência artificial sob a ótica dos direitos fundamentais: análise do caso Amazon. 2020.

O titular tem direito ao acesso facilitado ás informações sobre o tratamento de seus dados, os quais deverão ser disponibilizado de forma clara, adequada e ostensiva, devendo ser informado a finalidade específica do tratamento, a forma e duração, observados os segredos comercial e industrial, a identificação do controlador, a referência de contato do controlador, as noções acerca do uso compartilhado de dados pelo regulador, e a finalidade, as responsabilidades dos agentes que realizarão o tratamento e os direitos do titular[18].

Quando tratar-se dos dados sensíveis os quais segundo o art.5°, inciso II, será dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato dentre outros classificados dentro do artigo mencionado, eles somente ocorrerão quando o titular ou o seu responsável legal consentir, ou sem fornecimento de consentimento quando for indispensável para o cumprimento de obrigação legal ou regulatória, para tratamento compartilhado de dados necessários à execução, pela administração pública, para realização de estudos por órgãos de pesquisa, em exercício regular de direito, para proteção da vida ou da incolumidade física do titular ou de terceiros, para tutela da saúde e para garantir a prevenção à fraude e a segurança do titular, conforme disposto no art. 11[19].

Para Pinheiro[20] é essencial que os dados sensíveis sejam tratados de uma forma especial, pois eles são considerados indispensáveis em determinadas situações, e devem sempre ser tratados com cuidado, respeito e segurança, porque a sua violação poderia implicar riscos significativos. Por isso a importância do consentimento para a realização do tratamento de dados, e embora exista exceções os procedimentos devem respeitar a mesma seriedade e garantia da segurança ao tratamento.

Os dados relacionados a menores de idade devem ser realizados em seu melhor interesse, com o consentimento específico por pelo menos um dos pais ou pelo responsável legal, e devem obedecer ao princípio da finalidade e transparência, onde os controladores deverão repassar as informações sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício do direito, os quais estão elencados no art. 18. Também poderão ser coletados dados pessoais de crianças sem o consentimento, desde que necessário para contatar os pais ou responsável legal, entretanto esse dado deve ser utilizado somente dentro do seu propósito legal

[18] BASSAN, Richard; DE SOUSA TROVÃO, Lidiana Costa. Gestão e eficiência na recuperação do crédito tributário no âmbito da execução fiscal municipal através do uso da automação e da inteligência artificial. **Revista de Direitos Fundamentais e Tributação**, v. 1, n. 3, p. 165-187, 2020.

[19] KIRCHNER, Isabel Luiza. O uso de inteligência artificial sob a ótica dos direitos fundamentais: análise do caso Amazon. 2020.

[20] PINHEIRO, Patrícia Peck. Segurança Digital - Proteção de Dados nas Empresas. São Paulo: Grupo GEN, 2020.

e não poderá ser armazenado, e todas as informações sobre o tratamento de dados deverão ser fornecidas de forma clara, simples e acessível.

Conforme expõe a LGPD, o tratamento de dados não deve ser realizado por tempo indeterminado, sendo relativo ao limite de informações a serem coletadas e a finitude do procedimento no tempo. E para isso os arts. 15 e 16 regulamenta quanto ao término do tratamento de dados pessoais onde o mesmo ocorrerá quando for verificado que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada, quando ocorrer o fim do período de tratamento, quando a comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento ou por determinação da autoridade nacional.

DA RESPONSABILIDADE DA AUTORIDADE NACIONAL A FISCALIZAÇÃO DO TRATAMENTO DE DADOS PESSOAIS

Para Pinheiro[21], um dos impactos mais importantes da Lei Geral de Proteção de Dados é a necessidade de se garantir os direitos dos titulares, e para isso os arts. 17, 18,19, 20 e 21 abrange as garantias fundamentais do titular dos dados pessoais, haja vista que as informações pessoais são de âmbito privado. Com isso, o titular tem direito de obter do controlador: a conformação de existência de tratamento; acesso de dados; correção de dados incompletos; anonimização, bloqueio ou eliminação de dados desnecessários; eliminação dos dados pessoais tratados pelo consentimento do titular; informações das entidades públicas em que o controlador realizou compartilhamento de dados; informação sobre a possibilidade de não fornecer consentimento e revogação do consentimento.

Ao referir do tratamento de dados pessoais pelo Poder Público, a lei preceitua que da mesma forma que as instituições privadas devem apresentar uma finalidade clara e transparente, a pessoa jurídica de direito público deve adotar a finalidade e o interesse público ao tratar dos dados pessoais. As instituições públicas diferentemente das empresas privadas, poderão seguir prazos e procedimentos apontados pelas Lei nº 9.507/97, nº 9.784/99 e nº 12.527/11, entretanto a exploração direta de atividade econômica pelo Estado só será permitida quando necessário aos imperativos da segurança nacional ou a relevante interesse coletivo[22]

[21] PINHEIRO, Patrícia Peck. **Segurança Digital - Proteção de Dados nas Empresas**. São Paulo: Grupo GEN, 2020.
[22] Ibid.

Pronuncia o art. 26 que é dever do Poder Público garantir que o uso compartilhado de dados siga propósitos especiais que concernem a execução das políticas públicas, ponderando entre a necessidade da publicidade das informações disponíveis ao acesso e que garanta que os direitos dos titulares sejam respeitados. Sendo vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados que tenha acesso, exceto em situações em que os dados são acessíveis publicamente ou em que a execução de um serviço ou medida o exigir.

Será responsabilidade da autoridade nacional a fiscalização do tratamento de dados pessoais, conforme arts. 29 e 30, podendo solicitar, a qualquer momento, aos órgãos e às entidades do poder público a realização de operações de tratamento de dados pessoais, informações específicas sobre o âmbito e a natureza dos dados e outros detalhes do tratamento realizado e poderá emitir parecer técnico complementar para garantir o cumprimento da lei. A autoridade nacional também poderá estabelecer normas complementares para as atividades de comunicação e de uso compartilhado de dados pessoais, conforme as necessidades do cumprimento do seu exercício.

Ainda, havendo infrações a esta lei em decorrência da inobservância da proteção das informações pessoais por órgãos públicos, caberá a autoridade nacional solicitar aos agentes de tratamentos de dados a qualquer tempo relatórios para fazer cessar a violação. Nas ocasiões em que a lei tratar de transferência internacional de dados pessoais, ela somente será permitida para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado, no momento em que o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados, quando a transferência for necessária para cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional, quando a transferência for necessária para proteção da vida ou da incolumidade física do titular ou de terceiros, e em outros casos estipulados pelo art. 33 desta mesma lei[23].

A autoridade nacional, órgão da administração pública direta federal do Brasil que faz parte da Presidência da República, levará em consideração para avaliar a proteção de dados do país estrangeiro ou do organismo internacional, as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional , a natureza dos dados, a observância dos princípios gerais de proteção de dados pessoais e de direito de titulares, a adoção de medidas de segurança previstas em regulamento, a existência de garantias judiciais e

[23] KIRCHNER, Isabel Luiza. O uso de inteligência artificial sob a ótica dos direitos fundamentais: análise do caso Amazon. 2020.

institucionais para o respeito aos direitos de proteção de dados pessoais e outras circunstâncias específicas relativas à transferência.

Buscando um padrão internacional de proteção de dados pessoais, mostrou-se necessário adotar métodos avaliativos para a autoridade nacional em face de países estrangeiros e organismos internacionais. E ainda, conforme art. 36, quaisquer mudanças direcionadas as garantias deverão ser comunicadas à autoridade nacional, tendo por base o princípio da transparência. Para o cumprimento dos propósitos do tratamento de dados, será necessário que o controlador e o operador documentem as operações realizadas durante o tratamento, no entanto para o art. 24 e 30 do GRPR, também será necessário a revisão e a atualização dos procedimentos adotados de acordo com a necessidade que se apresente[24]

A autoridade nacional poderá também determinar ao controlador que elabore relatório referente a suas operações de tratamento de dados. Vinculando o operador e o controlador, o art. 39 dispõe que o operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

Sendo assim, o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador se equipara ao controlador, e os controladores que estiverem diretamente envolvidos no tratamento que decorreu os danos ao titular dos dados respondem solidariamente.

A lei julgará irregular todos os tratamentos de dados que deixarem de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, sendo considerado circunstâncias fundamentais: o modo pelo qual é realizado, o resultado e os riscos que razoavelmente dele se esperam, e ainda, as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado. Dependendo da violação de direitos, será aplicado penalidades dispostas na legislação consumerista ou pela regra geral do Código Civil Brasileiro[25]

Ao tratar-se das seguranças e das boas práticas, o art. 46 em seu *caput*, estipula que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a

[24] PINHEIRO, Patrícia Peck. Segurança Digital - Proteção de Dados nas Empresas. São Paulo: Grupo GEN, 2020.
[25] LEORATTI, Alexandre. Diretora diz esperar que autoridade de dados seja autarquia em 2020. Poder 360, 06 ago. 2021.

proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequada ou ilícita.

É essencial durante o processo de tratamento de dados a comunicação à autoridade nacional e ao titular, pelo controlador diante de incidentes de segurança, tendo em vista o princípio da boa-fé, transparência e responsabilização dos atos do agente. Ademais, qualquer procedimento, sistema ou equipamento essencial para o tratamento de dados deverá seguir os protocolos de segurança estipulado em lei, do contrário não obteria a eficácia pretendida. Os controladores e os operadores poderão, desde que no âmbito de sua competência, formular regras de boas práticas e de governança para que todos os requisitos para a manutenção da segurança dos dados sejam efetivados.

Entretanto, como explana Pinheiro[26], apesar de minunciosamente a lei tratar da proteção dos dados dos usuários na rede, alguns aspectos ficaram a margem para uma ampla interpretação, proporcionando inseguranças jurídicas por permitir espaço para subjetividade, no qual deveria ter sido só assertiva, e um exemplo é a determinação de prazos, pois enquanto o GDPR prevê prazos exatos, a LGPD prevê prazos razoável, ficando mercê para vastas compreensões. Por isso, se faz necessário a implementação de sistemas eficientes e normas decisivas, capazes de garantir uma proteção solida e permanente para todos os usuários perante o meio digital, assegurando os princípios e garantias basilares de privacidade e liberdade tão denotado no art. 5°, inciso V, da Constituição Federal de 1988.

A INTELIGÊNCIA ARTIFICIAL O AMBIENTE DIGITAL BRASILEIRO

É enorme a facilidade de comunicação e envios de informações que se tem hoje, na qual pessoas de diferentes localidades do mundo se conectam em instantes. Caminha-se para um progresso digital cada vez mais eficiente, com mais recursos e oportunidades, em que, em contrapartida, se observa a necessidade de uma educação da informatização para aqueles que estão se inserindo agora no ambiente virtual, tanto quanto aos que já estão familiarizados, porém, sem muitas noções de segurança neste ciberespaço. A *internet* em seu lado oculto, se tornou um meio de fácil acesso para delinquentes cometerem delitos virtuais, se valendo da vulnerabilidade de muitos utentes, fazendo dos vazamentos de dados uma atividade lucrativa no Brasil, ante as leis frágeis para pôr fim a tais práticas.

[26] PINHEIRO, Patrícia Peck. Direito Digital. 7. ed. São Paulo: Editora Saraiva, 2021.

Os crimes cibernéticos, conhecidos também por crimes eletrônicos, como o próprio nome diz, são aqueles em que se comete atos ilícitos no espaço virtual, com a utilização de ferramentas digitais. Pinheiro[27] leciona em sua obra sobre direito digital que os crimes eletrônicos possuem um elevado grau de dificuldade em se identificar e punir os infratores, devido em muitos casos não ser possível constatar de imediato a autoria do delito, pela ausência de recursos para investigação técnica pelas autoridades. Razão pela qual o ciberespaço abriga tantos criminosos, justamente pela facilidade dos infratores em esconder suas identidades.

Clive Robert Humby, um matemático britânico da área de ciência de dados, disse em 2006 a seguinte frase: "os dados são o novo petróleo." Esta frase ficou mundialmente conhecida, vindo a ser utilizada por diversos escritores e empresários do campo digital. Diante desta analogia, pode-se ter uma breve noção da importância dos dados pessoais na atualidade, assim como a relevância de mecanismos eficientes para a sua proteção e, nos casos em que estes dados forem alvos de atos ilícitos, a aplicação de rígidas sanções aos infratores, sejam nas áreas administrativas, cíveis ou penais.

Bioni[28], esclarece que os vazamentos de dados podem se originar por diversos meios, como por exemplo pela falha humana, ou uma falha técnica de sistemas de segurança da rede, ou, através de ataques de criminosos. Salienta ainda que, a gravidade dos riscos de tais vazamentos, tem profunda relação com a espécie dos dados que foram alvos do vazamento, vez que são inúmeras as possibilidades de danos aos titulares. Diante disto, a legislação vigente acerca do tema criou penalidades e órgãos para a fiscalização de eventuais violações dos dados pessoais.

Somente no ano de 2020, a américa latina foi alvo de 41 bilhões de tentativas de ataques cibernéticos, deste número total, 8,4 bilhões foram registrados só no Brasil, segundo aponta o relatório da empresa especializada em cibersegurança *Fortinet.* A empresa destaca que os criminosos se sobressaem com o passar dos anos, através de novas tecnologias que possibilitam ainda mais o acesso aos dados de forma indevida, mediante ataques a base de dados privadas[29].

A LGPD ao regular sobre a matéria, reservou, assim como no Código Civil e Código de Defesa do Consumidor, a responsabilidade civil, uma vez que resta previsto no art. 42, a obrigação do controlador ou operador de reparar o dano causado a outrem em razão da atividade

[27] PINHEIRO, Patrícia Peck. Direito Digital. 7. ed. São Paulo: Editora Saraiva, 2021.
[28] BIONI, Bruno et al (Coords.). Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Grupo GEN, 2020.
[29] FORTINET. A América Latina sofreu mais de 41 bilhões de tentativas de ataques cibernéticos em 2020. Fortinet, Flórida, 24 fev. 2021.

de tratamento de dados. No que diz respeito ao regime da responsabilidade civil, Leoratti[30], expõe que tanto a responsabilidade subjetiva quanto a objetiva se encontra presente na lei, se valendo de ambas para aplicação do dever de reparo ao titular dos direitos dos dados pessoais violados.

Após a promulgação da LGPD, o ambiente digital passou a ter regulamentação específica, complementando a lei conhecida como Marco Civil da Internet. No art. 52 da lei nº 13.709/2018, encontram-se as sanções administrativas, que inclui punições que vão desde a uma simples advertência, a multas que podem chegar até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, limitada ao total de 50 milhões de reais por infração, dentre outras penas, sendo julgada proporcionalmente conforme a gravidade do caso concreto, como disposto no artigo referido acima. Deste modo, com base na análise de cada caso isolado, torna-se possível a condenação dos agentes de tratamento de dados, pelas infrações cometidas, sendo pessoa física ou jurídica[31].

Ao buscar inserir novas normativas e boas práticas de condutas no espaço digital, e instituir uma entidade para acompanhar o cumprimento das normas, foi criada a partir da LGPD, a chamada Autoridade Nacional de Proteção de Dados (ANPD), um órgão da administração pública federal, integrante da Presidência da República, como expresso no art. 55-A da lei mencionada. Através deste órgão que é desempenhada a função de fiscalizar e aplicar as sanções previstas na lei nº 13.709/18, sendo atualmente um dos meios de combate aos ataques cibernéticos. A ANPD surgiu através da Medida Provisória número 869/18, que no ano posterior veio a ser convertida na Lei 13.853/2019, passando a alterar a Lei Geral de Proteção de Dados para que regulamentasse a proteção dos dados pessoais e a criação da respectiva autoridade[32].

Sua estrutura e organização se encontra prevista na própria LGPD, no capítulo IX, do art. 55-A ao art. 57, e no Decreto número 10.474/2020, onde estão descritos os órgãos que constituem a autoridade nacional e suas respectivas competências. Embora tenha sido instituída há alguns anos, pode-se dizer que ainda é um órgão muito novo, que vem buscando melhorias na forma de atuação, e inserindo o país como membro de muitas redes reguladoras de privacidade internacional, como a recém entrada da ANPD ao *Global Privacy Enforcement Network* –

[30] LEORATTI, Alexandre. Diretora diz esperar que autoridade de dados seja autarquia em 2020. Poder 360, 06 ago. 2021.
[31] ____ Lei nº 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD).
[32] BRASIL. Autoridade Nacional de Proteção de Dados. Autoridade Nacional de Proteção de Dados e Secretaria Nacional do Consumidor lançam guia "Como proteger seus dados pessoais", 2021.

GPEN), expandindo as capacidades de relações comerciais ao passo que o Brasil poderá receber e tratar dados do exterior[33].

No art. 55-C da Lei 13.709/2018, encontra-se previsto a composição da autoridade nacional, que é composta por seis entidades que auxiliam na execução das atividades, sendo elas: Conselho Diretor, órgão máximo de direção; Conselho Nacional de Proteção de Dados Pessoais e de Privacidade; Corregedoria, Ouvidoria; Órgãos de assessoramento jurídico próprio; e as Unidades administrativas e unidades especializadas necessárias à aplicação do disposta na lei. Uma vez que esgotados os recursos para solução de problemas relacionados aos dados pessoais, a autoridade nacional através de denúncias, poderá administrativamente, aplicar as sanções previstas na LGPD ao agente ou instituição infratora. O art. 55-D da mesma lei, regula a composição do conselho diretor, e os prazos de mandato que comporá cada um[34].

A Autoridade Nacional possui um órgão máximo, que é denominado de Conselho Diretor. Conforme previsto no art. 55-D da LGPD, este Conselho será composto por cinco diretores, incluindo o Diretor-Presidente, que por sua vez serão escolhidos pelo Presidente da República. Os membros pertencentes deste conselho deverão cumprir com alguns requisitos para o cargo, como por exemplo serem brasileiros, ter nível superior de educação e especialidade técnica para o cargo que exercerão, como consta no parágrafo segundo, do artigo mencionado[35].

Sabe-se que a autoridade nacional de proteção de dados é um órgão da administração pública direta, como disposto em sua regulação própria, mas em alguns artigos, como o referido acima, se verifica nitidamente a presença do governo na tomada de algumas escolhas. Um órgão que exerce o papel de fiscalização, para que se tenha total eficácia é de suma importância que ele seja autônomo, independente e que tenha recursos próprios para desempenhar suas atividades desde o momento de sua criação. Como destaca Teixeira[36], em sua composição interna, a ANPD se assemelha com outras instituições governamentais, no âmbito de interesses políticos, sendo indispensável para a atuação como autoridade de proteção de dados que seja desvinculada dos demais órgãos, passando a ter força própria.

Na seção II do capítulo IX da LGPD, encontra-se as disposições que versam sobre o Conselho Nacional de Proteção de Dados e Privacidade (CNPD), que se trata de um órgão

---

[33] LEORATTI, Alexandre. Diretora diz esperar que autoridade de dados seja autarquia em 2020. Poder 360, 06 ago. 2021.

[34] ____ Lei nº 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD).

[35] LEORATTI, Alexandre. Diretora diz esperar que autoridade de dados seja autarquia em 2020. Poder 360, 06 ago. 2021.

[36] TEIXEIRA, Tarcisio. A LGPD e o e-commerce. São Paulo: Editora Saraiva, 2021. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555598155/>. Acesso em: 12 de maio de 2023.

consultivo da ANPD. Assim como a Autoridade Nacional, o Conselho Nacional é regulamentado pela Lei Geral de Proteção de Dados e pelo Decreto nº 10.474/2020, que dispõe sobre a estrutura organizacional, bem como disciplina sobre a atuação de cada órgão e suas respectivas divisões.

O CNPD é um órgão integrado a ANPD, que presta serviços públicos. Conforme previsto no art. 58-A, ele é composto de vinte e três membros que são integrantes de diversos órgãos administrativos e legislativos. Ante a composição dos membros do conselho nacional, verifica-se desde logo que em virtude de haver a presença de representantes de vários setores, acaba por gerar o que se conhece como sistema de freios e contrapesos, vez que haverá a fiscalização mútua dos servidores, sendo que cada setor fiscalizará e será fiscalizado ao mesmo tempo (LIMA, 2020).

O art. 58-A, por sua vez, regula a competência expressa do Conselho Nacional, como já mencionado anteriormente, em se tratando de órgão consultivo, terá suas funções com tal finalidade, como por exemplo, o disposto no inciso III do presente artigo, que atribui a função de aconselhar a ANPD a realizar determinadas ações.

Embora haja regulamentações específicas sobre a proteção de dados pessoais, elas não se restringem a apenas uma lei ou código, já existindo outras anteriores a promulgação da LGPD. A exemplo, a Constituição Federal de 1988 consolida no art. 5º, inciso X, a inviolabilidade da intimidade, sendo um direito fundamental. O Código Penal também prevê tipificações que punem os crimes desta seara, como a invasão de dispositivo informático. Ainda, uma vez expostas as informações pessoais no campo digital, seja por falha técnica ou em razão de ataque, criminosos se apossam de tais documentos com a finalidade de se passarem pelos titulares, incorrendo em crimes de falsidade ideológica, crimes contra a honra, dentre outros que são reprimidos pela legislação penal[37].

Em que pese a criação de uma norma reguladora das atividades digitais, muito se discute quanto a sua eficiência no que tange a proteção dos direitos dos titulares e a punição daqueles que contrariam os preceitos legais. Uma das prerrogativas desta lei é a adequação das empresas e estabelecimentos comerciais a um sistema novo de coleta e tratamento de dados, contudo, por se tratar de uma lei recente, ainda há lacunas para serem preenchidas. Na era atual, com aparelhos cada vez mais modernos, é possível reunir informações de pessoas formando uma base de dados em diversos campos, o que aumenta ainda mais a quantidade de informações virtuais, como um sistema de dados de supermercado que armazena informações de seus clientes, um condomínio, uma academia etc., devendo abrir um questionamento se muitas das informações que são

[37] BIONI, Bruno et al (Coords.). Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Grupo GEN, 2020.

coletadas eletronicamente são realmente necessárias, ou se apenas aumentam os riscos de exposições.

Como já mencionado, os vazamentos de dados ocorrem por diversos meios e formas. De tal modo, um usuário pode ter suas informações expostas através de uma falha no sistema de proteção de um grande banco em que possui conta, ou até mesmo pela simples navegação em *sites* que são maliciosos. Neste contexto, percebe-se a vulnerabilidade dos indivíduos, vez que deve haver uma noção de segurança própria e pessoal para uso das redes, além de um sistema de segurança digital eficaz por parte das empresas e de todos aqueles que lidam com os tratamentos de informações, e ainda assim, apenas diminuirá os riscos, mas não o extinguirá por total, levando em consideração que é uma árdua tarefa resguardar e identificar a fonte precisa dos dados quando vazados, pelo fato de uma mesma pessoa possuir suas informações pessoais em diversos bancos de dados distintos[38].

A autoridade nacional de proteção de dados, assim como destacam Mendes e Doneda[39], possui um papel indispensável para assegurar a garantia dos direitos fundamentais, de forma individuais ou coletivos, não bastando, portanto, em alguns casos apenas a ação individual do interessado, mas sim, que tenha a presença de uma autoridade competente e independente para que atue na defesa de todos e com os recursos disponíveis para que proporcione uma proteção eficiente. Verifica-se, neste caso, que a ANPD atua como garantidora dos direitos, ao mesmo tempo que desempenha a função de fiscalizadora do cumprimento das regras previstas na LGPD.

Conforme o guia "como proteger seus dados pessoais" lançado pela ANPD em conjunto com a Secretaria Nacional do Consumidor do Ministério da Justiça e Segurança Pública (SENACON/MJSP) em 10/09/2021, pode-se compreender a cooperação dos órgãos protetores das informações pessoais na atuação de medidas para resguardar os titulares dos direitos. Através do guia, os usuários têm uma explicação sucinta de como se protegerem virtualmente, e os respectivos meios para solucionar quaisquer conflitos que ocorram no âmbito digital, como por exemplo o Departamento Estadual de Proteção e Defesa do Consumidor (PROCON), Ministério Público, Defensoria Pública, podendo também o titular dos direitos violados recorrer as delegacias de polícia para registrar boletim de ocorrência nos casos em que através da exposição de suas informações privadas, serem vítimas de cibercriminosos[40].

[38] TEIXEIRA, Tarcisio. A LGPD e o e-commerce. São Paulo: Editora Saraiva, 2021.
[39] MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. Revista de Direito do Consumidor, 2020.
[40] BRASIL. Autoridade Nacional de Proteção de Dados. Autoridade Nacional de Proteção de Dados e Secretaria Nacional do Consumidor lançam guia "Como proteger seus dados pessoais", 2021.

Uma das atribuições da ANPD, por meio da inclusão da conduta de boas práticas, dispõe sobre padrões técnicos para a prevenção do uso inadequado dos dados pessoais. Embora não seja expressamente mencionado, o art. 46 da LGPD remete a ideia de dois mecanismos de segurança e proteção de dados, denominados de *privacy by design* e *privacy by default*. Lima (2020), esclarece que ambos os termos surgiram a partir dos estudos de Ann Cavoukian, na década de 90, definindo *privacy by design* como um sistema de coleta de dados que garante a segurança e transparência no tratamento de dados dos usuários, e *privacy by default* como uma extensão do primeiro termo, mantendo a segurança e consentimento do usuário quanto a privacidade de dados.

Em entrevista ao jornal digital Poder 360, a diretora da autoridade nacional afirma que a ANPD tem como foco principal atuar como um meio preventivo, buscando por meio da conscientização e prevenção, instruir os agentes de tratamento a adequarem seus sistemas de segurança para tratarem os dados pessoais de forma segura, respeitando os direitos dos titulares, ficando as multas e sanções como último recurso nos casos de descumprimento. Buscam em um primeiro momento preparar e informar os responsáveis pelos tratamentos de informações a adotarem medidas próprias para a proteção dos dados conforme a lei, de forma a evitar incidentes futuros[41].

CONSIDERAÇÕES FINAIS

Em conclusão, a integração da tecnologia na sociedade humana trouxe benefícios significativos, mas também coloca desafios à proteção dos direitos fundamentais. A Lei Geral de Proteção de Dados (LGPD) foi criada para fazer cumprir os direitos fundamentais no uso da IA. Para garantir que a IA é utilizada de uma forma que respeita os direitos fundamentais, é essencial reforçar os quadros jurídicos, desenvolver orientações éticas e incorporar mecanismos humanos de supervisão e responsabilização nos sistemas de IA. Ao fazê-lo, podemos garantir que os benefícios da IA sejam concretizados, ao mesmo tempo que protegemos os direitos e a dignidade dos indivíduos.

A conclusão sobre a análise das éticas e legais do uso da inteligência artificial na coleta e tratamento de dados pessoais no Direito Civil brasileiro deve levar em consideração as leis vigentes no país. A Lei Geral de Proteção de Dados Pessoais (LGPD), que entrou em vigor em

[41] BIONI, Bruno et al (Coords.). Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Grupo GEN, 2020.

setembro de 2020, estabelece as regras para a coleta, tratamento e armazenamento de dados pessoais no Brasil.

Segundo a LGPD, é preciso obter o consentimento expresso e informado do titular dos dados para a coleta e uso dessas informações. Além disso, as empresas e organizações que coletam dados pessoais devem adotar medidas de segurança para protegê-los e garantir sua privacidade. No caso do uso da inteligência artificial, é necessário observar essas regras e garantir que a coleta e tratamento de dados pessoais seja feita de forma ética e legal. Isso inclui, por exemplo, a transparência na coleta e uso de dados, a adoção de medidas de segurança adequadas e o respeito aos direitos dos titulares dos dados.

A LGPD surgiu com uma proposta indispensável para a atualidade, que é a de regular e proteger os dados pessoais. Com os aumentos das exposições de informações de milhares de pessoas novas no espaço digital, se faz de suma importância a existência desta lei, que teve como inspiração o regulamento europeu, conhecido por Regulamento Geral sobre a Proteção de Dados (RGPD).

São diversos os fatores que vem influenciando para a migração da sociedade para o ciberespaço. A pandemia ocasionada pelo vírus da covid-19, a globalização, as novas gerações inseridas precocemente nas redes sociais, são as razões da alta vulnerabilidade presente nesse meio, que motiva a criação de novas leis e pesquisas a fim de se encontrar soluções para os constantes crimes cometidos virtualmente.

Conforme dados expostos, a cada ano o Brasil continua sendo alvo de ataques pelos cibercriminosos. A ausência de investimentos em segurança digital pelos órgãos e empresas prestadoras de serviços, atrelado a falta de conhecimento tecnológico por grande parte dos usuários, ocasionam os constantes vazamentos de dados trazendo prejuízos inestimáveis aos próprios órgãos e aos titulares dos direitos.

Atualmente, o modelo de autoridade previsto na lei para a proteção de dados ainda não é totalmente eficiente para assegurar a inviolabilidade dos dados pessoais. Portanto, espera-se que a ANPD seja desvinculada e instituída como um órgão independente, dispondo de recursos próprios para que se tenha um maior foco na segurança dos dados pessoais, através da adoção de meios modernos para proteger, fiscalizar, identificar e punir aqueles que contrariam as normas legais.

REFERÊNCIAS

BASSAN, Richard; TROVÃO, Lidiana Costa de Sousa. Gestão e eficiência na recuperação do crédito tributário no âmbito da execução fiscal municipal através do uso da automação e da inteligência artificial. **Revista de Direitos Fundamentais e Tributação**, v. 1, n. 3, p. 165-187, 2020.

BIONI, Bruno et al (Coords.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Grupo GEN, 2020. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788530992200/>. Acesso em: 05 de maio de 2023.

BRASIL. Autoridade Nacional de Proteção de Dados. Autoridade Nacional de Proteção de Dados e Secretaria Nacional do Consumidor lançam guia **"Como proteger seus dados pessoais"**, 2021. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/autoridade nacional-de-protecao-de-dados-e-secretaria-nacional-do-consumidor-lancam-201ccomo proteger-seus-dados-pessoais201d>. Acesso em: 06 de maio de 2023.

COSTA, Ramon Silva; KREMER, Bianca. Inteligência artificial e discriminação: Desafios e perspectivas para a proteção de grupos vulneráveis frente às tecnologias de reconhecimento facial. **Revista Brasileira de Direitos Fundamentais & Justiça**, v. 16, n. 1, 2022.

____ **Decreto nº 10.474, de 26 de agosto de 2020**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato20192022/2020/decreto/D10474.htm>. Acesso em: 05 de maio de 2023.

____ **Lei nº 13.709 de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 06 de maio de 2023.

FILHO, Eduardo T. **A Lei Geral de Proteção de Dados Brasileira**. São Paulo: Grupo Almedina, 2021. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786556271705/>. Acesso em: 06 de maio de 2023.

FORTINET. **A América Latina sofreu mais de 41 bilhões de tentativas de ataques cibernéticos em 2020**. Fortinet, Flórida, 24 fev. 2021. Disponível em: <https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2021/latin america-suffered-more-than-41-billion-cyberattack-attempts-in-2020>. Acesso em: 06 de maio de 2023.

KIRCHNER, Isabel Luiza. O uso de inteligência artificial sob a ótica dos direitos fundamentais: análise do caso Amazon. 2020.

LEORATTI, Alexandre. **Diretora diz esperar que autoridade de dados seja autarquia em 2020**. Poder 360, 06 ago. 2021. Disponível em: <https://www.poder360.com.br/economia/diretora-diz-esperar-que-autoridade-de-dados-seja autarquia-ja-em-2022/>. Acesso em: 09 de maio de 2023

LIETZ, Bruna. O uso da inteligência artificial e a fiscalização dos contribuintes na perspectiva dos direitos e deveres da relação tributária. 2021.

LIMA, Ana Paula Moraes de. **LGPD Aplicada**. São Paulo: Grupo GEN, 2021. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788597026931/>. Acesso em: 05 de maio de 2023.

LIMA, Cíntia Rosa Pereira de. **Autoridade Nacional de Proteção de Dados e a Efetividade da Lei Geral de Proteção de Dados**. São Paulo: Grupo Almedina, 2020. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788584936397/>. Acesso em: 09 de maio de 2023.

LIMA, Cíntia Rosa Pereira. de. **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Grupo Almedina, 2020. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788584935796/>. Acesso em: 09 de maio de 2023.

PINHEIRO, Patrícia Peck. **Direito Digital**. 7. ed. São Paulo: Editora Saraiva, 2021. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555598438/>. Acesso em: 08 de maio de 2023.

PINHEIRO, Patrícia Peck. **Segurança Digital - Proteção de Dados nas Empresas**. São Paulo: Grupo GEN, 2020. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788597026405/>. Acesso em: 27 de abril de 2023.

PINHEIRO, Patrícia. Peck. **Proteção de dados pessoais: Comentários à lei n. 13.709/2018 (LGPD)**. Editora Saraiva, 2021. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555595123/>. Acesso em: 30 de abril de 2023.

SOARES, Marcelo Negri; MEDINA, Valéria Julião Silva. A inteligência artificial como instrumento de acesso à justiça e seus impactos no direito da personalidade do jurisdicionado. **Revista de Direito Brasileira**, v. 26, n. 10, p. 277-291, 2020.

TEIXEIRA, Tarcisio. **A LGPD e o e-commerce**. São Paulo: Editora Saraiva, 2021. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555598155/>. Acesso em: 12 de maio de 2023.