UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
FACULDADE DE DIREITO
CURSO DE GRADUAÇÃO EM DIREITO

FAYLLEN LEMOS DA SILVA

A QUALIFICAÇÃO DO DADO NEURAL COMO DADO PESSOAL SENSÍVEL

Porto Alegre
2024

FAYLLEN LEMOS DA SILVA

A QUALIFICAÇÃO DO DADO NEURAL COMO DADO PESSOAL SENSÍVEL

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção do grau de Bacharel em Direito pela Faculdade de Direito da Universidade Federal do Rio Grande do Sul.

Orientadora: Profª Dra. Kelly Lissandra Bruch

Porto Alegre

2024

FAYLLEN LEMOS DA SILVA

A QUALIFICAÇÃO DO DADO NEURAL COMO DADO PESSOAL SENSÍVEL

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção do grau de Bacharel em Direito pela Faculdade de Direito da Universidade Federal do Rio Grande do Sul.

Porto Alegre, 19 de fevereiro de 2024

BANCA EXAMINADORA

_____

Prof.ª Dra. Kelly Lissandra Bruch

Orientadora

_____

Prof.ª Dra. Maria Cláudia Mércio Cachapuz

_____

Prof. Dr. Fabiano Menke

AGRADECIMENTOS

Ao concluir esta etapa tão significativa da minha jornada acadêmica, não posso deixar de expressar minha gratidão a todos aqueles que me acompanharam e apoiaram ao longo deste percurso.

Inicialmente, minha profunda gratidão à minha família, em especial à minha mãe, Ana Lucia, cujo amor, incentivo e compreensão foram fundamentais em cada momento de dúvida e cansaço. Sua força e sabedoria foram a luz que me guiou nos momentos mais desafiadores e sua presença constante é o maior presente que poderia receber.

Aos meus amigos, especialmente Betina e Vitória, que estiveram ao meu lado durante todo o curso, compartilhando não apenas as alegrias e sucessos, mas também os momentos de dificuldade e desânimo. Sua amizade e apoio incondicional foram essenciais para que eu não perdesse a motivação e continuasse a perseguir meus objetivos com determinação.

Um agradecimento especial à minha orientadora, Profª Kelly Bruch, por sua sabedoria, paciência e dedicação incansável. Seu auxílio na elaboração deste trabalho foi indispensável, e seus ensinamentos transcenderam as páginas deste estudo, contribuindo de maneira significativa para meu crescimento acadêmico e pessoal.

A todos vocês, meu sincero agradecimento. Cada palavra de incentivo, cada gesto de apoio, cada momento compartilhado contribuiu para que este trabalho chegasse à sua forma final. Que este seja apenas um dos muitos marcos que celebraremos juntos.

Obrigado.

RESUMO

Ao alvorecer da era digital, em que a mente humana se torna um território explorável pela tecnologia, este trabalho investiga a potencial classificação dos dados neurais como dados pessoais sensíveis segundo a Lei Geral de Proteção de Dados (LGPD). Empregando uma abordagem hipotético-dedutiva e interdisciplinar, este estudo procura verificar a seguinte hipótese: os dados neurais requerem o mesmo de nível de proteção atribuído aos dados pessoais sensíveis em razão de: 1) sua natureza sensível ou 2) de sua capacidade de revelar informações sensíveis sobre os indivíduos ao serem tratados. Os resultados indicam que, em virtude de sua natureza íntima e da potencial revelação de informações sensíveis por seu tratamento, os dados neurais podem ser considerados sensíveis dentro do escopo da LGPD. Tal conclusão corrobora a hipótese inicial, enfatizando a necessidade de harmonizar a legislação à vanguarda das neurotecnologias para a salvaguarda dos direitos fundamentais à privacidade e à proteção de dados.

Palavras-chave: neurotecnologia; neurodireito; privacidade mental; interface cérebro-computador; autodeterminação informativa.

ABSTRACT

At the dawn of the digital era, where the human mind becomes a territory explorable by technology, this study investigates the potential classification of neural data as sensitive personal data under the General Data Protection Law (LGPD). Using a hypothetical-deductive and interdisciplinary approach, this study seeks to verify the following hypothesis: neural data require the same level of protection attributed to sensitive personal data due to 1) their sensitive nature or 2) their ability to reveal sensitive information about individuals when processed. The results indicate that, due to their intimate nature and the potential revelation of sensitive information through their treatment, neural data can be considered sensitive within the scope of the LGPD. Such a conclusion corroborates the initial hypothesis, emphasizing the need to harmonize legislation with the forefront of neurotechnologies for the safeguarding of fundamental rights to privacy and data protection.

Keywords: neurotechnology; neuro-right; mental privacy; brain–computer interface; informational self-determination.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

BCI	Interface cérebro-computador
EEG	Eletroencefalografia
GDPR	Regulamento Geral sobre a Proteção de Dados
LGPD	Lei Geral de Proteção de Dados Pessoais

SUMÁRIO

1 **INTRODUÇÃO**

No alvorecer da era digital, a humanidade se vê no limiar de uma nova realidade, navegando na confluência do mundo tangível com o intangível, do físico com o digital. Nas sombras dessa fronteira difusa, a neurotecnologia desponta não só como uma ferramenta pioneira do progresso, mas também como um farol que ilumina um futuro em que as profundezas da mente humana — seus sentimentos mais secretos, pensamentos mais abstratos e desejos mais latentes — podem não somente ser mapeados e entendidos, mas potencialmente moldados e transformados.

Em meio à turbulência dessa mudança de paradigma, a privacidade mental ascende como uma nova fronteira a ser desbravada e, com vigor, defendida. É uma era em que o pensamento e a cognição emergem do privado para se afirmarem como bastiões da privacidade pessoal — um território inexplorado que clama por exploração e compreensão, mas também por uma vigilância rigorosa contra invasões e manipulações.

Este trabalho é uma expedição jurídica nas entranhas da consciência humana, uma odisseia que busca traçar como a Lei Geral de Proteção de Dados (LGPD) se estende aos confins inexplorados dos dados neurais. Aqui, procura-se responder a um enigma moderno: podem os ecos digitais de nossos pensamentos, sonhos e temores ser considerados dados pessoais sensíveis, merecedores de uma armadura legal especial que os proteja contra as incursões do mundo exterior?

Esta jornada de pesquisa se desenvolve tendo como pano de fundo uma sociedade cada vez mais digitalizada, onde os dados pessoais são o novo ouro; um recurso cobiçado, extraído, comercializado e, muitas vezes, explorado sem o consentimento dos seus verdadeiros donos. Assim como a invenção da imprensa por Gutenberg democratizou o conhecimento e desencadeou uma revolução cultural, as neurotecnologias têm o potencial de democratizar o entendimento do próprio ser, transformando radicalmente áreas como medicina, educação e segurança e entretenimento. No entanto, sem salvaguardas adequadas, essa nova fronteira pode também se tornar a distopia orwelliana de "1984", onde a privacidade da mente é violada, e os pensamentos do indivíduo não são mais exclusivamente seus.

"*Black Mirror*", a aclamada série que explora as sombrias facetas das inovações tecnológicas e seus impactos na sociedade, nos oferece uma janela visceral para o potencial aterrorizante das neurotecnologias através do episódio "*Playtest*" (2016). Neste capítulo, somos apresentados a Cooper, um jovem aventureiro que, em busca de emoção e fuga da realidade, se voluntaria para testar um jogo de realidade aumentada experimental. O jogo, porém, acessa diretamente seu cérebro, transformando seus medos mais profundos em uma assustadora realidade virtual. Aqui, "*Black Mirror*" não apenas nos faz questionar a distinção entre real e virtual, mas também destaca a vulnerabilidade dos dados neurais — a essência do que nos torna quem somos — frente às tecnologias emergentes.

A jornada de Cooper é um microcosmo das preocupações mais amplas que este trabalho procura abordar. Como protegemos o refúgio mais íntimo do ser humano — a mente — quando ele se torna acessível pela tecnologia? A invasão de Cooper pelo jogo é uma metáfora para os potenciais abusos no tratamento de dados neurais, desde manipulação de memórias até a criação de realidades alternativas indistinguíveis da nossa própria. Assim como o protagonista de "*Playtest*" se vê envolvido em uma espiral de realidades sobrepostas, este trabalho busca desvendar as camadas que compõem os dados neurais, questionando não apenas como eles devem ser classificados, mas também como podem ser protegidos em um mundo onde a distinção entre humano e máquina se torna cada vez mais borrada.

Esta questão não é nova. A literatura e o cinema há muito exploram a ideia da mente como o último refúgio da liberdade humana — e o último alvo da opressão. "Neuromancer", de William Gibson, com seu *cyberspace* e hackers cerebrais, alerta sobre o poder e os perigos da conectividade mental. "As Portas da Percepção", de Aldous Huxley, examina a expansão da consciência através de meios químicos, prenunciando a busca por experiências além do físico, agora ao alcance através da tecnologia.

Na mitologia grega, Prometeu desafiou os deuses ao conceder aos mortais o dom do fogo, uma ferramenta de poder inimaginável e duplo propósito. Esse ato não só simboliza a entrega do conhecimento e do progresso à humanidade, mas também introduz o dilema moral associado ao uso desse poder. Na era contemporânea, essa alegoria encontra um paralelo notável no advento das neurotecnologias e na proteção dos dados neurais, uma faísca moderna prometeica

que promete iluminar as profundezas inexploradas da mente humana, ao mesmo tempo em que suscita preocupações éticas e de privacidade sem precedentes.

Na busca por respostas frente a esses desafios, este trabalho se aprofunda na análise da legislação vigente, particularmente a LGPD, para investigar sua capacidade de salvaguardar contra potenciais violações à privacidade que a neurotecnologia pode acarretar. Assim como Prometeu enfrentou dilemas ao entregar o fogo aos humanos, pondera-se até que ponto as normas vigentes são capazes de proteger o cidadão contra presentes e futuras ameaças à privacidade mental. Questiona-se a suficiência das leis atuais em antecipar e mitigar os riscos associados ao avanço dessas tecnologias, anteriormente previstos e explorados em narrativas de ficção, como em episódios visionários de "*Black Mirror*", mas que agora se tornam realidade palpável.

À medida que a neurociência avança, o que antes pertencia ao domínio da ficção científica agora desafia as fronteiras do direito, provocando debates sobre o impacto da neurotecnologia na concepção de privacidade e individualidade. Este cenário coloca em evidência a necessidade de que a privacidade e a proteção de dados sejam defendidas com o mesmo rigor aplicado a outros direitos fundamentais, frente aos desafios impostos pelas tecnologias emergentes.

Neste contexto, o presente estudo se lança em uma investigação interdisciplinar, costurando juntos os campos do direito, da neurociência e da tecnologia. Busca-se desvendar respostas situadas na confluência entre as normativas jurídicas e as possibilidades quase inexploradas que as neurotecnologias oferecem. Questiona-se se, ao modo do filme "A Origem" de Christopher Nolan, podemos construir fortalezas mentais intransponíveis ou se caminhamos para um futuro em que o conceito de privacidade mental é obsoleto.

Diante desse cenário, contemplam-se as implicações legais de um mundo onde a neurociência avança a passos largos para além do laboratório, infiltrando-se no cotidiano. Explora-se a dicotomia de um futuro em que, por um lado, há a esperança de que as neurotecnologias possam abrir caminhos revolucionários para a cura de doenças cerebrais, o aprimoramento do processo educacional e a expansão das formas de comunicação. Por outro lado, enfrenta-se o medo de um cenário distópico onde a intimidade dos nossos pensamentos é uma mercadoria negociável.

Assim, este trabalho tem como objetivo principal a análise acerca da possível classificação dos dados neurais como dados pessoais sensíveis no âmbito da LGPD. Examina-se a pertinência dessa categorização considerando os avanços expressivos em neurotecnologias, que suscitam novas questões sobre privacidade e proteção de dados. Como objetivos específicos, propõe-se não apenas identificar as propriedades distintas dos dados neurais, mas também explorar sua essência e a capacidade de desvelar informações privadas, estabelecendo conexões com categorias já consideradas sensíveis pela LGPD.

A investigação inclui, ainda, uma análise detalhada do marco legal brasileiro no que tange à proteção de dados sensíveis, com enfoque no artigo 5º, inciso II, e no § 1º do artigo 11 da LGPD. O propósito é verificar se a legislação vigente abrange eficazmente os dados neurais, assegurando um tratamento que respeite os direitos fundamentais dos indivíduos. Ademais, objetiva-se examinar as implicações de um manejo impróprio dos dados neurais, destacando os perigos de discriminação e as infrações de privacidade que podem emergir na falta de uma proteção legal específica. Finalmente, a pesquisa visa expandir seu escopo para o contexto internacional, buscando compreender os paradigmas de regulamentação aplicáveis a dados pessoais sensíveis e neurodireitos em uma perspectiva global.

A metodologia adotada por este trabalho segue o método hipotético-dedutivo, partindo da seguinte hipótese: os dados neurais requerem o mesmo de nível de proteção atribuído aos dados pessoais sensíveis em razão de (1) sua natureza intrínseca e (2) de sua capacidade de revelar informações sensíveis sobre os indivíduos ao serem tratados. Baseando-se nessa premissa, deduz-se que se os dados neurais têm o potencial de desnudar aspectos íntimos, então eles se alinham com as categorias de dados pessoais sensíveis já estabelecidas pela LGPD, como informações de saúde, genéticas ou biométricas associadas a um indivíduo. Além disso, a gestão imprópria desses dados poderia levar a discriminações ou violações de privacidade, similarmente ao risco apresentado por outros dados sensíveis.

A validação dessa hipótese ocorrerá através de uma análise detalhada de casos práticos e pesquisas que ilustram o uso dos dados neurais na obtenção de informações pessoais delicadas, mapeando o progresso das neurotecnologias e suas aplicações em áreas diversificadas como marketing, segurança e educação. Um exame aprofundado da legislação, da jurisprudência e da doutrina relacionadas

à proteção de dados sensíveis no Brasil será realizado. Posteriormente, será discutida a viabilidade da classificação do dado neural como dado pessoal sensível conforme os ditames da LGPD, abrindo caminho para uma proteção jurídica consonante com os desafios impostos pela era digital.

Conforme avançamos, deparamo-nos com um cenário de confronto onde os direitos individuais colidem frontalmente com os progressos tecnológicos, delineando um território em que a dignidade humana e a curiosidade ilimitada estão em constante disputa. Mergulhamos numa era em que não só a privacidade se encontra em risco, mas a própria essência da individualidade está exposta à vulnerabilidade provocada pela incursão tecnológica. Os dados neurais, com seu potencial revelador dos nossos mais profundos pensamentos e emoções, demandam não apenas uma proteção legal robusta, mas também a defesa de nossa singularidade e liberdade.

Neste estudo, busca-se em um diálogo interdisciplinar, cruzando as fronteiras entre ciência e direito, para investigar até que ponto a legislação vigente serve como um escudo contra a exposição não autorizada de nossa intimidade mental. Explora-se a possibilidade de estabelecer direitos e garantias que não somente acompanhem, mas que também orientem o desenvolvimento tecnológico, assegurando que a essência do ser humano seja protegida em meio à crescente capacidade de acessar e decifrar os segredos da mente.

Este é um momento crítico, em que a lei deve ser visionária, antecipando cenários futuros e estabelecendo um ambiente seguro, no qual a tecnologia se desenvolve respeitando os limites da ética e da individualidade. Assim, a presente pesquisa constitui uma ponte entre o presente e o futuro, oferecendo perspectivas sobre como moldar um quadro legal que efetivamente resguarde os valores da dignidade humana na era digital, mantendo a individualidade como o núcleo inalienável da experiência humana.

2 **NEUROCIÊNCIA E TRATAMENTO DE DADOS NEURAIS**

Esta seção analisa as implicações da intersecção entre neurociência, tecnologia e o tratamento de dados neurais. Inicialmente, discute-se a variedade de neurotecnologias, focando em seu uso de dados neurais e impacto na extensão das capacidades humanas, bem como na autodeterminação informativa e corporal. Em seguida, investiga-se os emergentes neurodireitos, abordando dilemas éticos e a necessidade de salvaguardar o tratamento de dados neurais. Finalmente, ressalta-se a distinção da privacidade mental frente a outras formas de privacidade, sublinhando sua importância para a integridade psicológica do indivíduo.

2.1 NEUROTECNOLOGIAS E DADOS NEURAIS

O tratamento de dados neurais incorpora um domínio interdisciplinar no qual a neurociência converge com tecnologias emergentes para decifrar e moldar informações derivadas do cérebro humano. A disponibilidade destes dados tem experimentado um crescimento exponencial, impulsionado por inovações contínuas em neurotecnologias (KASS; EDEN; BROWN, 2014).

A neurociência moderna, armada com ferramentas tecnológicas avançadas, está desvendando os mistérios da cognição, emoção e comportamento humanos. Por meio de técnicas como eletroencefalografia (EEG) e imagem por ressonância magnética funcional (fMRI, na sigla inglesa), os cientistas mapeiam padrões de atividade cerebral as quais podem ser correlacionadas com processos mentais específicos (COX; SAVOY, 2003). Estas descobertas ampliam a compreensão sobre o funcionamento cerebral, oferecendo novas perspectivas sobre a consciência e a cognição.

Nesse contexto, a Interface Cérebro-Computador (BCI, na sigla inglesa) é uma das mais promissoras neurotecnologias. Ao converter sinais neurais em comandos digitais, as BCIs estão revolucionando a interação humana com a tecnologia e abrindo caminho para próteses controladas pela mente, tratamentos para distúrbios neurológicos e até interfaces de realidade aumentada (GUPTA; VARDALAKIS; WAGNER, 2023). Além disso, as neuropróteses estão

transformando o modo de vida das pessoas, permitindo que indivíduos com deficiências motoras recuperem funções perdidas (MENDES; LIMA; SOUZA, 2020).

Uma das iniciativas mais divulgadas é a Neuralink de Elon Musk, que visa desenvolver implantes cerebrais para ajudar pessoas com lesões na medula espinhal e eventualmente permitir a fusão do cérebro humano com a inteligência artificial. A demonstração de um protótipo em um porco recebeu ampla atenção da mídia (CRANE, 2020), tendo o primeiro humano recebido um implante em 28 de janeiro de 2024 (MUSK, 2024).

Casos de indivíduos utilizando próteses controladas por pensamento têm sido frequentemente destacados na mídia, simbolizando um marco na reabilitação e na medicina regenerativa (DEUTSCHE WELLE, 2021). A aplicação de neurotecnologias, porém, se estende muito além do campo da saúde, disseminando-se em várias áreas que vão desde a educação até a indústria e o meio artístico.

Neurotecnologias estão sendo exploradas, por exemplo, para personalizar experiências educacionais. Dispositivos de monitoramento cerebral, como fones de ouvido EEG, podem ser usados para avaliar o estado de atenção dos alunos, permitindo ajustes em tempo real nas estratégias de ensino (RAMÍREZ-MORENO et al., 2021). A China tem sido pioneira ao introduzir em seu sistema de ensino o uso de neurotecnologias. Em algumas escolas chinesas, estudantes têm seus níveis de concentração monitorados por um dispositivo acoplado a suas cabeças, o qual é capaz de captar ondas cerebrais (BAYNES, 2019).

Na indústria, interfaces cérebro-computador (BCIs) estão sendo desenvolvidas para melhorar a interação homem-máquina. Operadores podem controlar maquinário ou sistemas robóticos remotamente usando apenas sinais cerebrais. Isso não apenas aumenta a eficiência operacional, mas também reduz os riscos em ambientes perigosos, permitindo que trabalhadores controlem equipamentos à distância (LIU; HABIBNEZHAD; JEBELLI, 2021). Algumas empresas têm utilizado tecnologias BCI como a eletroencefalografia (EEG) para analisar sinais de sonolência ao volante (EMOTIV, 2014). Empresas que empregam trabalhadores que operam maquinário perigoso, bem como pilotos de avião ou cirurgiões, podem vir a utilizar neurotecnologias a fim de que seus funcionários sejam monitorados de maneiras semelhantes.

O neuromarketing, por sua vez, utiliza técnicas de neuroimagem para entender as respostas dos consumidores a produtos e publicidades. Ao monitorar as respostas cerebrais, as empresas podem obter insights sobre as preferências e comportamentos dos consumidores de maneira mais direta e objetiva do que métodos de pesquisa tradicionais (AGARWAL; DUTTA. 2015). Na implementação de uma significativa campanha de publicidade, avaliada em 100 milhões de dólares, a empresa Yahoo empregou métodos de neuromarketing para aferir a atividade cerebral de consumidores potenciais. Como elemento central da estratégia de marketing, a campanha incluiu a criação de um anúncio publicitário que apresentava indivíduos alegremente dançando em diversos locais ao redor do globo. A técnica de eletroencefalograma (EEG) foi utilizada pela empresa para medir as reações neurais dos consumidores ao anúncio (NEURAL EXPERIENCE, 2021).

No campo da arte, artistas estão usando neurotecnologias para criar experiências imersivas e interativas. Por exemplo, instalações artísticas que mudam em resposta às ondas cerebrais dos espectadores, oferecendo uma experiência única e personalizada (GRANDCHAMP; DELORME, 2016). Na obra de arte performática intitulada “Dual Brains”, a artista Eva Lee e o designer Aaron Trocola, conectados por um fone de ouvido personalizado impresso em 3D, utilizam ondas cerebrais para criar arte. O dispositivo, equipado com eletrodos, monitora os padrões neurais e os batimentos cardíacos dos participantes. Em 2016, a ópera cerebral "Noor" foi apresentada pela primeira vez, proporcionando uma experiência teatral imersiva ambientada na Segunda Guerra Mundial. Nessa obra, a intérprete Ellen Pearlman utiliza um headset Emotiv que processa suas ondas cerebrais para ler estados como frustração, interesse, excitação e meditação. Esses estados cerebrais são então visualizados como bolhas coloridas em grandes telas, acompanhadas de imagens que narram histórias com temas emocionais (DORFFMAN, 2018).

Tais exemplos demonstram a ampla gama de aplicações das neurotecnologias fora da saúde, revelando seu potencial para transformar diversas facetas da vida cotidiana. Como conseguência destes usos, surge uma nova dimensão intrínseca ao desenvolvimento desta tecnologia: a ampliação do corpo humano. As neurotecnologias não apenas remodelam interações e experiências

externas, mas também integram e expandem as capacidades físicas e cognitivas inerentes ao ser humano, marcando um avanço significativo na fusão entre o biológico e o tecnológico.

2.1.1 **Neurotecnologias e a ampliação do corpo humano**

A tecnologia da informação possibilitou às pessoas criarem representações digitais de si mesmas, mas estas eram claramente distintas de suas identidades físicas. Tradicionalmente, a identidade digital era vista como uma extensão não intrínseca do ser físico. Ao tratar de conceitos tradicionais, como personalidade, autodeterminação ou liberdade, dentro do contexto do processamento de dados, o Direito buscava caracterizá-los como “digitais” ou “informáticos”. Quando surgiram as primeiras leis europeias sobre proteção de dados, na década de 1970, estas referenciavam explicitamente as tecnologias utilizadas. Posteriormente, porém, a Diretiva 46/95/CE, que unificou tais regras no espaço europeu, passou a tratar de forma indistinta acerca de banco de dados eletrônicos ou manuais. Segundo explica Doneda (2006), as repercussões tecnológicas se tornaram tão intensas nas diversas instâncias pessoais de modo a impossibilitar a separação dos fenômenos da informática de outros considerados tradicionais.

No contexto contemporâneo, conforme argumenta Rodotà (2005), a noção de pessoa humana transcende a mera existência física para incorporar uma dimensão digital significativa, definida por ele como “corpo eletrônico”. Logo, a concepção da integralidade da pessoa humana engloba não somente o corpo físico, mas também sua dimensão digital, sendo esta constituída por seu conjunto de dados pessoais. Ao integrarem dispositivos eletrônicos com o sistema nervoso humano, as neurotecnologias materializam o conceito de corpo eletrônico. A incorporação da dimensão digital na conceituação do ser humano sugere uma redefinição dos direitos fundamentais, especialmente no que tange à proteção de dados e à integridade pessoal no ambiente digital.

Com o avanço da neurociência, a tecnologia não apenas transforma a compreensão humana acerca das máquinas, mas redefine o próprio ser humano (HAYLES, 1999). Conforme explorado por Hayle (1999), o conceito de pós-humanismo exprime a ideia de que a consciência e a inteligência não são

exclusivas do organismo biológico, mas podem ser estendidas e integradas com sistemas tecnológicos. No âmbito das neurotecnologias, esta fusão é particularmente evidente nas interfaces cérebro-computador (BCIs), que conectam diretamente a atividade cerebral a dispositivos eletrônicos, efetivamente ampliando a cognição humana para além dos limites físicos do corpo.

Em seu trabalho, Nicolelis e Lebedev (2009) investigaram a viabilidade de decodificar os sinais neurais e traduzi-los em comandos para controlar dispositivos externos, como próteses robóticas. O experimento consistiu em implantar eletrodos no cérebro de macacos e treiná-los para realizar tarefas específicas enquanto sua atividade cerebral era monitorada. O objetivo era entender como os padrões de atividade neural correspondiam a movimentos específicos e, em seguida, usar esses dados para controlar próteses. Com o conhecimento adquirido, foi possível projetar um exoesqueleto que ganhou notoriedade mundial quando foi demonstrado na cerimônia de abertura da Copa do Mundo FIFA 2014, no Brasil. Na abertura deste evento, um jovem paraplégico, equipado com o exoesqueleto, foi capaz de dar o pontapé inicial simbólico do torneio (BRASIL, 2014).

O corpo humano no contexto da emergência das neurotecnologias, representa uma confluência entre o biológico e o tecnológico, remodelando profundamente as noções tradicionais de corpo, identidade e autonomia. De certa forma, estas tecnologias consagram a fusão entre orgânico e inorgânico imaginada pelo Manifesto Ciborgue (HARAWAY, 1985). Além de explorar a interação entre o biológico e o tecnológico, a obra ilustra e as implicações sociais e éticas do avanço tecnológico. O acesso a estas inovações pode vir a amplificar as desigualdades sociais e as dinâmicas de poder, uma vez que a possibilidade de melhoramento cognitivo e físico através de neurotecnologias pode ampliar as disparidades existentes. Outrossim, os avanços práticos da neurociência também possuem implicações nas teorias filosóficas sobre a mente e a cognição.

Na obra “The Extended Mind”, Clark e Chalmers (1998), propõem a ideia de que os processos mentais não se limitam ao cérebro ou mesmo ao corpo, mas podem estender-se para além do organismo físico, englobando ferramentas e dispositivos externos. As neurotecnologias, que incluem dispositivos como interfaces cérebro-computador (BCIs) e próteses neurais, comprovam essa tese. Por meio dessas tecnologias, a atividade cerebral pode ser diretamente conectada

e integrada com dispositivos externos, expandindo a capacidade cognitiva e perceptiva do usuário. Essa extensão física do processamento cerebral para fora do corpo humano ilustra literalmente o conceito de uma mente estendida.

Com a disseminação da habilidade de acessar e manipular dados neurais, surgem questões éticas prementes. A privacidade dos dados cerebrais torna-se uma preocupação crescente a medida em que ferramentas tecnológicas tornam-se parte integrante da mente. Se a mente pode ser estendida para incluir dispositivos eletrônicos, A possibilidade de "hackear" pensamentos ou manipular memórias levanta questões pertinentes sobre a segurança e a integridade do "eu" individual (BUBLITZa, 2013). Além disso, se a mente não está mais confinada ao crânio, a ideia de uma mente distribuída e interativa com o ambiente sugere um novo paradigma para entender a cognição humana (CLARK; CHALMERS 1998).

Harari (2018) destaca a potencial erosão da privacidade e da autonomia individual que pode advir com a expansão dessas tecnologias. A coleta de dados neurais por empresas e governos pode levar a uma compreensão e manipulação sem precedentes dos indivíduos. Segundo Harari, essa capacidade de "ler" e potencialmente "escrever" no cérebro humano traz consigo preocupações sobre a manipulação de comportamentos, preferências e até identidades. Quando Harari fala sobre a capacidade de "ler" o cérebro, ele se refere à coleta de dados neurais que revelam informações sobre pensamentos, emoções, preferências e intenções de uma pessoa. A ideia de "escrever" no cérebro humano vai um passo além. Isso envolve a manipulação direta da atividade neural, o que pode influenciar ou alterar processos cognitivos e emocionais. Por exemplo, técnicas como a estimulação cerebral profunda ou a optogenética (que usa luz para controlar neurônios modificados geneticamente) podem ser usadas para modificar comportamentos, emoções ou até mesmo memórias. Essa capacidade não apenas levanta questões éticas profundas sobre a manipulação da mente, mas também sobre a autonomia e a liberdade individual.

A questão do controle sobre os dados neurais adquire uma complexidade adicional quando considerada a ampliação do corpo humano proporcionada pelas neurotecnologias. Neste contexto, os dados neurais estão profundamente entrelaçados com a essência do ser, refletindo não apenas pensamentos e emoções, mas também potencializando as capacidades humanas além dos limites

biológicos tradicionais. (PAZ, 2021). O controle inadequado pode levar a violações de privacidade e a potenciais abusos, como a possibilidade de explorar e manipular pessoas por meio do acesso direto a seus processos neurais (CHIESA et al., 2017). Além disso, a ampliação do corpo humano por meio de neurotecnologias ressalta a importância da autodeterminação informativa e corporal. Esses conceitos, essenciais para a identidade e individualidade humanas, são desafiados pela integração da tecnologia com a fisiologia humana.

2.1.2 **Neurotecnologias e autodeterminação informativa e corporal**

O conceito de autodeterminação informativa, um princípio fundamental no contexto da proteção de dados pessoais, adquire uma nova dimensão no contexto do tratamento de dados neurais. Originado do direito alemão, tendo sido reconhecido pelo Tribunal Constitucional na decisão sobre o caso do censo demográfico, denominada *Volkszählungsurteil* (ALEMANHA, 1983), este conceito representa o direito do indivíduo de exercer controle sobre o acesso, uso e compartilhamento de suas informações pessoais (MENDES, 2020). No âmbito das neurotecnologias, isso implica o direito de decidir como e por quem os dados neurais serão tratados, protegendo a autonomia individual e prevenindo abusos. A autodeterminação informativa se expande para incluir a soberania sobre informações neurais, que se tornam parte integrante da experiência e expressão humanas.

A autonomia corporal, por sua vez, conceituada como a capacidade intrínseca de um indivíduo para tomar decisões autônomas em relação ao próprio corpo, é firmemente ancorada no domínio da existencialidade ou extrapatrimonialidade (MORAES; CASTRO. 2014). A autodeterminação corporal, portanto, é uma manifestação da autonomia existencial, enfatizando o direito de cada indivíduo de governar e controlar o próprio corpo livre de coerção externa, em conformidade com seus valores, crenças e escolhas pessoais.

Rodotà (2009) defende a ideia de que o corpo, junto com os dados que o compõem, deve ser entendido como um elemento integral à realização da pessoa, seu único titular legítimo. E prossegue ao enfatizar que o corpo e os dados

associados a ele não devem ser vistos como commodities a serem exploradas por outras entidades, sejam elas corporações, governos ou outras instituições. No contexto das neurotecnologias, em que a interface entre o corpo físico e o digital se torna cada vez mais íntima e complexa, a autodeterminação corporal, historicamente focada na integridade física, passa a abranger a integridade neural, dada a capacidade das neurotecnologias de alterar ou ampliar funções cerebrais.

Na perspectiva de Menke (2015), uma das preocupações primordiais associadas ao instituto da proteção de dados reside na possibilidade de indivíduos serem objeto de manipulação por intermédio de informações detidas por seus interlocutores, quer sejam entidades estatais ou privadas, sem o seu conhecimento Conforme o autor, em situações onde o prévio conhecimento sobre dados da contraparte é estabelecido, o possuidor dessas informações adquire, invariavelmente, uma posição de vantagem, facilitando a manipulação e o direcionamento da interação. Nesse sentido, de acordo com Farahany (2023), a neurotecnologia apresenta desafios únicos para a privacidade, pois os dados coletados diretamente do cérebro podem revelar informações muito mais íntimas do que os dados tradicionais. Com o desenvolvimento de neurotecnologias, que têm o poder de acessar, interpretar e manipular dados neurais, a fronteira entre os dados (informativos) e o corpo (físico) está se dissolvendo. Consequentemente, a relação entre autodeterminação informativa e autodeterminação corporal torna-se cada vez mais intrincada e significativa.

Não se pode considerar, porém, que a relação entre neurotecnologias e autodeterminação seja estritamente unidirecional. Se por um lado a tecnologia desafia a privacidade, por outro ela também oferece novos meios para fortalecer a autodeterminação informativa. As BCIs, por exemplo, podem ser usadas para possibilitar que indivíduos com limitações de comunicação expressem suas preferências e consentimento de maneiras que anteriormente não seriam possíveis (SELLERS; RYAN; HAUSER, 2014). Nesse contexto, conforme Cachapuz (2019), o que se almeja com a noção de autonomia informativa é a existência de uma reciprocidade ideal no comportamento dentro da esfera pública, envolvendo todos os participantes em um processo de troca de informações. Segundo a autora, essa expectativa baseia-se na ideia de que qualquer limitação à liberdade de transmissão de informações vai além do interesse meramente individual do titular da informação.

Além disso, conforme Cachapuz (2019), a demanda por reciprocidade não se restringe somente ao desejo de limitar uma liberdade de maneira isolada, englobando também a promoção de uma conduta responsável entre todos os participantes que, de forma recíproca, envolvem-se no espaço de troca de informações.

Nesta perspectiva, Ienca e Andorno (2017), ao abordarem a regulamentação de tais tecnologias, ressaltam a necessidade de serem considerados não apenas os aspectos técnicos da coleta de dados, mas também as implicações éticas e sociais relacionadas à autodeterminação. Isso inclui a necessidade de consentimento informado, explicitamente detalhando como os dados neurais serão usados, armazenados e potencialmente compartilhados. Além disso, a abordagem de Ienca e Andorno sugere a necessidade de abordar as implicações sociais mais amplas dessas tecnologias. Isso envolve considerar questões como equidade no acesso às neurotecnologias, os riscos de exacerbamento das desigualdades sociais e os impactos sobre grupos vulneráveis. A proteção dos dados neurais, portanto, não é apenas uma questão de privacidade individual, mas também uma preocupação coletiva que toca no cerne da justiça social e dos direitos humanos.

Neste contexto, pesquisadores como Rafael Yuste e Sara Goering (2017) têm se dedicado ao debate sobre a formulação de leis e diretrizes adequadas em face dos avanços em neurotecnologias. Eles não só reconhecem a urgência de responder aos desafios emergentes das neurotecnologias, mas também propõem o conceito de neurodireitos para proteger a integridade e a privacidade das funções cerebrais dos indivíduos. A discussão sobre neurodireitos, como será detalhado na subseção 2.2, é um exemplo de como os avanços tecnológicos em neurociência requerem uma reavaliação constante das normas jurídicas, ressaltando a importância de um diálogo interdisciplinar entre cientistas, legisladores, juristas e o público em geral.

O avanço das neurotecnologias e a crescente capacidade de realizar os mais diversos tratamentos de dados neurais desafiam as concepções tradicionais de corpo, identidade e autonomia, exigindo uma reavaliação das normas éticas e legais (MACKENZIE; WALKER, 2015). A questão do controle sobre os dados neurais e a preservação da privacidade neural são críticas neste novo paradigma (BUBLITZb, 2019). O direito à privacidade neural, neste sentido, destaca-se como

um preceito chave para assegurar que a integração das neurotecnologias na sociedade respeite a dignidade e os direitos fundamentais dos indivíduos no tratamento de dados neurais.

2.2 NEURODIREITOS E O TRATAMENTO ÉTICO DE DADOS NEURAIS

O desenvolvimento de neurotecnologias com a capacidade de "ler" estados mentais, decodificando informações sobre processos cerebrais por meio da análise de padrões de atividade neural, possibilitou avanços significativos no campo da neurociência. Como abordado no item 2.1, esses avanços desencadearam o desenvolvimento de neurotecnologias não invasivas de consumo, com diversas aplicações não clínicas, incluindo nas áreas educacionais, artísticas e industriais. Entretanto, essas aplicações ainda não foram completamente exploradas ou regulamentadas por leis nacionais ou tratados internacionais, conforme identificado por Fernandez et al. (2015).

Nos anos recentes, este paradigma tem sido, contudo, alterado. Em 25 de outubro de 2021, o Chile se tornou a primeira nação do mundo a possuir uma constituição em vigor que aborda explicitamente os direitos dos indivíduos em relação às neurotecnologias emergentes (GUZMÁN, 2022). Aprovada por unanimidade pelo Senado, a Lei nº 21.383 altera o Artigo 19 da Constituição Política da República do Chile de 1980, com a inclusão de um parágrafo estipulando que “o desenvolvimento científico e tecnológico estará a serviço das pessoas e será realizado com respeito à vida e à integridade física e mental. A lei regulará os requisitos, condições e restrições para o seu uso pelas pessoas, e deve proteger especialmente a atividade cerebral, bem como as informações provenientes dela.[1]” (CHILE, 2021, tradução nossa).

Também no Chile, em uma decisão recente e unânime, publicada em 9 de abril de 2023, a Corte Suprema ordenou que a empresa de neurotecnologia Emotiv apagasse todos os dados cerebrais coletados do ex-senador Guido Girardi. A

[1] Texto original na língua espanhola: “El desarrollo científico y tecnológico estará al servicio de las personas y se llevará a cabo con respeto a la vida y a la integridad física y psíquica. La ley regulará los requisitos, condiciones y restricciones para su utilización en las personas, debiendo resguardar especialmente la actividad cerebral, así como la información proveniente de ella.”

Emotiv, uma empresa norte-americana de bioinformática, é responsável pela fabricação de um dispositivo chamado Insight, que opera sem fio e funciona como uma faixa com sensores coletando informações sobre a atividade elétrica do cérebro. Este dispositivo obtém dados sobre gestos, movimentos, preferências, tempos de reação e atividade cognitiva do usuário. Girardi comprou um dispositivo Insight através do site da Emotiv, recebendo-o em sua residência. Ao seguir as instruções do dispositivo com o objetivo de gravar e acessar seus dados cerebrais, criou uma conta na nuvem de dados da Emotiv, após aceitar os termos e condições da empresa. Posteriormente, instalou em seu computador o software Emotiv Launcher, um ponto de acesso a toda a informação, ferramentas e gestão de dispositivos Emotiv, associando sua conta ao dispositivo Insight, sendo necessário aceitar novamente os termos e condições da empresa. Devido ao uso da licença gratuita, e não a 'PRO', o ex-senador não podia exportar nem importar nenhum registro dos dados cerebrais. Girardi decidiu não pagar pela licença e começou a usar o dispositivo. Consequentemente, seus dados foram gravados e armazenados na nuvem da Emotiv, sem que ele tivesse acesso a eles. Contudo, a Emotiv reservava-se o direito de utilizar os dados de Girardi para treinar seus algoritmos e para fins de pesquisa científica. Considerando as ações da empresa, a Corte concluiu que a Emotiv violou o Artigo 19, parágrafos 1º e 4º, da Constituição Política da República do Chile de 1980, que protegem o direito à integridade física e mental e o direito à privacidade (CHILE, 2023). Em resposta à decisão da Corte, a Emotiv revelou que havia suspendido as vendas do Insight no Chile e que deletaria a conta de Girardi, bem como todos os dados associados (ASHER-SHAPIRO; BAPTISTA, 2023). Esta foi a primeira vez no mundo em que uma corte determinou que empresas de neurotecnologia não podem violar os neurodireitos.

Paralelamente, o Artigo 26 da Carta Espanhola de Direitos Digitais, aprovada pelo Governo Espanhol em 14 de julho de 2021, representa um segundo esforço pioneiro na definição de direitos específicos para a regulamentação da neurotecnologia, conhecidos como "neurodireitos". O artigo prevê que “para garantir a dignidade da pessoa, a igualdade e a não discriminação, e de acordo com os tratados e convenções internacionais, a lei poderá regular aqueles casos e condições de uso das neurotecnologias que, além de sua aplicação terapêutica, pretendam o aumento cognitivo ou a estimulação ou potenciação das capacidades

das pessoas”[2] (ESPANHA, 2021, tradução nossa). A inclusão deste artigo demonstra que em diferentes jurisdições, as instituições públicas têm dedicado atenção à necessidade de proteger os indivíduos contra o uso indevido de suas informações neurais.

No Brasil, o Estado do Rio Grande do Sul foi o primeiro a incluir em sua Constituição, por meio da Emenda Constitucional nº 85/2023[3], a proteção à integridade mental do ser humano como requisito para a política e a pesquisa cientifica e tecnológica. Todas essas experiências jurídicas - chilena, espanhola e gaúcha - foram influenciadas pelo trabalho desenvolvido pela Neurorights Foundation, um grupo interdisciplinar liderado pelo neurocientista Rafael Yuste, o qual propõe a salvaguarda de cinco direitos neurais fundamentais: o Direito à Identidade Pessoal, o Direito ao Livre-arbítrio, o Direito à Privacidade Mental, o Direito ao Acesso Equitativo às Tecnologias de Aprimoramento Cognitivo e o Direito à Proteção Contra Vieses Algorítmicos (IBERDROLA, 2023). Esses direitos representam uma reformulação conceitual de direitos já reconhecidos (liberdade de pensamento, integridade corporal) em resposta às oportunidades tecnológicas emergentes de registrar e manipular diretamente o cérebro (REINER; NAGEL, 2017).

O Direito à Identidade Pessoal é um conceito que busca proteger a integridade e a singularidade de cada indivíduo em face do avanço da tecnologia. Isso significa que limites devem ser estabelecidos para proibir que a tecnologia perturbe o senso que cada um possui de si mesmo. Quando a neurotecnologia

---

[2] Texto original em língua espanhola: 1. Las condiciones, límites y garantías de implantación y empleo en las personas de las neurotecnologías podrán ser reguladas por la ley con la finalidad de: a) Garantizar el control de cada persona sobre su propia identidad. b) Garantizar la autodeterminación individual, soberanía y libertad en la toma de decisiones. c) Asegurar la confidencialidad y seguridad de los datos obtenidos o relativos a sus processos cerebrales y el pleno dominio y disposición sobre los mismos. d) Regular el uso de interfaces persona-máquina susceptibles de afectar a la integridad física o psíquica. e) Asegurar que las decisiones y procesos basados en neurotecnologías no sean condicionadas por el suministro de datos, programas o informaciones incompletos, no deseados, desconocidos o sesgados. 2. Para garantizar la dignidad de la persona, la igualdad y la no discriminación, y de acuerdo en sucaso con los tratados y convenios internacionales, la ley podrá regular aquellos supuestos y condiciones de empleo de las neurotecnologías que, más allá de su aplicación terapéutica, pretendan el aumento cognitivo o la estimulación o potenciación de las capacidades de las personas.

[3] Constituição do Estado do Rio Grande do Sul (1989)“Art. 235. .....Parágrafo único. A política e a pesquisa científica e tecnológica basear-se-ão no respeito à vida, à saúde, à dignidade humana, à integridade mental do ser humano e aos valores culturais do povo, na proteção, controle e recuperação do meio ambiente, e no aproveitamento dos recursos naturais. (alterado pela Emenda Constitucional nº 85/2023)"

conecta indivíduos a redes digitais, existe o potencial de borrar a linha entre a consciência de uma pessoa e as entradas tecnológicas externas. Em ambientes de realidade virtual ou aumentada, as fronteiras entre o mundo físico e o digital podem se tornar difusas (TRANSFORMAÇÃO DIGITAL, 2018). Proteger o Direito à Identidade Pessoal implica garantir que a pessoa mantenha controle sobre sua identidade e privacidade quando interage com esses ambientes. A série antológica de ficção especulativa 'Black Mirror', distribuída pelo serviço de streaming Netflix, abordou no episódio 'Joan é péssima' as possíveis consequências da perda do controle sobre a própria identidade no mundo digital. Neste episódio, a personagem Joan descobre que acontecimentos de sua vida estão sendo recontados à medida que ocorrem em um programa de televisão (JOAN, 2023). Na série, a utilização da identidade de Joan foi autorizada pela assinatura dos termos e condições de um serviço de streaming fictício.

O Direito à Identidade Pessoal pressupõe que uma pessoa não deve ser submetida a manipulações de sua identidade através de imagens geradas por computação gráfica, jogos de realidade virtual ou aplicações do metaverso sem o seu consentimento. No entanto, ao se presumir que o uso de neurotecnologias com fins de aprimoramento é inevitável e que o acesso equitativo deve ser promovido, é necessário avaliar que qualquer intervenção no cérebro pode causar alguma alteração na mente e potencialmente ameaçar a identidade pessoal (IWRY et al., 2017). Nesse sentido, um neurodireito ao aprimoramento cognitivo entra em uma antinomia com o Direito à Identidade Pessoal. Dependendo da definição de si mesmo, identidade e autenticidade, proibir a tecnologia de alterar esses traços pessoais pode implicar na proibição das neurotecnologias em geral. Assim, um dos grandes obstáculos para a implementação deste neurodireito é a dificuldade de delinear os limites na definição da identidade pessoal e sua interrupção (INGLESE; LAVAZZA, 2021).

O Direito ao Livre-arbítrio, por sua vez, visa proteger a autonomia e a capacidade de decisão individual, sem interferências indevidas de tecnologias externas. Essa proteção implica que os indivíduos devem ter controle sobre seu próprio processo de tomada de decisão, sem manipulações ocultas provenientes de neurotecnologias externas. Em alguns casos, as neurotecnologias têm sido exploradas para influenciar a opinião pública e o comportamento político, o que

pode incluir o uso de técnicas de neuromarketing em campanhas políticas. As campanhas bem-sucedidas de Barack Obama nos Estados Unidos em 2008 e de Maurício Macri na Argentina em 2015, para os cargos de presidente de seus respectivos países, utilizaram técnicas de neuromarketing para persuadir eleitores (ZIMMERMANN, 2021). Para proteger o Direito ao Livre-arbítrio, é necessário estabelecer regulamentações que assegurem que as escolhas políticas dos indivíduos sejam feitas de maneira informada e autônoma. O caso Cambridge Analytica, um escândalo de dados envolvendo a coleta não autorizada de informações pessoais de milhões de usuários do Facebook, destaca-se significativamente no contexto do neuromarketing (CADWALLADR, 2018). O caso trouxe à tona o problema do targeting psicológico, uma técnica de neuromarketing, que já vinha sendo implementado por várias agências de publicidade e para o qual o Facebook havia patenteado tecnologia semelhante em 2012 (NOWAK; ECKLES, 2012). Este caso destaca a interseção entre neuromarketing e o uso de grandes volumes de dados para influenciar comportamentos e decisões, demonstrando as implicações éticas e legais que surgem quando a tecnologia ultrapassa os limites da privacidade e do consentimento informado.

No entanto, parece conceitualmente problemático propor um neurodireito sob a denominação de “Direito ao Livre-arbítrio”. O livre-arbítrio é uma questão filosófica que tem sido objeto de estudo por filósofos há mais de dois milênios. Platão e Aristóteles refletiram sobre o conceito de controle sobre as próprias ações. Platão, em "A República", discutiu aspectos racionais, espirituosos e apetitivos da alma humana, vendo a liberdade como uma forma de autodomínio (PLATÃO, 1972). Aristóteles, particularmente em "Ética a Nicômaco", enfatizou o papel da escolha no início de ações que formam hábitos e caráter, afirmando que os humanos têm o poder de agir ou não agir, e que as escolhas são voluntárias (ARISTÓTELES, 1991). Durante a era helenística, debates sobre o livre-arbítrio frequentemente focavam nos conceitos de determinismo e de destino. Os estóicos, como Crísipo, acreditavam no determinismo causal, mas argumentavam que as ações humanas ainda estavam 'a nosso critério'. Por outro lado, os epicuristas, seguindo Epicuro, postulavam que os átomos, constituintes da alma, poderiam ter 'desvios', introduzindo um elemento de imprevisibilidade ou liberdade (O'CONNOR; FRANKLIN, 2022).

Santo Agostinho, por sua vez, desempenhou um papel crucial na conexão entre o pensamento antigo e medieval sobre o livre-arbítrio. Sua obra "O Livre Arbítrio", aborda o conceito do mal surgindo do uso indevido do livre-arbítrio e da vontade humana corrompida que necessita da graça divina para salvação (AGOSTINHO, 1995). As visões de Agostinho sobre o livre-arbítrio são debatidas, com algumas interpretações o vendo como um proponente do livre-arbítrio libertário e outras como uma espécie de compatibilista (O'CONNOR; FRANKLIN, 2022). Tentando sintetizar a filosofia de Aristóteles com a teologia cristã, Tomás de Aquino via a vontade como naturalmente inclinada para a bondade. Ele discutiu como a liberdade entra em jogo ao considerar vários meios para alcançar fins, sendo a vontade livre na escolha dos meios. A posição de Aquino sobre o livre-arbítrio é complexa, com algumas interpretações sugerindo compatibilismo e outras inclinando-se para o libertarianismo (KANE, 2012). Um importante defensor medieval de uma concepção fortemente libertária da vontade, John Duns Scotus argumentou que a vontade é a causa total de sua atividade, afirmando que, mesmo diante de bens atraentes, a vontade retém a liberdade de se abster de desejá-los (HARRIS, 2012).

Na filosofia contemporânea, o debate sobre o livre-arbítrio está longe de ser uma questão pacífica. Atualmente, existem duas posições principais: compatibilismo e incompatibilismo (MUÑOZ, 2012). Por um lado, o compatibilismo é a tese de que é metafisicamente possível que o determinismo seja verdadeiro e que as pessoas tenham livre-arbítrio (MCKENNA; PEREBOOM, 2016; VAN INWAGEN, 2017). Por outro lado, o incompatibilismo radical é a tese de que nossas ações são ou eventos determinísticos ou verdadeiramente aleatórios, e ambas as possibilidades excluem o livre-arbítrio e a responsabilidade moral (PEREBOOM, 2003). Há inclusive quem defenda a tese de a humanidade habita uma simulação[4] criada por uma inteligência artificial avançada, não restando espaço para livre-arbítrio (BOSTROM, 2003).

[4] A hipótese da simulação é a hipótese de que a humanidade vive em uma simulação. A hipótese da simulação é uma hipótese metafísica, não epistêmica, mas alguns argumentam que a consideração cuidadosa da hipótese metafísica pode ensinar lições epistêmicas valiosas. A hipótese da simulação está relacionada à hipótese da física digital, ou seja, a hipótese de que a realidade física (ou, de qualquer forma, a porção dela com a qual estamos em contato) é, em última análise, computacional ou 'digital'. No entanto, a hipótese da simulação afirma ainda que existe algum tipo de realidade superior, presumivelmente incluindo um criador, vivendo fora da simulação.

Ademais, a própria neurociência tem produzido argumentos que questionam a existência do livre-arbítrio. Um dos mais famosos é o experimento de Benjamin Libet na década de 1980 (LIBET et al., 1983). Libet mediu a atividade cerebral de participantes que foram instruídos a realizar um movimento simples do pulso. Ele descobriu que a atividade cerebral, especificamente o Potencial Preparatório, começava cerca de meio segundo antes dos participantes terem consciência da decisão de mover o pulso. Esse experimento sugeriu que as decisões podem ser iniciadas por processos cerebrais inconscientes antes de se tornarem conscientes, questionando assim a noção tradicional de livre-arbítrio. Desse modo, a tentativa de estabelecer o livre-arbítrio como uma categoria de neurodireitos pode encontrar obstáculos na definição de termos conceituais (MUÑOZ, 2019).

Já o Direito à Privacidade Mental significa que quaisquer dados obtidos a partir da captação da atividade neural devem ser mantidos em privacidade. Além disso, a venda, transferência comercial e uso desses dados neurais devem ser rigorosamente regulamentados. Por exemplo, pesquisadores estão experimentando o uso 'passthoughts' (pensamentos-senha) como uma alternativa às senhas tradicionais. Essa neurotecnologia torna possível que pessoas acessem diversos dispositivos e plataformas utilizando apenas seus pensamentos (WALTZ, 2016). Esta inovação tecnológica, embora promissora, levanta questões significativas relacionadas ao Direito à Privacidade Mental. A utilização de 'passthoughts' implica um acesso direto a dados neurais extremamente pessoais e únicos de cada indivíduo. Um acesso a dados de modo semelhante ocorre com o uso do já mencionado dispositivo Insight da Emotiv, o qual pode ser utilizado para o controle de ferramentas e aparelhos apenas com o pensamento. Tais dados, se mal administrados ou inadequadamente protegidos, podem expor os usuários a riscos de privacidade, como o acesso não autorizado a informações cerebrais que poderiam revelar muito mais do que a simples intenção de desbloquear um dispositivo ou acessar uma plataforma. Nesse contexto, técnicas como a aprendizagem federada[5] estão sendo desenvolvidas para proteger e garantir a

[5] A aprendizagem federada é um modelo de aprendizado de máquina que permite treinar algoritmos de forma distribuída, mantendo os dados nos dispositivos dos usuários, em vez de centralizá-los em um único servidor. Este modelo é projetado para melhorar a privacidade e a segurança, reduzindo a necessidade de transferir dados pessoais para um servidor central. Na aprendizagem federada, um algoritmo é enviado aos dispositivos dos usuários, onde é treinado localmente com os dados

segurança de informações valiosas. Esse modelo de aprendizado de máquina visa fornecer processamento de dados local, de modo que as informações pessoais possam ser utilizadas por algoritmos de IA enquanto mantêm a integridade dos dados e a privacidade dos usuários. Atualmente, sistemas confiáveis de aprendizagem federada estão sendo implementados em redes móveis (Kang et al., 2020) e, com o avanço da tecnologia, essas técnicas poderão ser utilizadas para o tratamento de dados neurais no futuro.

O Direito ao Acesso Equitativo às Tecnologias de Aprimoramento Cognitivo, por sua vez, busca estabelecer diretrizes tanto em níveis internacionais quanto nacionais regulamentando o desenvolvimento e as aplicações de neurotecnologias de potencialização mental. Essas diretrizes devem ser fundamentadas no princípio da justiça e garantir a igualdade de acesso a todos os cidadãos. Um grupo de pesquisadores militares nos Estados Unidos está desenvolvendo um implante cerebral capaz de restaurar recordações, com potencial para beneficiar pessoas com Mal de Alzheimer e soldados com lesões cerebrais. O dispositivo visa interagir diretamente com o hipocampo para restaurar a memória declarativa (EXAME, 2014). Contudo, essa inovação tecnológica levanta questões importantes relacionadas ao direito ao acesso equitativo a tais tecnologias. A equidade no acesso a essas tecnologias é crucial para garantir que todos os segmentos da sociedade, independentemente de sua condição socioeconômica ou geográfica, possam se beneficiar desses avanços. No entanto, a criação de criar um direito que promova o acesso a tecnologias de aprimoramento, pois isso pode levar a possíveis aplicações transumanistas[6] que podem exigir certa cautela.

À medida que a alteração da natureza humana[7] se torna um fato social, a liberdade daqueles que não desejam se aprimorar pode ser significativamente

---

disponíveis nesses dispositivos. Posteriormente, apenas os parâmetros ou atualizações do modelo são enviados de volta ao servidor central, onde são agregados para melhorar o modelo geral. Isso permite que o algoritmo aprenda com uma ampla gama de dados sem comprometer a privacidade individual dos dados.

[6] O transumanismo é uma corrente filosófica e cultural que defende o uso de tecnologias avançadas para melhorar as capacidades humanas, tanto físicas quanto mentais. Ele explora o potencial para a humanidade ultrapassar as limitações biológicas atuais por meio da aplicação de avanços tecnológicos, como a engenharia genética, a nanotecnologia, a inteligência artificial e a biotecnologia.

[7] Fukuyama (2002) define que "a natureza humana é o somatório dos comportamentos e características típicas da espécie humana, decorrentes de fatores genéticos em vez de ambientais". Pepperell (2003), por sua vez, defensor do pós-humanismo, sustenta que: “a era pós-humana

afetada. Isso poderia levar a criação de padrões sociais, trabalhistas e acadêmicos que exerceriam pressão sobre pessoas que não optassem pelo aprimoramento, as quais poderiam ser consideradas inferiores nesses campos em comparação com seus pares aprimorados. O exposto entra em contradição com o neurodireito ao livre-arbítrio, no sentido de que as pessoas não estariam dando consentimento livre de vícios, mas sim cedendo diante das novas normas sociais criadas com esse novo direito ao aprimoramento cognitivo. Ademais, um neurodireito ao aprimoramento, se não adequadamente limitado, pode implicar que o Estado deveria assumir um novo ônus financeiro para fornecer e subsidiar esses tipos de tecnologias a grupos vulneráveis de cidadãos. Ocorre que em muitas nações em desenvolvimento, o Estado não é capaz de suprir necessidades básicas como nutrição, saneamento ou mesmo garantir a proteção dos direitos humanos. Consequentemente, as diferenças entre países desenvolvidos e em desenvolvimento poderão ser ampliadas, aumentando as assimetrias de poder. Além disso, este neurodireito pode atender mais aos interesses corporativos das empresas que desenvolvem neurotecnologias do que aos indivíduos, uma vez que o Estado estaria financiando aquisições de tecnologias cujos propósitos não são estritamente terapêuticos, nem de saúde pública, apenas em razão deste novo direito (BORBÓN, 2021).

E, por fim, o Direito à Proteção Contra Vieses Algorítmicos significa que contramedidas para prevenir que as pessoas sejam discriminadas com base em qualquer fator, tal como um mero pensamento, que possa ser obtido por meio do uso de neurotecnologias. À medida que os algoritmos de inteligência artificial se tornam mais comumente usados, amplia-se o potencial de dano dos vieses algorítmicos. Como solução, a Neurorights Foundation propõe a inclusão de dados de grupos de usuários demograficamente relevantes nos conjuntos de dados de treinamento dos algoritmos. Entretanto, conforme mencionado por Danks e London (2017), muitos desses vieses são neutros ou podem até ser benéficos. Os autores destacam que, em alguns casos, um viés algorítmico pode ser usado para mitigar o efeito de outro e contribuir para o desempenho do sistema de acordo com os

---

começa quando não encontramos mais necessário, ou possível, distinguir entre humanos e natureza; um momento em que realmente passamos da condição humana para a condição pós-humana de existência".

padrões éticos e legais relevantes. Além disso, este direito estabelece a necessidade de incluir contribuições de grupos de usuários para abordar fundamentalmente o viés. No setor tecnológico, compartilhar os dados usados para treinar sistemas inteligentes pode ser uma ferramenta de promoção da transparência, a partir da qual outros podem trabalhar ativamente para melhorar a responsabilidade dos algoritmos (BUOLAMWINI; GEBRU, 2018). Contudo, montar um conjunto de dados não tendencioso nem sempre é possível ou sustentável. Em muitos casos, os dados e algoritmos utilizados comercialmente são protegidos por direitos autorais e patentes. Isso torna o processo de criação de conjuntos de dados representativos uma tarefa custosa do ponto de vista financeiro, e/ou inexequível do ponto de vista legal, porque a divulgação das informações deve ser limitada devido a questões de privacidade e proteção de dados.

Esses cinco direitos se baseiam, expandem e/ou especificam os direitos humanos reconhecidos internacionalmente para a proteção da dignidade humana, liberdade e segurança das pessoas, não discriminação, igualdade de proteção e privacidade (ONU, 1948). A ideia subjacente é que, em suas versões anteriores, esses direitos abordam de forma muito genérica certas dimensões eticamente relevantes da vida humana, frequentemente sujeitas a interpretação, e a regulamentação das ramificações da neurotecnologia requer maior especificidade (Yuste et al., 2017; 2021). Desse modo, o Direito à Identidade Pessoal enfatiza a proteção da dignidade humana no contexto das neurotecnologias. O Direito ao Livre-arbítrio aplica o direito à liberdade de forma específica ao tema. Por sua vez, o Direito à Proteção Contra Vieses Algorítmicos é uma manifestação do direito à não discriminação como neurodireito. Já o Direito ao Acesso Equitativo às Tecnologias de Aprimoramento Cognitivo é uma adaptação do direito à igualdade. E, por último, o Direito à Privacidade Mental especifica o já consagrado direito à privacidade frente ao paradigma dos avanços neurotecnológicos.

Goering et. al (2021) alinham-se com Ienca e Andorno (2017) ao reconhecerem a necessidade de direitos explicitamente declarados para que os indivíduos possam manter seu espaço mental interno livre de acessos e manipulações indesejadas. No entanto, os pesquisadores vão além do reconhecimento dos neurodireitos ao examinarem os dilemas éticos relacionados ao desenvolvimento de neurotecnologias. Para enfrentar esses dilemas, eles

propõem a realização de cúpulas democráticas e inclusivas com o objetivo de estabelecer diretrizes éticas e sociais coordenadas globalmente para o desenvolvimento e aplicação de neurotecnologia, bem como novos métodos de identificação e prevenção de vieses. Além disso, eles recomendam diretrizes públicas para a distribuição segura e equitativa de dispositivos neurotecnológicos.

A recente cúpula global sobre segurança em inteligência artificial (IA), realizada em Londres em novembro de 2023, fornece um modelo perspicaz para prever os resultados de uma futura cúpula sobre neurotecnologias. Assim como a cúpula de IA (NATURE, 2023), uma cúpula focada em neurotecnologias enfrentaria desafios semelhantes, incluindo a necessidade de regulamentação, a diversidade de opiniões sobre como essa regulamentação deve ser implementada e a dinâmica de poder entre os principais blocos geopolíticos.

A cúpula de IA destacou um consenso global sobre a necessidade de regulamentar tecnologias emergentes. Isso se aplica igualmente às neurotecnologias, que, como a IA, apresentam riscos potenciais significativos que necessitam de diretrizes internacionais. Nesse sentido, a regulamentação é crucial para garantir que essas tecnologias sejam desenvolvidas e utilizadas de maneira ética e segura. Contudo, da mesma forma que houve desacordo sobre como regular a IA (COULTER; SANDLE, 2023), é provável que uma cúpula sobre neurotecnologias também revele divergências. Diferentes países ou blocos podem ter visões variadas sobre questões como privacidade de dados, ética no uso de neurotecnologias e o equilíbrio entre inovação e regulamentação

Ademais, a cúpula de IA ilustrou como os principais blocos de poder, como os EUA, a UE e a China, tentaram impor sua dominância. Em uma cúpula de neurotecnologias, essa mesma dinâmica de poder seria evidente, com cada bloco buscando influenciar as normas globais de acordo com seus próprios interesses e valores. Isso poderia levar a negociações complexas e a um acordo final (REINO UNIDO, 2023) que reflete uma falta de compromisso entre essas diferentes posições. Nesse sentido, a cúpula de IA oferece um exemplo prático de como uma cúpula sobre neurotecnologias poderia se desdobrar. Questões de regulamentação, divergências sobre abordagens e a luta pelo poder geopolítico são prováveis de serem características centrais, assim como foram na cúpula de IA.

Aprimorar o consentimento informado para neurotecnologia é outra recomendação proposta por Goering et. al (2021). Os pesquisadores defendem que os usuários sejam plenamente informados sobre os possíveis efeitos psicossociais antes da adoção de qualquer dispositivo neural, com atenção para garantir que os indivíduos compreendam os riscos a curto e longo prazo. Eles prescrevem que o processo de consentimento para o uso de neurotecnologias deve ser específico e que "os esforços futuros devem garantir que os dados cerebrais sejam incluídos como uma classe emergente de dados pessoais sensíveis". Além disso, propõem que a postura padrão em relação a qualquer coleta de dados neurais exija uma autorização explícita "opt-in"[8]. Isso significa que os dados cerebrais não devem ser coletados passivamente ou depender da opção de "opt-out"[9] por parte dos indivíduos que não desejam que seus dados sejam coletados. Em vez disso, segundo os pesquisadores, o padrão deve exigir que os controladores de dados obtenham um consentimento específico não apenas para a coleta de dados, mas também para como os dados serão usados, para que finalidade e por quanto tempo. A definição atual de consentimento, contudo, não leva em conta as mudanças de percepção e cognição que as próprias neurotecnologias podem induzir (CINEL; VALERIANI; POLI, 2019). Isso cria um paradoxo: o indivíduo que dá consentimento pode não ser o mesmo, em termos de cognição e percepção, após a adoção da neurotecnologia. Assim, o consentimento inicial pode não refletir adequadamente as escolhas ou preferências da pessoa afetada pela tecnologia.

Outra recomendação proposta por Goering et al. (2021) é que a criptografia de dados neurais seja mantida ao longo de todo o seu tratamento. Por exemplo, usando criptografia homomórfica[10], os dados podem ser analisados enquanto

[8] O modelo de escolha “opt-in” pode ser definido como um sistema onde os indivíduos precisam dar um consentimento explícito e proativo para participar ou receber certos serviços, ofertas ou comunicações. No contexto da privacidade de dados, por exemplo, o modelo "opt-in" é considerado uma prática mais respeitosa e segura, pois garante que as informações pessoais dos usuários sejam coletadas e processadas apenas após eles terem dado consentimento explícito.

[9] O modelo de escolha "opt-out" refere-se a um sistema de consentimento em que os indivíduos são automaticamente inscritos em um serviço ou programa, e devem tomar uma ação específica se desejarem não participar. Neste modelo, presume-se que os indivíduos concordam com a participação ou com o recebimento de determinadas comunicações ou serviços até que expressem explicitamente seu desejo de se excluir. Na privacidade de dados, é considerado prejudicial ao consentimento informado e à autonomia do usuário, pois pode potencializar a falta de atenção ou entendimento e ampliar a necessidade de esforço do indivíduo para se desinscrever.

[10] A criptografia homomórfica é um tipo avançado de criptografia que permite a realização de operações computacionais em dados criptografados sem a necessidade de descriptografá-los

permanecem criptografados (KHEDR; GULAK, 2017). Entretanto, a criptografia homomórfica ainda é uma tecnologia emergente e computacionalmente intensiva, o que pode limitar sua aplicabilidade prática, especialmente em dispositivos com recursos limitados. De modo semelhante, os pesquisadores propõem que a coleta e o armazenamento devem ocorrer em formatos de dados abertos usando código aberto, mas com rastreamento de blockchain[11]. Em um contexto acadêmico, isso significa que os dados neurais devem ser coletados e armazenados de maneira que sejam acessíveis e compreensíveis, promovendo a colaboração e a replicabilidade da pesquisa. Ao mesmo tempo, ao aplicar o blockchain à gestão de dados neurais, cada instância de coleta, acesso, modificação ou compartilhamento de dados seria registrada como uma transação no blockchain. Isso torna possível rastrear e verificar todas as interações com os dados, garantindo que qualquer acesso ou uso não autorizado possa ser identificado de forma confiável. Este registro imutável e transparente de transações aumenta a segurança dos dados e facilita a atribuição de responsabilidade em caso de violações de privacidade ou uso indevido dos dados. Complementarmente, a recomendação propões que os dados neurais devem ser governados pelo princípio da necessidade, filtrando e transmitindo apenas os dados mínimos necessários em cada etapa ao longo do percurso dos dados.

Goering et al. (2021) também recomendam uma restrição significativa no compartilhamento ou comércio de dados neurais, devido aos riscos de reidentificação e preocupações relacionadas ao aumento dos mercados comerciais. Essas restrições podem ser comparadas às regulamentações existentes em outros contextos, como o uso comercial de tecidos e órgãos humanos, que são rigorosamente vedados em países como o Brasil (1997). A venda de órgãos é estritamente proibida para evitar incentivos monetários e proteger a integridade do corpo humano. Da mesma forma, proteções semelhantes podem ser necessárias para proteger a privacidade e a integridade mental.

---

primeiro. Essa característica a torna extremamente valiosa para a proteção da privacidade em ambientes de computação em nuvem e em aplicações de análise de dados sensíveis.

[11] O blockchain é um sistema de registro distribuído que mantém um histórico imutável e verificável de todas as transações. Cada bloco de dados no blockchain contém um registro de várias transações, junto com o horário em que ocorreram e um elo para o bloco anterior, criando uma cadeia contínua.

A necessidade de reconhecimento e transparência em relação aos vieses presentes na pesquisa e desenvolvimento de neurotecnologias é outro ponto abordado por Goering et al. (2021). Eles consideram crucial que os vieses, sejam eles apropriados ou inapropriados, intencionais ou não intencionais, sejam reconhecidos ao longo do processo de pesquisa (SULLIVAN et al., 2018). Isso inclui a discussão regular do papel dos vieses relacionados à amostra selecionada, às concepções de bem-estar e qualidade de vida, às pressões dos financiadores ou da indústria, entre outros aspectos. Além disso, defendem que é fundamental comunicar como esses vieses afetam uma intervenção ou produto, seja por meio de publicidade direta ao consumidor, publicações revisadas por pares ou na mídia popular (RACINE, 2007). Contudo, nem sempre é claro o que constitui um viés, especialmente em contextos complexos e multidimensionais como neurotecnologia. Determinar quais vieses são inapropriados ou prejudiciais pode ser subjetivo e variar entre culturas e indivíduos (HE; VAN DE VIJVER, 2012).

Ainda em relação aos vieses, Goering et al. (2021) recomendam o combate ativo aos vieses na pesquisa e no desenvolvimento de neurotecnologias. Eles propõem que estratégias eficazes para combater o viés, tanto estruturais quanto individuais, sejam consideradas. Além disso, defendem a importância da diversificação das equipes de pesquisa. Equipes compostas por membros de diferentes origens, disciplinas e identidades sociais têm maior probabilidade de identificar abordagens alternativas para um problema compartilhado e reconhecer questões que poderiam ser negligenciadas (GOERING; KLEIN, 2019). Nesse sentido, os pesquisadores sugerem que cientistas e especialistas em ética devem colaborar com empresas para garantir que as neurotecnologias sejam desenvolvidas com uma visão ética apropriada. A IBM, por exemplo, desenvolveu um framework de ética para inteligência artificial, comprometendo-se a adotá-lo em seu processo de pesquisa e desenvolvimento (CUTLER; PRIBIĆ; HUMPHREY, 2019). Iniciativas semelhantes podem ser implementadas em relação às neurotecnologias.

Adicionalmente, os pesquisadores defendem a promoção do acesso equitativo às neurotecnologias, com o objetivo de garantir que produtos eficazes sejam subsidiados e disponibilizados para pessoas com baixa renda que desejem utilizá-los. Por fim, Goering et al. (2021) propõem a criação de uma ampla comissão

internacional, com reuniões periódicas, com o objetivo de avaliar os desenvolvimentos em neurotecnologia e fornecer orientações éticas para inovação responsável. Uma iniciativa similar foi realizada em relação às implicações éticas e sociais da edição genética humana (OLSON, 2016). Entretanto, a criação de uma comissão internacional para avaliar e orientar o desenvolvimento ético das neurotecnologias enfrenta o desafio de alcançar um consenso moral e ético em um cenário global diversificado, com diferentes valores culturais e políticos, tal como visto na conferência global sobre IA e repetidas vezes nas conferências globais sobre as mudanças climáticas (MASSAI, 2019).

As recomendações propostas por Goering et al. complementam os neurodireitos listados pela Neurorights Foundation, na perspectiva de estabelecer princípios éticos, transparência e responsabilidade no desenvolvimento e nas aplicações das neurotecnologias. Ao afirmarem categoricamente a necessidade de inclusão dos dados neurais na categoria de dados sensíveis, os pesquisadores ressaltam o alto nível de proteção que deve ser atribuído a esses dados. Nesse contexto, o Direito à Privacidade Mental se destaca entre os direitos propostos pela fundação, por estar intrinsecamente ligado a esta alegada sensibilidade dos dados neurais.

2.3 PRIVACIDADE MENTAL E INTEGRIDADE PSICOLÓGICA

Os princípios básicos relacionados à pesquisa com seres humanos, ou seja, a autonomia, a integridade, a beneficência e a justiça fundamentam as diferentes dimensões de privacidade (SALLES et al., 2017). Segundo Laurie et. al (2010), a privacidade pode ser analisada em termos de privacidade física, relacionada ao acesso a pessoas e espaços pessoais; privacidade da informação, que diz respeito ao acesso a informações pessoais; privacidade decisória, relacionada a interferências de governos e de terceiros em escolhas pessoais; e privacidade proprietária, que se refere à apropriação e propriedade de interesses relacionados à personalidade humana. Por sua vez, a privacidade mental, a ideia de que as pessoas devem ter controle sobre o acesso informacional a seus estados mentais

ou neurais, muitas vezes não é apresentada como uma quinta dimensão de privacidade, mas sim como parte de uma das outras quatro, embora não esteja contida integralmente em nenhuma delas.

Enquanto a privacidade proprietária trata do domínio sobre informações pessoais já externalizadas, a propriedade mental vai além ao abranger uma dimensão interna e íntima do indivíduo. Nesse sentido, a principal diferença entre privacidade mental e privacidade proprietária reside no objeto de proteção. Enquanto a privacidade mental foca nos processos internos e inacessíveis do pensamento e da consciência, a privacidade proprietária lida com informações pessoais que já foram expressas ou registradas de alguma forma. A privacidade mental abrange o que é inerentemente íntimo e não manifestado, enquanto a privacidade proprietária trata do controle sobre informações que já foram externalizadas (ALLEN, 2000). As neurotecnologias podem potencialmente acessar informações que nunca foram expressas ou registradas, entrando no domínio da privacidade mental, que vai além do que a privacidade proprietária pode proteger.

A privacidade decisória, por outro lado, está relacionada ao direito de tomar decisões pessoais sem interferência externa. Ela envolve aspectos como a liberdade de escolha, a autonomia para tomar decisões sobre a própria vida, corpo e futuro, e o direito de agir com base nessas decisões (LAURIE et al., 2010). Enquanto a privacidade mental abrange os processos de pensamento e cognição internos, a privacidade decisória diz respeito à liberdade e autonomia na esfera das ações e escolhas externas que uma pessoa faz. Harari (2018), em suas reflexões sobre a erosão da fronteira entre máquinas eletrônicas e corpos orgânicos, aborda a capacidade emergente de neurotecnologias acessarem e inferirem processos mentais. O conceito de privacidade decisória e a reflexão de Harari (2018) estão interligados, pois ambos destacam o desafio crescente de proteger os processos mentais internos. Contudo, privacidade decisória não abrange completamente a privacidade mental porque os processos de pensamento e cognição internos podem não se traduzir necessariamente em decisões ou ações externas. Harari (2018) destaca a possibilidade de intrusão e análise dos pensamentos, ressaltando a importância crescente da privacidade mental diante do avanço das neurotecnologias. Um indivíduo pode ter pensamentos e ideias que nunca se manifestam em decisões ou comportamentos observáveis. A privacidade decisória

não aborda adequadamente a proteção contra a intrusão ou análise desses processos internos. Com o desenvolvimento de neurotecnologias que podem acessar ou inferir processos mentais, a privacidade mental ganha destaque por seu papel na proteção desses processos internos, que podem ocorrer independentemente de qualquer decisão ou ação externa.

Uma abordagem possível para a proteção dos dados neurais é considerar que, dado que eles satisfazem a definição de informação pessoal, eles são abrangidos pela privacidade da informação. A privacidade da informação é a ideia de que devemos ser protegidos contra os diferentes tipos de danos, por exemplo, discriminação, que podem resultar da difusão de nossos dados pessoais e, portanto, baseia-se nos princípios da beneficência e da justiça (SALLES et al., 2017). Isso implica, por exemplo, na obrigação de anonimizar os dados empregados em contextos de pesquisa. De acordo com essa visão, os neurodireitos já são protegidos pelas regulamentações aplicadas a outros tipos de informação pessoal, como a Lei Geral de Proteção de Dados Pessoais. Assim, se alguém tem uma expectativa razoável de privacidade em relação às informações identificadoras derivadas de amostras de seu sangue ou saliva, também tem uma expectativa razoável de privacidade em relação aos dados decodificados de seu próprio cérebro (SHEN, 2013).

Contudo, em muitas situações, a privacidade da informação não é suficiente para abranger todos os aspectos da privacidade mental. Isto porque, o acesso à informação sobre a mente humana pode, às vezes, ser idêntico ao acesso à própria mente, ou mais especificamente, às suas propriedades informacionais, um fenômeno que Ienca e Andorno (2017) denominam de 'inception problem'[12]. Essa problemática se assemelha à trama do filme *"A Origem"* (INCEPTION, 2010*),* onde os personagens entram nos sonhos uns dos outros, manipulando e acessando informações profundas. No filme, a ideia de alterar ou manipular a mente de uma pessoa sem seu consentimento, exemplificada pelo conceito de "inception", é central, refletindo as preocupações discutidas pelos autores. Assim, a privacidade

[12] O "inception problem", conforme discutido por Ienca e Andorno, aborda a preocupação ética em relação às tecnologias avançadas capazes de acessar ou manipular estados mentais. Este conceito enfatiza o potencial de violação da privacidade mental e da autonomia pessoal, destacando desafios únicos que vão além das preocupações tradicionais de privacidade. O problema ressalta a importância de abordagens regulatórias e legais específicas para proteger contra intrusões não consentidas em estados cognitivos internos, uma questão crítica na era das neurotecnologias.

mental está relacionada ao controle sobre os diferentes aspectos, incluindo, mas não se limitando às propriedades informacionais, que constituem a mente humana. Podemos definir a integridade psicológica como a ideia de que ninguém pode alterar ou manipular a mente de um indivíduo, por exemplo, modular sua informação neural por meio de estimulação cerebral elétrica ou magnética, sem seu consentimento (IENCA; HASELAGER, 2016; LAVAZZA, 2018). Observa-se, nesse sentido, uma relação mais estreita entre privacidade mental e a integridade psicológica do que entre aquela e a privacidade da informação.

Os pesquisadores da Neurorights Foundation, por sua vez, sugerem que, dada a natureza biológica dos sinais que transportam os dados neurais, estes deveriam ser protegidos pela privacidade física (GOERING; YUSTE, 2016; GOERING et al., 2021; YUSTE et al., 2017). Esta dimensão da privacidade está relacionada ao acesso às amostras orgânicas dos corpos das pessoas, considerando o fato de que estas não poderiam ser coletadas e armazenadas sem consentimento e, portanto, tem como base a integridade corporal. Seguindo este mesmo raciocínio, atualmente, tramita na Câmara dos Deputados chilena o Projeto de Lei dos Neurodireitos (número de protocolo 13.828-19), uma proposta que vai além da reforma constitucional, que reconheceu a existência dos neurodireitos, ao buscar salvaguardar os cinco direitos propostos pela Neurorights Foundation. No que diz respeito à privacidade mental, o Projeto de Lei estabelece que os dados neurais são uma categoria especial de dados sensíveis de saúde. Especificamente, o Artigo 7º afirma que “a coleta, armazenamento, tratamento e disseminação dos dados neurais e da atividade neuronal das pessoas serão ajustados às disposições contidas na lei nº 19.451 sobre transplante e doação de órgãos, na medida em que lhe seja aplicável, e às disposições do código sanitário respectivas”[13] (CHILE, 2020, tradução nossa).

Considerando a legislação brasileira, no contexto da privacidade física, sobretudo a Lei 9.434/1997, que dispõe sobre a remoção de órgãos, tecidos e partes do corpo humano, não seria possível o consentimento para a comercialização de dados neurais, permitindo apenas sua doação para fins

[13] Texto original na língua espanhola: Artículo 7: La recopilación, almacenamiento, tratamiento y difusión de los datos neuronales y la actividad neuronal de las personas se ajustará a las disposiciones contenidas en la ley n°19.451 sobre trasplante y donación de órganos, en cuanto le sea aplicable, y las disposiciones del código sanitário respectivas.

altruístas. Entretanto, a ideia de proteger os dados neurais por meio da integridade corporal é enfraquecida por diferenças substanciais entre os dados neurais e os tipos de objetos cobertos pela integridade corporal, ou seja, órgãos ou componentes corporais e tecido orgânico. Além disso, existem diferenças entre a extração de dados neurais e a retirada de órgãos corporais. Uma observação chave, conforme destacado por Montgomery (2017), é que nossos corpos não são a única fonte de dados neurais. Existem fontes externas de dados relacionados à integridade mental, como as análises realizadas por clínicos e pesquisadores ao confrontar dados individuais com informações sobre padrões de ondas cerebrais de outros indivíduos.

Outra diferença entre a extração de dados neurais e a retirada de órgãos corporais é que a primeira não envolve transferência de material orgânico. Esta diferença pode ser explicada usando a distinção de Borgatti (2015) entre replicação e transferência de informações. A comunicação via transferência simplesmente move um objeto portador de informação de uma fonte para um receptor, como enviar uma carta pelo correio a outra pessoa. Por sua vez, a comunicação via replicação consiste em reproduzir uma nova cópia, materialmente diferente, de uma mensagem em outro ponto de uma rede, ou seja, a mensagem material original não sai da fonte, como no caso do envio de um arquivo de um computador para outro.

Nesse sentido, ao contrário de uma biópsia, na qual o tecido contendo dados médicos é extraído e preservado para análise, a coleta de dados neurais se assemelha à replicação de informações. Isso pode ser exemplificado pela gravação de eletroencefalograma (EEG). Os componentes básicos de um sistema de EEG incluem eletrodos ou sensores de voltagem, amplificadores e dispositivos de saída. Inicialmente, os dados contidos nas ondas neurais de íons são replicados por um sinal materialmente diferente constituído por elétrons nos eletrodos do EEG, que são afetados por (ou correlacionados com) essas ondas. Após esse segundo sinal ser amplificado, os dados são replicados novamente em um novo formato material pelos dispositivos de saída. No EEG analógico, isso envolve um sistema de escrita com caneta movido por galvanômetro que registra os dados neurais em papel. No EEG digital, o sinal amplificado é enviado para um circuito ADC (conversor analógico-digital) que produz um sinal digital, uma versão do sinal analógico original, constituído por sequências de dígitos que podem ser armazenados em uma

variedade de mídias físicas (YEH, 2017). Isso significa que o registro físico de dados neurais mantido por pesquisadores para análise muitas vezes não é constituído por nenhum material orgânico.

Uma questão relevante é se, embora possuam propriedades não-orgânicas, os dados neurais ainda assim poderiam ser considerados como algo constitutivo do ser humano. A ausência de transferência material ou orgânica na extração de dados neurais reforça a ideia de que os dados neurais possuem propriedades que são constitutivas do ser humano, mas cuja identidade é relativamente independente do meio físico ou material que as implementa. Estas propriedades neurocognitivas específicas do cérebro humano são, portanto, propriedades funcionais, um tipo de propriedade caracterizada por esta autonomia ontológica. Essa ideia encontra seu fundamento em argumentos clássicos sobre a realizabilidade múltipla[14] e, crucialmente, tem sido argumentado que muitos estados psicológicos são autônomos neste sentido (PUTNAM, 1967). Portanto, embora os dados neurais não sejam análogos aos estados puramente físicos do corpo humano, eles podem ser análogos aos estados psicológicos.

Filósofos mecanicistas[15], como Piccinini (2015) e Milkowski (2013), apontam que alguns mecanismos cognitivos são constituídos por tipos de propriedades, funcionais e estruturais, que exibem certo grau de independência de seu meio

[14] A realizabilidade múltipla é um conceito filosófico importante, especialmente na filosofia da mente e na ciência cognitiva, que se refere à ideia de que uma única propriedade mental ou um único estado mental pode ser fisicamente realizado de várias maneiras diferentes. Em outras palavras, o mesmo estado ou função mental pode ser produzido por diferentes tipos de sistemas físicos. Este conceito foi introduzido para argumentar contra o reducionismo na ciência da mente, sugerindo que explicações puramente físicas ou biológicas podem ser insuficientes para entender completamente os fenômenos mentais. A realizabilidade múltipla sugere que, embora os estados mentais estejam correlacionados com estados cerebrais, eles não são restritos a um tipo específico de substrato físico. Por exemplo, a dor ou a percepção visual poderiam teoricamente ser realizadas por sistemas neurais não-humanos, sistemas de computador ou outras estruturas materiais, desde que a estrutura correta e as funções sejam replicadas. Este conceito tem implicações significativas para o entendimento da mente e da consciência, bem como para o desenvolvimento da inteligência artificial, pois sugere que a mente não é restrita à biologia humana e que a consciência e outros estados mentais podem, em teoria, ser replicados em sistemas não-biológicos.

[15] O mecanicismo, ou filosofia mecânica, é um termo que se refere a uma abordagem na filosofia da ciência e, mais especificamente, na filosofia da mente e da biologia, que enfatiza a compreensão dos sistemas biológicos e mentais em termos de seus mecanismos subjacentes. Esta abordagem procura explicar fenômenos naturais em termos das partes que os compõem e das interações entre essas partes. Historicamente, a filosofia mecânica tem raízes na revolução científica do século XVII e foi influenciada pelas obras de filósofos e cientistas como René Descartes e Isaac Newton, que tentaram explicar os fenômenos naturais em termos de leis mecânicas e princípios de movimento. No contexto contemporâneo, essa abordagem é central em áreas como a neurociência e a biologia molecular, onde a compreensão dos mecanismos a nível celular e molecular é crucial para explicar o funcionamento dos organismos vivos.

físico. Por exemplo, Piccinini (2015) sugeriu que a informação neural e o cálculo neural são constituídos por propriedades "independentes do meio". Assim, um determinado cálculo pode ser implementado em vários meios físicos, por exemplo, mecânico, eletromecânico, eletrônico ou magnético, desde que os meios possuam um número suficiente de dimensões de variação que possam ser adequadamente acessados e manipulados e que os componentes do mecanismo estejam organizados funcionalmente de maneira apropriada (PICCININI; BAHAR, 2013). Desse modo, embora os dados neurais não dependam de material orgânico para sua replicação, eles ainda assim constituem os sistemas neurocognitivos da mente humana (BOONE; PICCININI, 2016).

Ao não constituírem matéria orgânica, os dados neurais são fundamentalmente informações pessoais sobre estados, processos e estruturas neurais. Na filosofia da neurociência, a ideia de carregar informações sobre algo é frequentemente compreendida através do conceito de informação semântica. Piccinini e Scarantino (2011) distinguem entre informação semântica não natural (nNSI) e informação semântica natural (NSI). A informação semântica natural é compreendida em termos de correlações confiáveis entre tipos de eventos (DRETSKE, 1981). Um evento *a* do tipo *A* carrega informação natural sobre um evento *b* do tipo *B* apenas se *A* se correlacionar de forma confiável com *B*. Anéis de árvores, juntamente com outras variáveis, carregam informações sobre a idade da árvore; a perda aguda do olfato ou paladar carrega informação semântica natural sobre a doença Covid-19, entre outros casos. Esta é uma noção frequentemente empregada para caracterizar sinais neurais: estes são "sobre" as propriedades que definem seus campos receptivos. O campo receptivo de um neurônio é caracterizado em termos das propriedades ambientais específicas, por exemplo, barras, bordas, limites etc., cuja instanciação[16] está correlacionada de forma confiável com propriedades específicas de resposta neural, por exemplo, variações na taxa de disparo.

[16] No contexto neural, instanciação refere-se ao processo pelo qual informações ou propriedades específicas são representadas ou expressas no sistema nervoso. Esse conceito está associado à forma como determinadas características, como pensamentos, memórias ou estados cognitivos, são codificadas ou manifestadas em padrões de atividade neural. A instanciação neural envolve a tradução de informações abstratas ou conceitos em padrões específicos de atividade elétrica ou química nos neurônios.

Os diferentes processos de produção de dados neurais implicam que eles estejam sempre correlacionados com propriedades de sinais neurais e, portanto, carreguem informação semântica natural sobre eles. Por exemplo, como visto anteriormente, propriedades de ondas neurais de íons estão correlacionadas com propriedades de elétrons em eletrodos de EEG, que por sua vez estão correlacionados com as sequências de dígitos produzidas pelo conversor analógico-digital (YEH, 2017). Da mesma forma, os sistemas típicos empregados em registros de dados neurais são baseados em correlações entre mudanças de voltagem em neurônios, estados de microeletrodos, amplificadores e dispositivos de gravação. Técnicas de neuroimagem, como PET (tomografia por emissão de pósitrons) ou fMRI (ressonância magnética funcional), também dependem de correlações entre sinais de saída recebidos por dispositivos digitais e variáveis neurofisiológicas, como fluxo sanguíneo ou nível de oxigênio, que, por sua vez, estão correlacionados com padrões de atividade cerebral e processos neurocognitivos.

Nesse contexto, cabe ressaltar que os dados neurais são definidos como informações pessoais sobre processos neurais. Ou seja, não se trata meramente de informação semântica natural sobre propriedades do cérebro de um determinado indivíduo, mas, crucialmente, informações que podem ser rastreadas até este mesmo indivíduo. Em outras palavras, um estado de uma estrutura neural carrega informação neural pessoal apenas se estiver correlacionado com a instanciação de uma determinada propriedade neural em um indivíduo particular. Informações sobre o cérebro nem sempre são pessoais neste sentido. Algumas estruturas têm estados que são causados de maneira confiável pela instanciação de determinada propriedade em diferentes indivíduos. Portanto, esses estados fornecem apenas informações existenciais sobre a instanciação desta propriedade, ou seja, a informação de que existe um cérebro no qual ela foi instanciada. Por exemplo, uma configuração específica de elétrons em eletrodos de EEG poderia ser causada pela instanciação de um padrão específico de atividade neural em vários cérebros diferentes. Esse sinal revela apenas que o padrão foi instanciado em algum cérebro conectado aos eletrodos de EEG, sem ser capaz de indicar a quem o cérebro pertence (PAZ, 2022).

A proteção de dados neurais pessoais é crucial, principalmente porque em determinados contextos, esses dados podem ser usados para prejudicar indivíduos,

principalmente ao possibilitar comportamentos discriminatórios ou estigmatizantes. Nesses contextos, as informações podem ser especificamente vinculadas aos indivíduos afetados. É por esta razão que uma das tecnologias-chave desenvolvidas para a proteção de dados são os métodos de anonimização (PAZ, 2022). Estes visam transformar os dados de tal maneira que eles não possam ser rastreados de volta aos indivíduos que os originaram, ou seja, de forma que os sujeitos não possam ser reidentificados.

A identificação, o processo de produção de dados pessoais, requer a junção de uma parte de dados existenciais d1, ou seja, informações sobre a instanciação de uma determinada propriedade em algum indivíduo, como registros digitais produzidos por dispositivos de EEG, com outros dados ou informações (d2, d3, ... dn). Dessa forma, uma estrutura que carrega o conjunto {d1, d2, d3, ... dn} estaria especificamente correlacionada com a instanciação de uma propriedade específica em um determinado indivíduo. A identificação é frequentemente alcançada por meio de identificadores, que são partes de informação exclusivamente relacionadas a *um* indivíduo, como um nome ou número de identidade. Quando esses identificadores são removidos, obtém-se dados desidentificados. No entanto, considerando que existem maneiras alternativas de alcançar a identificação, dados desidentificados não são equivalentes a dados anonimizados. A anonimização requer a remoção ou distorção de quase-identificadores, que são dados não exclusivamente relacionados a um sujeito particular, como estado civil, idade, gênero etc., mas que podem ser usados juntamente com outras informações para identificá-lo de maneira confiável. Em outras palavras, um identificador pode ser produzido juntando diferentes quase-identificadores (SALLES et al., 2017).

Ao determinar o tipo de informação semântica natural (NSI) transmitida pelos dados neurais de um determinado indivíduo, é necessário avaliar se essa NSI é um dos estados, processos ou estruturas cobertas por sua integridade psicológica (PAZ, 2022). Como mencionado anteriormente, a integridade psicológica é a ideia de que o consentimento informado do sujeito é necessário para alterar ou manipular os componentes de sua mente. Um tipo de estado mental, como uma experiência perceptiva particular, pertence à mente de um indivíduo porque é nela que ele é instanciado. Sendo eventos particulares com propriedades espaço-temporais específicas, esses estados não são instanciados simultaneamente em diferentes

cérebros. Portanto, essa condição pode ser suficiente para explicar por que um determinado estado mental pertence exclusivamente a identidade neural de um sujeito específico.

A capacidade que um determinado indivíduo possui de pensar e raciocinar sobre os estados mentais de seu cérebro implica que seu cérebro efetivamente instancia e processa o tipo específico de informação que define seus dados neurais. No entanto, isso é insuficiente para determinar que esta informação lhe pertence no sentido relevante (PAZ, 2022). O dilema surge quando se diz que alguma informação pessoal sobre um indivíduo pertence a este mesmo indivíduo, isto é, que ele tem o direito exclusivo de controlar essa informação, não apenas sobre uma instância particular desta informação, mas sim sobre o tipo de informação em si. Qualquer instância desta informação pertence ao individuo neste sentido, ou seja, ele tem o direito de controlar qualquer cópia física de sua informação pessoal. No entanto, um determinado tipo de informação na maioria das vezes não é instanciado exclusivamente em um objeto específico. Especificamente, muitas instâncias dos dados neurais de um individuo podem ser realizadas em estruturas físicas separadas de seu cérebro, como registros digitais em dispositivos de gravação ou neurodispositivos acoplados a seu corpo. Assim, visto que “ser instanciado em” não é uma relação exclusiva entre um determinado indivíduo e seus dados neurais, o local da instância não é suficiente para fundamentar o controle exclusivo sobre esta informação.

Para a maioria dos tipos de dados pessoais, aqueles protegidos pela privacidade da informação, a conexão exclusiva entre a informação e um indivíduo específico é determinada simplesmente pelo conteúdo semântico: qualquer instância desta informação pertence a um individuo porque é sobre este e não sobre qualquer outro. Em contraste, a propriedade de um indivíduo sobre seus dados neurais pode ser fundamentada na integridade psicológica, pois existe uma conexão ontológica distinta entre este tipo de informação e seu cérebro que satisfaz a condição de exclusividade. Diferentes tipos de informações podem moldar a arquitetura cognitiva humana, isto é, o conjunto de estruturas relativamente fixas ou estáveis através das quais as capacidades mentais são implementadas (PYLYSHYN, 1998). Embora a maioria das propriedades que definem as arquiteturas cognitivas seja compartilhada por diferentes cérebros, os dados neurais

sobre um cérebro específico constituem um aspecto único da arquitetura desse cérebro. Isso porque, existe um segundo sentido no qual as informações podem fazer parte dos sistemas cerebrais humanos, um sentido que envolve mais do que a mera instanciação de informações e se refere a própria constituição da mente.

Uma noção frequentemente empregada para caracterizar como diferentes tipos de informação moldam os sistemas cognitivos humanos é a de especificidade de domínio. Alguns tipos de mecanismos mentais são ditos como constituindo módulos, que são sistemas especializados para realizar funções cognitivas específicas (FODOR, 1983) e são frequentemente definidos por um conjunto de características especiais, como encapsulação informacional e arquitetura neural fixa, entre outros (ROBBINS, 2017). Uma das principais características implicadas pela especialização funcional é a especificidade de domínio. Um sistema é específico de domínio na medida em que existe um tipo de informação ao qual ele é dedicado para processar. Alguns exemplos típicos incluem sistemas para percepção de cor, análise de forma visual, análise de frases e reconhecimento de rostos e vozes (FODOR, 1983).

Naturalmente, definir um domínio no cérebro de um indivíduo específico muitas vezes não é uma relação exclusiva entre um tipo de informação unicamente neste cérebro. Os domínios de muitos sistemas cognitivos são amplamente compartilhados por diferentes cérebros, por exemplo, informações sobre forma visual, movimento, cor etc. Esta relação pode fundamentar os direitos exclusivos deste indivíduo em relação ao tipo de informação apenas se esta definir um domínio que seja único para sua arquitetura cognitiva (CARRUTHERS, 2006). Na maioria das vezes, os domínios informacionais são entendidos em um sentido intensional[17]. Dizer que diferentes sistemas cognitivos compartilham um domínio, significa que eles são dedicados a processar informações sobre os mesmos tipos de propriedades. No entanto, também é possível dizer que os domínios são compartilhados no sentido de que eles processam informações sobre a instanciação

[17] O termo intensional (com s) refere-se a um conceito relacionado à maneira como o significado ou o conteúdo de uma expressão, termo ou conceito é entendido e definido. Em filosofia, lógica e linguística, a intensionalidade está relacionada com as propriedades, atributos ou critérios que um objeto precisa satisfazer para ser incluído no conteúdo ou na extensão de um termo ou conceito. A intensionalidade é frequentemente contrastada com a "extensão", onde a extensão se refere ao conjunto de todos os objetos que realmente satisfazem as propriedades definidoras de um conceito. Enquanto a intensionalidade lida com as propriedades e critérios de inclusão, a extensão lida com os objetos reais que se enquadram nesses critérios.

dessas propriedades no mesmo conjunto de objetos. Neste caso, eles compartilham o que podemos chamar de dimensão extensional de um domínio. Por exemplo, subsistemas visuais de diferentes cérebros podem processar informações sobre um conjunto comum de propriedades, como forma, posição, movimento, cor etc. (domínios intensionais compartilhados), instanciados em um conjunto comum de objetos disponíveis para todos eles no ambiente externo (domínios extensionais compartilhados). Em contraste, mecanismos interoceptivos[18] em diferentes cérebros processam informações sobre a instanciação das mesmas propriedades, por exemplo, estados dos sistemas cardiovascular, respiratório ou gastrointestinal, em diferentes objetos, ou seja, no corpo ao qual cada mecanismo pertence. Ou seja, os domínios desses mecanismos são extensionalmente únicos (SAMUELS, 2000).

Como mencionado anteriormente, um domínio é definido por um tipo particular de conteúdo informacional e a caracterização de conteúdo em mecanismos neurais ocorre em termos de informação semântica. Além disso, a informação semântica é sensível a diferenças tanto nos aspectos intensionais quanto extensionais do conteúdo. Assim é possível distinguir informações sobre a instanciação de uma propriedade em um determinado sujeito de informações sobre a instanciação da mesma propriedade em um sujeito diferente. Portanto, a dimensão extensional é parte do conteúdo que define um determinado domínio cognitivo (PAZ, 2022).

No sistema interoceptivo, os sinais que as estruturas neurais produzem respondem seletivamente às instanciações de uma propriedade específica no corpo de um indivíduo específico e, crucialmente, eles não responderiam à instanciação dessa propriedade em outro indivíduo. De acordo com a definição de informação pessoal, isso implica que a informação semântica natural que esses aferentes carregam é pessoal. Seus sinais estão correlacionados com a instanciação de uma determinada propriedade em um indivíduo particular. Por exemplo, a cardiopercepção depende de neurônios sensoriais no coração de um indivíduo que detectam pressão, frequência cardíaca, ritmo cardíaco e hormônios, os quais servem como entradas para vias ascendentes tanto na coluna vertebral quanto nos

[18] Sistema interoceptivo refere-se ao conjunto de estruturas e processos fisiológicos no corpo humano responsáveis pela percepção e interpretação das sensações internas do corpo. Este sistema está fundamentalmente envolvido na detecção e regulação dos estados internos do organismo, tais como a fome, a sede, o equilíbrio de fluidos, a temperatura corporal e a dor interna.

nervos vagos, viajando do coração para a medula, hipotálamo, tálamo e amígdala e, em seguida, para o córtex cerebral (PAZ, 2022). Dado que um sinal carregando informações sobre uma determinada frequência cardíaca depende exclusivamente desta via descrita conectando o coração de um indivíduo específico ao cérebro deste mesmo individuo, o sinal não seria ativado se esta frequência não fosse instanciada pelo coração do próprio indivíduo, mas sim pelo coração de outra pessoa. De modo geral, a informação que esses mecanismos processam é pessoal porque seu padrão característico de conexões determina que existe apenas um objeto com a estrutura neural necessária para instanciar determinada propriedade específica em um sujeito particular.

Além disso, o objeto na origem dos mecanismos do sistema interoceptivo em diferentes corpos será diferente. Os domínios dos mecanismos interoceptivos de diferentes cérebros são extensionalmente distintos. Embora esses mecanismos carreguem informações sobre os mesmos tipos de propriedades, comuns a todas as pessoas, cada mecanismo processará apenas informações sobre a instanciação dessas propriedades no corpo do indivíduo particular a que pertence (PAZ, 2022). O mecanismo de cardiopercepção de um indivíduo específico é dedicado a coletar e processar informações sobre pressão, frequência, ritmo e hormônios do coração apenas deste indivíduo. É neste sentido que os domínios dos mecanismos interoceptivos são únicos para cada organismo.

Ienca e Andorno (2017) sugerem que o que é especial sobre os dados neurais é que eles não são meramente informações sobre os estados neurais ou neurocognitivos. Ao contrário de outros tipos de informações, eles têm uma forte conexão ontológica com sua fonte, no sentido de que não podem ser facilmente distinguíveis ou mesmo separados dos estados mentais ou neurais. Isso é o que eles chamam de "inception problem". As informações neurais às vezes não são meramente informações sobre o cérebro, mas também informações no cérebro, ou seja, uma parte componente dos processos neurocognitivos. Os dados neurais de um determinado indivíduo constituem um tipo de informação que forma sua identidade neural, moldando aspectos únicos de sua arquitetura cognitiva, não diferente de uma impressão digital mental. É neste sentido que os dados neurais de um determinado indivíduo não são simplesmente informações sobre seu cérebro, mas parte do que constitui o cérebro deste sujeito. Se os dados neurais de um

indivíduo constituem um domínio informacional único e os domínios informacionais são parte da própria constituição cognitiva deste indivíduo, então coletar, analisar e transmitir os dados neurais deste individuo é de fato análogo a lidar com a própria arquitetura mental que o constitui como pessoa. Assim, este tipo de informação está diretamente ligado à integridade psicológica das pessoas.

Esta conexão entre privacidade mental e integridade psicológica está relacionada à ideia de que a privacidade é, essencialmente, a capacidade cognitiva de se expressar seletivamente, capacidade essa que poderia ser prejudicada pelo acesso à mente concedido pelas neurotecnologias (IENCA; ANDORNO, 2017). Essa habilidade, frequentemente associada à tomada de decisão consciente e ao planejamento, está profundamente enraizada na arquitetura cognitiva humana. Ela envolve a seleção e amplificação de sinais pré-conscientes pelo próprio mecanismo subjacente à consciência. A conexão entre privacidade mental e integridade psicológica demonstra que a primeira visa proteger um aspecto fundamental da subjetividade humana. Entretanto, a ausência de previsão legal específica em relação aos dados neurais no ordenamento jurídico brasileiro pode afetar diretamente o nível de proteção conferida a estas informações e, consequentemente, o exercício do direito à privacidade mental.

3 A PROTEÇÃO DE DADOS PESSOAIS SENSÍVEIS NO BRASIL

A presente seção dedica-se ao exame do cenário atual de proteção dos dados pessoais sensíveis no contexto do ordenamento jurídico brasileiro. Inicialmente, será abordada a dimensão do direito fundamental à proteção de dados, conforme estabelecido na CF/1988. Em seguida, a atenção se volta para a proteção específica conferida pela LGPD aos dados pessoais sensíveis, abarcando uma análise das bases legais pertinentes ao tratamento dessas categorias de dados. Dada a natureza intrinsecamente sensível das informações reveladas por dados neurais, torna-se crucial avaliar o nível de proteção que seria atribuído a esses dados, na hipótese de serem classificados como sensíveis. Esta análise envolve um escrutínio detalhado das salvaguardas presentes na LGPD e de como elas se aplicariam aos dados neurais, considerando as peculiaridades e a potencial vulnerabilidade associadas a essa forma de dados.

3.1 A PROTEÇÃO DE DADOS COMO DIREITO FUNDAMENTAL

O tratamento de dados pessoais, especialmente aqueles realizados por meio de procedimentos automatizados, representa uma atividade intrinsecamente associada a riscos significativos. Esses riscos se materializam na potencial exposição, utilização inadequada ou abusiva dos dados pessoais, bem como na possibilidade de representação incorreta do titular desses dados. A possibilidade de terceiros utilizarem esses dados sem o conhecimento do titular constitui uma preocupação legítima. Nesse contexto, torna-se imperativo estabelecer mecanismos que capacitem a pessoa a ter conhecimento e controle sobre seus próprios dados, os quais são uma expressão direta de sua personalidade (MENDES, 2011). Por essa razão, a proteção de dados pessoais é reconhecida em diversos ordenamentos jurídicos como um instrumento essencial para salvaguardar a dignidade da pessoa humana e constitui um direito fundamental.

Antes da promulgação da Emenda Constitucional nº 115, em 2022, a Constituição da República Federativa do Brasil de 1988 (CF/88) tratava a proteção da informação primariamente por meio das garantias de liberdade de expressão e direito à informação. Frequentemente, essas garantias se confrontavam com a

proteção da personalidade, especialmente no que tange ao direito à privacidade. Na ausência de uma menção explícita, inferia-se que o direito fundamental à proteção de dados pessoais era reconhecido pela consideração dos riscos associados ao tratamento automatizado em relação à proteção da personalidade. Essa interpretação se dava à luz das garantias constitucionais de igualdade substancial, liberdade e dignidade pessoal humana, bem como da proteção da intimidade e da vida privada (DONEDA, 2021).

Conforme Doneda (2021), ao se considerar a proteção de dados pessoais como uma extensão direta do direito à privacidade, em uma relação de gênero e espécie, pode-se argumentar que a tutela da privacidade se estende à proteção de dados pessoais. Esta, por sua vez, seria uma ampliação da primeira. Entretanto, essa abordagem, embora apropriada para enquadrar a disciplina no contexto constitucional, tende a simplificar excessivamente os fundamentos da tutela de dados pessoais, o que pode limitar seu alcance. Doneda (2021) também aponta que essa interpretação anteriormente adotada arriscava promover uma permissividade excessiva na utilização de informações pessoais. Como exemplo, uma decisão do Supremo Tribunal Federal (STF), relatada pelo Ministro Sepúlveda Pertence, reconheceu explicitamente a ausência de uma garantia constitucional de inviolabilidade de dados armazenados em computadores, endossando a tese de Tércio Sampaio Ferraz Júnior de que o ordenamento jurídico brasileiro protege o sigilo das comunicações, mas não necessariamente dos dados em si. Esta decisão destaca as dificuldades no tratamento da informação pessoal, frequentemente abordada de forma binária, sem considerar adequadamente sua complexidade. Este julgamento foi posteriormente citado como precedente em várias decisões do STF, onde se concluiu que a natureza fundamental da proteção de dados é restrita ao momento da transmissão.

Em maio de 2020, ocorreu uma mudança concreta na posição do Supremo Tribunal Federal (STF) sobre a proteção de dados, durante o julgamento de uma liminar nas Ações Diretas de Inconstitucionalidade (ADIs) 6387, 6388, 6389, 6390 e 6393. O STF reconheceu a proteção de dados e a autodeterminação informativa como direitos fundamentais autônomos, conferindo-lhes proteção especial tanto como um mecanismo de reforço da proteção individual quanto para limitar a intervenção estatal. O Plenário da Corte endossou a Medida Cautelar concedida

pela Ministra Rosa Weber, relatora da ADI 6387. Em consequência, o Tribunal suspendeu a eficácia da Medida Provisória 954/2020, que, em seu artigo 2º, caput, obrigava empresas de telecomunicações a compartilhar com o Instituto Brasileiro de Geografia e Estatística (IBGE) o nome, o número de telefone e o endereço de seus consumidores de telefonia móvel e fixa. A decisão da Corte resultou em uma ampliação significativa da proteção constitucional destinada aos dados pessoais, estendendo-se além da proteção de dados íntimos. Conforme destacado pela Ministra Cármen Lúcia, ‘foi-se o tempo das antigas listas telefônicas de papel’; no contexto atual de avanço tecnológico, não existem dados insignificantes ou neutros. Assim, o Tribunal superou a percepção de que o compartilhamento de dados como nome, endereço e número de telefone não seria problemático, dado o caráter público dessas informações.

Em seu voto na ADI 6387, a relatora, Ministra Rosa Weber, salientou que, quando cruzados com outras informações e compartilhados com pessoas ou entidades distintas, dados, mesmo que públicos, podem adquirir um novo valor no contexto da sociedade da informação. Eles podem ser utilizados para fins muito distintos dos inicialmente expostos na coleta e são capazes de identificar o seu titular, formando, no plano virtual, perfis a seu respeito, porém sem a sua participação. Não por acaso, ressaltou-se a centralidade do tema da proteção de dados na manutenção atual da democracia, dado que informações aparentemente insignificantes ou públicas podem ser utilizadas até mesmo para distorcer processos eleitorais. Nesse contexto, o Ministro Luiz Fux destacou que o 'recente escândalo envolvendo a Cambridge Analytica revelou como modelos de negócios são rentabilizados pela análise de dados e alertou para o risco de seu uso indevido lesar [...] a própria democracia'. Assim, o Tribunal formulou uma tutela constitucional mais ampla e abstrata do que o direito à inviolabilidade da esfera íntima e da vida privada. O conteúdo desse direito fundamental ultrapassa o protegido pelo direito à privacidade, pois não se limita apenas aos dados íntimos ou privados, mas refere-se a qualquer dado que identifique ou possa identificar um indivíduo.

Com a aprovação posterior do texto da Emenda Constitucional (EC) 115/22, foi adicionado o inciso LXXIX ao artigo 5º da Constituição Federal (CF), estabelecendo que 'é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais'. Nesse contexto, apesar das interseções e

articulações com outros direitos, a proteção de dados é reconhecida como um direito fundamental autônomo, com um âmbito de proteção próprio. Enquanto parte integrante da constituição formal, os direitos fundamentais detêm um status normativo superior em relação a todo o restante do ordenamento jurídico nacional. O direito fundamental à proteção de dados ganha particular relevância diante da existência de lacunas regulatórias, visto que a Lei Geral de Proteção de Dados (LGPD) não abrange setores como segurança nacional, segurança pública, investigação criminal e execução penal, entre outros. Por essa razão, com o reconhecimento deste direito fundamental, preenche-se uma lacuna na proteção dos dados pessoais na ordem jurídica brasileira. Conforme Mollinaro e Sarlet (2019) destacam, o reconhecimento de um direito fundamental à proteção de dados confere um novo e atual significado à proteção da pessoa humana e à dignidade, autonomia e às demais esferas de liberdade inerentes.

Para efeitos de sua proteção constitucional, é essencial compreender os dados em um sentido amplo, ressaltando a inexistência de dados pessoais irrelevantes no contexto do processamento eletrônico na sociedade da informação. Isso decorre, principalmente, do fato de que os dados, como projeções da personalidade, podem potencialmente violar direitos fundamentais em seu tratamento, independentemente de sua natureza (MENDES; DONEDA, 2018). No que tange à proteção de dados neurais, é importante notar que a Lei Geral de Proteção de Dados (LGPD) não menciona explicitamente este tipo específico de dados ao listar os tipos considerados sensíveis os quais recebem um nível mais elevado de proteção. No entanto, o reconhecimento do direito fundamental à proteção de dados pessoais pode ser interpretado como um meio de preencher essa lacuna, assegurando proteção a esses dados no nível necessário para garantir o exercício desse direito.

Embora o direito à proteção de dados esteja intrinsecamente relacionado com o princípio da dignidade da pessoa humana e com outros direitos fundamentais, especialmente o direito ao livre desenvolvimento da personalidade, o direito à privacidade e alguns direitos especiais de personalidade, como o direito à autodeterminação informativa, ele não se confunde com o objeto de proteção desses outros direitos (SARLET, 2020). Ainda assim, a compreensão do âmbito de proteção de um direito fundamental à proteção de dados pessoais envolve um constante

contraste com outros direitos, notadamente o direito à privacidade e o direito à autodeterminação informativa, que, embora também autônomos entre si, apresentam zonas de interseção. Dessa forma, torna-se necessário distinguir o direito à proteção de dados e seu alcance desses demais direitos.

Esta visão foi ecoada pela decisão histórica do Tribunal Constitucional Federal alemão em 1983, sobre a constitucionalidade de aspectos da lei do censo. O Tribunal reconheceu a existência implícita de um direito fundamental à autodeterminação informativa, baseado no princípio da dignidade da pessoa humana e no direito ao livre desenvolvimento da personalidade. Este direito consiste, em essência e conforme entendido pelo Tribunal, na prerrogativa de cada indivíduo de decidir, em princípio e substancialmente, sobre a divulgação e utilização de seus dados pessoais. Contudo, tal decisão não estabeleceu um direito de propriedade dos indivíduos sobre seus dados. Em vez disso, alertou a Corte sobre o fato de que o direito à autodeterminação informativa não confere a cada cidadão um controle absoluto sobre seus próprios dados. Isso se deve à natureza da inserção e da responsabilidade comunitária e social do ser humano, o qual deve aceitar eventuais restrições a esse direito em favor do interesse público, conforme destacado por Hornung e Schnabel (2009). Nesse contexto, conforme articulado por Menke (2020), o conceito de autodeterminação informativa não deve ser interpretado como um mecanismo que assegura ao indivíduo um controle absoluto sobre os dados pessoais, como se estes fossem propriedade exclusiva, isolando-os de todos os demais membros da sociedade.

Conforme Cachapuz (2017), é imprescindível, para assegurar uma proteção eficaz das informações pessoais dos indivíduos em uma sociedade altamente informatizada, facultar ao titular dos dados ampla capacidade de controle sobre o armazenamento e a transmissão dessas informações. Isso implica conceder a cada indivíduo a possibilidade de supervisionar as justificativas tanto para o armazenamento de dados baseado em interesse público quanto para a transmissão do conteúdo informativo a terceiros. É reconhecida, portanto, a prerrogativa do indivíduo de intervir no processo de acesso e correção de seus dados, estabelecendo-se como um princípio geral a possibilidade de interferência do titular na gestão das suas informações pessoais. Além disso, a liberdade dos cidadãos face à repressão estatal foi um ponto central na decisão da Corte Constitucional

alemã, conforme elucidado por Bull (2009). Este julgamento realçou a importância da transparência na coleta de informações como um meio para proteger a autonomia individual, reforçando a noção de que o direito à autodeterminação informativa tem uma dimensão coletiva crucial para a manutenção de uma ordem informacional livre e democrática. Nesse contexto, ele se distingue de uma concepção individualista de privacidade e de uma sobreposição completa com a proteção de dados. Conforme explica Sarlet (2020), a relação do direito à autodeterminação informativa com o princípio da dignidade da pessoa humana manifesta-se tanto pela sua vinculação com a noção de autonomia quanto com a do livre desenvolvimento da personalidade. A proteção dos dados pessoais envolve também a salvaguarda da possibilidade concreta desse desenvolvimento, para o qual a garantia de uma esfera privada e íntima é indispensável.

De forma similar, não existe uma superposição integral entre os objetos dos direitos à privacidade e à proteção de dados. Tradicionalmente, a privacidade caracteriza-se pela lógica de decisão sobre o recolhimento ou exposição de aspectos específicos da vida íntima ou privada de um indivíduo. Em contrapartida, a proteção de dados relaciona-se ao controle sobre as informações que o indivíduo decide, ou em certos casos é obrigado, a compartilhar para estabelecer relações sociais, profissionais, comerciais, ou ainda para acessar serviços públicos ou privados. Conforme Bioni (2020) aponta, proteção de dados pessoais não se limita à esfera íntima ou privada de um indivíduo, mas abarca todas as informações relativas a uma pessoa natural. Ao transcender a dicotomia entre o público e o privado, o direito à proteção de dados se distingue substancialmente do direito à privacidade. Assim, qualquer tentativa de restringir a proteção de dados pessoais a uma extensão do direito à privacidade é uma simplificação que limita o alcance e a eficácia do direito à proteção de dados. Essa compreensão é reforçada por Doneda (2021), que adverte sobre a necessidade de considerar diferentes interesses e possibilidades de controle na manipulação de dados pessoais. Assim, considerando que a informação pessoal pode ser submetida a tratamentos que sujeitem o titular a práticas discriminatórias, os dados necessitam de uma tutela que vá além da esfera do direito à privacidade.

Ademais, a elevação do direito à proteção de dados à categoria de direito fundamental autônomo, conforme discutido, distancia-o ainda mais de ser uma mera

extensão do direito à privacidade, alinhando-o mais estreitamente com a proteção da personalidade do indivíduo. A decisão do Tribunal Constitucional alemão, que declarou a inconstitucionalidade parcial da Lei do Censo em 1983, introduziu a ideia de que os dados pessoais constituem uma extensão da personalidade humana. Isso se deve ao fato de que informações aparentemente triviais, coletadas de plataformas digitais, podem revelar aspectos da personalidade de um indivíduo, tais como orientação sexual, religiosa, política, racial, entre outros dados sensíveis. Esses dados são passíveis de serem utilizados para a elaboração de perfis individuais e coletivos que, se mal utilizados, podem levar a práticas discriminatórias (BIONI, 2020). Portanto, as violações que podem ocorrer em um contexto de controle irregular e ilegal de dados pessoais estendem-se a muitas outras esferas da vida do cidadão, colocando em risco até mesmo sua autonomia e individualidade (FRAZÃO, 2019).

Nesse contexto, a análise de Mendes (2014) oferece uma perspectiva ampliada sobre o direito fundamental à proteção de dados, enfatizando que este engloba tanto um direito subjetivo de defesa do indivíduo quanto um dever de proteção por parte do Estado. A concessão de um direito subjetivo ao cidadão cria uma esfera de liberdade individual que deve ser resguardada de intervenções indevidas tanto do poder estatal quanto do privado. Esta perspectiva se torna particularmente relevante no contexto das neurotecnologias, onde as informações relacionadas à mente, como os dados neurais, são consideradas parte integrante da esfera íntima e pessoal do indivíduo. A dimensão objetiva do direito à proteção de dados evidencia a necessidade de delimitação e concretização deste direito através da proteção estatal, garantindo sua efetividade nas relações privadas. Em um cenário marcado por avanços neurotecnológicos, essa responsabilidade do Estado se traduz na necessidade de estabelecer mecanismos legais e regulatórios que assegurem a segurança, privacidade e ética no tratamento de dados neurais.

Portanto, do direito fundamental à proteção de dados surge uma obrigação clara do Estado no que tange à utilização dos dados pessoais dos indivíduos. O Estado, sob pena de violar a privacidade e o livre desenvolvimento da personalidade dos cidadãos, não pode empregar os dados pessoais de forma abusiva em operações de tratamento que possam resultar em qualquer tipo de discriminação ou constrangimento. Além disso, espera-se que o Estado se abstenha de utilizar

informações pessoais como ferramentas de poder e controle, particularmente no que se refere aos perfis de comportamento derivados da coleta de dados, ou para tomar decisões econômicas, políticas e sociais sem respeitar os princípios relacionados à proteção de dados. Este dever de abstenção do Estado não se limita aos dados em si, mas se estende aos valores e garantias fundamentais incorporados ou derivados da LGPD. Essa legislação é um verdadeiro arcabouço de direitos subjetivos, evidenciando sua importância crítica para a estabilidade da ordem constitucional brasileira. Nesse panorama, Doneda (2019) sublinha que "a proteção de dados pessoais é uma garantia de caráter instrumental, derivada da tutela da privacidade, mas não limitada por esta; abrange também um conjunto de garantias fundamentais presentes no ordenamento jurídico brasileiro".

A LGPD oferece um prisma adicional para entender a proteção de dados no Brasil, estabelecendo uma série de posições jurídicas subjetivas que se alinham com a CF/1988. A análise detalhada dos artigos 17[19] e 18[20] da LGPD, como aponta Sarlet (2020), revela que os direitos atribuídos ao titular dos dados pessoais, que

[19] Lei 13.709/2018. Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.

[20] Lei 13.709/2018. Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: I - confirmação da existência de tratamento; II - acesso aos dados; III - correção de dados incompletos, inexatos ou desatualizados; IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei; VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei. § 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional. § 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei. § 3º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento. § 4º Em caso de impossibilidade de adoção imediata da providência de que trata o § 3º deste artigo, o controlador enviará ao titular resposta em que poderá: I - comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou II - indicar as razões de fato ou de direito que impedem a adoção imediata da providência. § 5º O requerimento referido no § 3º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento. § 6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional. § 7º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador. § 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor.

são o foco da proteção legal, desempenham um papel fundamental na definição e delimitação do âmbito de proteção do direito fundamental à proteção de dados. Esses direitos, em sua natureza, possuem uma dupla função: são ao mesmo tempo um direito negativo, no sentido de defesa, e um direito positivo, no sentido de prestações.

Nesse contexto, é possível afirmar que o direito fundamental à proteção de dados, ao impor um dever de abstenção por parte do Estado, exige também do poder público uma série de ações para garantir a não violação, por parte sua e de terceiros, da intimidade, da privacidade e do livre desenvolvimento da personalidade dos indivíduos. No âmbito das neurotecnologias, o dever estatal torna-se ainda mais crucial. No tratamento de dados neurais, o Estado não deve apenas se abster de intervenções abusivas que violem a intimidade e privacidade dos indivíduos, mas também deve implementar medidas efetivas. Quanto às ações requeridas, estas envolvem a implementação de normas jurídicas organizacionais e procedimentais que 'concretizem os direitos fundamentais e assegurem que estas sejam interpretadas em conformidade com os direitos fundamentais que as fundamentam' (MENDES, 2019). Isso inclui garantir, por exemplo, que os titulares dos dados neurais tenham pleno conhecimento do tratamento a eles aplicado, possam exercer o direito de acesso e retificação desses dados, além de impor limites rigorosos à sua utilização e transferência. Assim, assegura-se que as considerações éticas e a proteção dos direitos individuais sejam efetivamente aplicadas no cenário das neurotecnologias, prevenindo potenciais riscos e abusos. A promulgação da Lei 13.709/2018, embora anterior à EC 115/22, representa uma manifestação da dimensão positiva do direito fundamental à proteção de dados, uma vez que a LGPD estabelece normas específicas que visam criar as condições materiais indispensáveis para o exercício efetivo desse direito.

Sob uma perspectiva objetiva, os direitos fundamentais, conforme delineado por Sarlet (2020), constituem decisões valorativas de natureza jurídico-objetiva emanadas da Constituição, com eficácia em todo o ordenamento jurídico. Eles fornecem diretrizes para os órgãos legislativos, judiciários e executivos, configurando-se, nesse aspecto, como um reforço à proteção dos direitos subjetivos. Essa característica faz com que as normas de direitos fundamentais adquiram uma perspectiva voltada para a promoção e proteção desses direitos em toda a

sociedade, transcendendo a mera defesa do indivíduo. Isso torna os direitos fundamentais, em sua dimensão objetiva, também direitos transindividuais, a exemplo da proteção de dados. No contexto das neurotecnologias, a compreensão dos direitos fundamentais como transindividuais ressalta a importância de assegurar a proteção dos dados neurais, não apenas para salvaguardar os interesses individuais, mas também para promover o bem-estar e os direitos da sociedade como um todo diante dos avanços tecnológicos na manipulação de informações cerebrais.

Como resultado dessa visão jurídico-objetiva, é possível reconhecer que os direitos fundamentais exercem eficácia sobre toda a ordem jurídica. Nesse contexto, Mendes (2014) enfatiza “o dever do Estado de não apenas se abster de intervir no âmbito de proteção desses direitos, mas também de protegê-los contra agressões advindas de atos de terceiros”. Os direitos fundamentais, situados no ápice da hierarquia jurídica e projetando-se por todo o ordenamento, tornam-se um marco essencial para a proteção da privacidade mental e do livre desenvolvimento da personalidade. No âmbito das neurotecnologias, onde o tratamento de dados neurais é uma realidade, esses direitos direcionam uma interpretação conforme a Constituição, exigindo que o Estado não apenas se abstenha de intervenções contrárias aos interesses do titular nesses direitos, mas também os proteja contra potenciais agressões resultantes do tratamento inadequado de dados neurais por terceiros.

Nesse cenário, considerando que o objetivo da proteção de dados pessoais é conceder ao indivíduo o controle sobre seus dados pessoais, a promulgação da Lei 13.709/2018, embora anterior à EC 115/22, pode ser interpretada como um instrumento significativo de proteção, derivado dessa perspectiva objetiva dos direitos fundamentais. Esta legislação não apenas institui medidas preventivas contra os riscos do uso indevido de dados, mas também incorpora medidas positivas destinadas a assegurar a fruição desse direito fundamental e de outros direitos a ele correlatos, como o direito à privacidade, à intimidade e à liberdade. Conforme enfatiza Frazão (2019), a LGPD adota as premissas e fundamentos necessários para que a proteção dos dados atue como um instrumento de preservação dos direitos fundamentais e valores mencionados, visando contornar, na medida do

possível, os efeitos prejudiciais de um capitalismo cada vez mais pautado na vigilância e na opacidade.

A Lei Geral de Proteção de Dados (LGPD) não explicita a proteção de dados pessoais como seu objetivo expresso no artigo 1º. Contudo, essa tutela é reconhecida, conforme tratado anteriormente, como um direito fundamental na CF/1988 (art. 5º, LXXIX), abrangendo a complexidade e a dinamicidade dos direitos à privacidade, à liberdade e ao livre desenvolvimento da personalidade da pessoa humana, conforme estabelecido no artigo 1º da LGPD. Doneda (2021), analisando a tutela ao livre desenvolvimento da personalidade da pessoa natural (art. 1º, LGPD), destaca que considerar a tutela de dados pessoais como um aspecto da dignidade da pessoa humana implica que a extensão de sua proteção deve garantir aspectos existenciais de uma pessoa no desenvolvimento de sua personalidade. Isso inclui não apenas o aspecto negativo e positivo do desenvolvimento jurídico da privacidade e da tutela de dados, mas também a garantia de tutela ao aspecto existencial, isto é, o poder de decisão sobre o ser, o comportar, o mudar (aspectos individuais) e sobre como a pessoa deseja ser representada perante a sociedade (aspecto coletivo).

O direito à proteção de dados pessoais, conforme apresentado por Doneda (2021), tem sua concretização complementada pelo regime dual de responsabilidade civil previsto na LGPD. Este regime foca tanto na adequação normativa de um tratamento de dados quanto na proteção aos direitos do titular de dados. Além disso, Doneda (2021) aponta que a prática do direito da informação deu origem à criação de uma categoria específica de dados, os dados sensíveis. Estes são tipos de informação que, se conhecidos e processados, podem levar a uma utilização discriminatória ou particularmente prejudicial e que apresentam maiores riscos potenciais para o indivíduo e, frequentemente, para uma coletividade. Exemplos desses dados incluem informações sobre raça, credo político ou religioso, orientações sexuais, histórico médico ou dados genéticos.

O debate sobre dados sensíveis é fundamental na história da proteção de dados, estando presente desde as primeiras discussões acadêmicas e iniciativas legislativas sobre o tema. A lei nacional de dados pessoais da Suécia de 1973 foi pioneira ao abordar a questão dos dados sensíveis, seguida por legislações na França, Dinamarca, Noruega e Luxemburgo entre 1978 e 1979 (DONEDA;

MENDES, 2016). A LGPD, por sua vez, aborda de forma taxativa os dados pessoais sensíveis em seu artigo 5º, II, sublinhando a importância de uma proteção específica e reforçada para essas categorias de dados, em virtude de seu potencial impacto sobre os direitos e liberdades fundamentais dos indivíduos.

A proteção de dados, como direito fundamental, estabelece uma base normativa para a elaboração de políticas e regulamentações específicas que enfrentam os desafios éticos e regulatórios do tratamento de dados neurais, assegurando a privacidade mental dos indivíduos. O direito à privacidade mental pode ser interpretado como derivado da combinação do direito à privacidade com o direito à proteção de dados. A preservação da intimidade mental e do livre desenvolvimento da personalidade está intrinsecamente vinculada à garantia de que as informações relacionadas à mente (dados neurais) sejam protegidas. Assim, o direito fundamental à proteção de dados, ao abranger informações relativas à pessoa natural, contribui significativamente para a defesa da privacidade mental, assegurando que dados neurais ou informações pertinentes ao pensamento e à mente estejam incluídos no âmbito da proteção legal. No entanto, o grau de proteção conferido aos dados neurais pode diferir daquele atribuído a outros tipos de dados pessoais. Isso se deve ao fato de que o principal instrumento legal de proteção de dados, e consequentemente de efetivação deste direito fundamental, estabelece diferentes níveis de proteção com base na sensibilidade dos dados pessoais.

3.2 A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

Até agosto de 2018, o Brasil carecia de uma legislação específica dedicada à proteção de dados pessoais. A tutela desses dados era fundamentada em disposições contidas na Constituição Federal e em diversas normas setoriais, que, de maneira direta ou indireta, abordavam questões relacionadas à privacidade e aos dados pessoais. Normas como o Código de Defesa do Consumidor (Lei nº 8.078/90), o Marco Civil da Internet (Lei nº 12.965/14), a Lei de Acesso à Informação (Lei nº 12.527/11) e a Lei do Cadastro Positivo (Lei nº 12.414/11) eram referenciadas para essa finalidade. No entanto, este conjunto de regulamentações apresentava-se como impreciso e insuficiente para oferecer garantias adequadas às

pessoas. Tal lacuna regulatória não apenas gerava insegurança jurídica e aumentava a vulnerabilidade das informações pessoais, mas também contribuía para diminuir a competitividade do Brasil em relação ao cenário internacional, especialmente no que tange à proteção de dados (MCTI, 2018).

Na esfera da economia digital, a valoração dos dados está intrinsecamente ligada à capacidade de capturar e mobilizar a atenção dos usuários em plataformas online. A premissa operacional desses ambientes digitais é maximizar o tempo de permanência dos usuários, pois um maior engajamento resulta em uma acumulação ampliada de dados e melhora a precisão dos mecanismos algorítmicos. Este incremento na coleta de dados tem como consequência direta o aumento do valor potencial das receitas geradas pelos serviços (GOLDHABER, 1997). Dessa forma, diversas estratégias de mercado têm sido implementadas com o objetivo de desenvolver mecanismos eficientes para capturar a atenção dos usuários, incentivando-os a permanecerem ativos nas plataformas e a fornecerem informações que posteriormente serão processadas e monetizadas, gerando lucro em curto, médio e longo prazo. Este fenômeno, como identificado por Franck (1999), reflete uma tendência crescente na economia digital, onde a atenção e os dados dos usuários se tornam commodities valiosas. De forma análoga, a neurotecnologia, ao lidar com dados neurais, eleva esse paradigma a um novo patamar.

Nesse contexto, Pasquale (2015) introduziu o conceito de "one way mirror" (espelho unidirecional) para descrever a dinâmica em que os dados pessoais dos cidadãos são utilizados por governos e grandes corporações. Neste modelo, esses agentes detêm um conhecimento abrangente sobre os indivíduos, enquanto estes últimos possuem pouca ou nenhuma informação sobre as entidades que coletam e utilizam seus dados. Essa assimetria de informações resulta em previsões e análises que são realizadas sobre os indivíduos, mas não necessariamente em benefício destes. Esta situação é caracterizada por um monitoramento e controle contínuos de cada aspecto da vida dos indivíduos, consolidando o que Zuboff (2019) denomina de "capitalismo de vigilância". Nesta estrutura, a experiência humana é considerada como um recurso bruto, gratuito e disponível para práticas comerciais ocultas, que incluem a extração, a predição e a venda de dados. Por meio da oferta de serviços aparentemente gratuitos a bilhões de usuários, os fornecedores desses serviços

monitoram o comportamento dos indivíduos, capturando detalhes reveladores e influenciando, e até mesmo moldando, comportamentos futuros.

As empresas de tecnologia, principais agentes do capitalismo de vigilância, perceberam que a manipulação de dados vai além do simples conhecimento sobre o comportamento humano, ou seja, elas podem também modelá-lo ativamente. Essa possibilidade de influenciar o comportamento humano através da manipulação de dados, encontra um paralelo importante no avanço das neurotecnologias e no uso de dados neurais. Segundo O'Brolcháin e Gordijn (2014), a neurotecnologia tem o potencial de decifrar não apenas as reações observáveis, mas também os estados internos, como emoções e pensamentos, dos indivíduos. Isso eleva a vigilância de um nível comportamental externo para um nível neural interno, potencialmente permitindo uma influência mais direta e refinada sobre o comportamento e as decisões humanas.

Harari (2018) destaca um cenário emergente na era digital, onde o avanço dos sensores biométricos permite que uma quantidade crescente de dados flua dos corpos e cérebros das pessoas para máquinas inteligentes. Essa realidade facilita para corporações e agências governamentais não apenas conhecer profundamente os indivíduos, mas também manipulá-los e tomar decisões em seu nome. A capacidade de decifrar os mecanismos profundos do corpo e da mente humana confere a essas entidades um poder quase divino, o que levanta uma questão crucial: a propriedade desses dados. Harari questiona se os dados relacionados ao DNA, ao cérebro e à vida de uma pessoa pertencem ao indivíduo, ao governo, a corporações ou à coletividade humana.

No Brasil, a Lei Geral de Proteção de Dados (LGPD) estabelece que cada pessoa natural tem a titularidade assegurada de seus dados pessoais, partindo do pressuposto de que todos os dados pessoais são relevantes, conforme enfatizado por Doneda (2021). A LGPD adota um conceito expansionista de dado pessoal, definindo-o como qualquer "informação relacionada a pessoa natural identificada ou identificável". Seguindo o modelo europeu, a lei brasileira oferece uma conceituação ampla e abrangente. Além disso, a LGPD institui a categoria de dados sensíveis, que requerem uma tutela específica e reforçada devido à sua natureza delicada.

No panorama atual, marcado pelo avanço das neurotecnologias e pelo uso de dados neurais, torna-se crucial compreender os dados sensíveis, suas formas de

tratamento e as medidas de proteção necessárias. Esses dados abrangem informações sobre processos cerebrais e padrões de pensamento, as quais são extremamente delicadas e reveladoras, podendo oferecer insights profundos sobre os estados emocionais e cognitivos dos indivíduos. Apesar da sua relevância e sensibilidade, é importante notar que, sob a ótica da Lei Geral de Proteção de Dados (LGPD) brasileira, tais dados neurais não são classificados expressamente como sensíveis.

Nesse contexto, as reflexões de Doneda (2021) sobre a utilização dos termos "dado" e "informação" se mostram pertinentes. Conforme Doneda explica, embora "dado" e "informação" se sobreponham em várias circunstâncias e sejam frequentemente usados de maneira intercambiável, cada termo possui suas peculiaridades. O "dado" tem uma conotação mais primitiva e fragmentada, associado a uma espécie de “pré-informação”, antes de ser transmitida e interpretada. Em contraste, a "informação" refere-se a algo além da mera representação contida no dado, chegando ao limiar da cognição. A informação implica uma depuração de conteúdo, carregando consigo um sentido instrumental na redução da incerteza.

Essa distinção entre dado e informação é especialmente relevante no contexto dos dados neurais. Embora esses dados possam ser considerados como "pré-informação" em seu estado bruto, a sua análise e interpretação podem transformá-los em informações significativas, com implicações éticas e legais substanciais. A seleção de quais informações são classificadas como dados sensíveis reflete a compreensão de que a circulação de determinadas informações pessoais pode ter um potencial lesivo significativo para seus titulares em um contexto social e político específico (QUINN; MALGIERI, 2020). Nesse sentido, é pertinente compreender quais dados são considerados sensíveis sob a LGPD, suas semelhanças em relação aos dados neurais e qual a proteção concedida a estes dados.

3.2.1 **Dados pessoais sensíveis**

O fundamento essencial para a proteção de dados sensíveis reside na prevenção de formas prejudiciais de discriminação contra os titulares desses dados.

Esse princípio foi enfatizado pela Organização das Nações Unidas (ONU) em 1990, quando emitiu Diretrizes para a Regulamentação de Arquivos de Dados Pessoais Computadorizados. Essas diretrizes destacam a importância do princípio da não discriminação, afirmando que: "dados que possam dar origem a discriminação ilegal ou arbitrária, incluindo informações sobre origem racial ou étnica, cor, vida sexual, opiniões políticas, crenças religiosas, filosóficas e outras, bem como a filiação a uma associação ou sindicato, não devem ser compilados". Embora, em muitos casos, a depender da finalidade do tratamento, não seja possível deixar de compilar e armazenar essas categorias de dados, a abordagem adotada pela ONU reflete uma compreensão ampla sobre a natureza potencialmente discriminatória desses dados e a importância de salvaguardar a privacidade e os direitos fundamentais dos titulares de dados.

O artigo 1º da Lei Geral de Proteção de Dados (LGPD) estabelece claramente o objetivo da legislação de proteger os direitos fundamentais de liberdade e privacidade, bem como o livre desenvolvimento da personalidade da pessoa natural. A citação expressa pela LGPD do livre desenvolvimento da personalidade implica o reconhecimento de que cada indivíduo deve ter a liberdade de escolher seu próprio caminho na vida. Esta concepção sustenta que cada pessoa tem o direito de desenvolver e manifestar seu projeto de vida de maneira abrangente, agindo de acordo com suas escolhas e convicções (RODOTÁ, 2008). Tal princípio assegura autonomia para que cada indivíduo construa sua personalidade de forma livre, sem imposições ou interferências externas, abrangendo tanto o direito à individualidade quanto o direito à diferença.

Essa proteção à integridade da pessoa vai além dos direitos expressamente positivados no ordenamento jurídico. Contrariamente a uma abordagem paternalista, na qual o Estado assumiria o papel de protetor dos indivíduos contra si mesmos, promove-se a autonomia individual e a liberdade de escolha sobre o próprio destino (MORAES, 2010). Essa visão enfatiza a importância de garantir que as pessoas tenham o poder de tomar decisões sobre suas vidas, incluindo a maneira como suas informações pessoais são coletadas, usadas e compartilhadas, respeitando sua individualidade e seu direito à autodeterminação.

O livre desenvolvimento da personalidade, reconhecido como um direito fundamental, exige do Estado e de terceiros a criação de atos, iniciativas e políticas

que permitam aos indivíduos desenvolverem sua personalidade plenamente (PINTO, 1999). Este direito implica a necessidade de um quadro normativo regulatório que reconheça capacidades, atribua poderes e estabeleça deveres, com o objetivo de garantir à pessoa humana um amplo espaço para o exercício de suas escolhas (MOREIRA, 2016). Neste contexto, a proteção de dados sensíveis assume uma relevância particular para a salvaguarda dos direitos e liberdades fundamentais dos titulares. Devido à natureza e ao teor das informações que contêm, os dados sensíveis estão intrinsecamente ligados à personalidade de seus titulares. O tratamento inadequado ou o vazamento desses dados pode resultar em riscos significativos para os indivíduos, potencializando preconceitos e discriminações ilícitas ou abusivas (DONEDA, 2021).

Conforme elucidado por Rodotá (2019), dados sensíveis são, tradicionalmente, aqueles relacionados à saúde, vida sexual, opiniões e pertencimento étnico ou racial, entre outros, sendo categorias semelhantes às utilizadas em normativas contra discriminações. Essa perspectiva evidencia que a proteção de dados sensíveis transcende a simples salvaguarda da vida privada, atuando como um mecanismo de promoção da igualdade entre as pessoas. Na análise da categoria de dados sensíveis, identifica-se um conteúdo intrinsecamente ligado à intimidade, identidade e proteção da igualdade material da pessoa. Estas informações, em sua essência, dizem respeito primariamente ao indivíduo a quem pertencem. No entanto, no contexto das dinâmicas de poder e expressão contemporâneas, observa-se que tais informações sensíveis frequentemente transcendem a esfera privada e passam a integrar o domínio público onde se situa seu titular. Este fenômeno reflete a natureza complexa da identidade pública de um indivíduo, composta pelas convicções e características que ele opta por manifestar publicamente (RODOTÁ, 2008). Tais elementos são componentes cruciais da identidade pública e contribuem para a forma como o indivíduo é percebido e interage no contexto social. Assim, a proteção de dados sensíveis não se limita apenas à preservação da privacidade e intimidade, mas também engloba a salvaguarda da identidade pública do indivíduo, assegurando que ele possa expressar livremente suas convicções sem o risco de discriminação ou violação de seus direitos fundamentais.

O Regulamento Geral de Proteção de Dados (GDPR), marco regulatório europeu, o qual teve uma influência significativa na formulação da Lei Geral de Proteção de Dados (LGPD) brasileira (GUIDI, 2017), confere uma proteção abrangente à categoria de dados sensíveis, a qual denomina “categorias especiais de dados pessoais”, estabelecendo diretrizes rigorosas para o seu tratamento. De acordo com o GDPR, as categorias especiais de dados incluem informações que revelam origem racial ou étnica, opiniões políticas, convicções religiosas ou filosóficas, filiação sindical, dados genéticos, dados biométricos, dados relativos à saúde ou à orientação sexual, sendo expressamente proibida a coleta desses dados, conforme estipulado no artigo 9º[21]. Contudo, o regulamento estabelece exceções a essa proibição, permitindo a coleta de dados sensíveis em contextos específicos. Tais contextos incluem medicina preventiva e ocupacional, avaliação da capacidade de trabalho de empregados, diagnóstico médico, prestação de cuidados médicos ou sociais, tratamento ou gestão de sistemas e serviços de saúde ou assistência social. Esta autorização ocorre “se os dados forem tratados por ou sob a responsabilidade de um profissional sujeito à obrigação de sigilo profissional, nos termos do direito da União ou dos Estados-Membros ou de regulamentação estabelecida pelas autoridades nacionais competentes, ou por outra pessoa igualmente sujeita a uma obrigação de confidencialidade ao abrigo do direito da União ou dos Estados-Membros ou de regulamentação estabelecida pelas autoridades nacionais competentes” (GDPR, art. 9.3).

O GDPR estabelece bases específicas para o tratamento de dados sensíveis e impõe restrições à tomada de decisões automatizadas baseadas nesses tipos de dados. Ademais, o GDPR delineia requisitos administrativos específicos para casos em que ocorra o tratamento de dados sensíveis em grande escala. Conforme estipulado no Artigo 37 (1) (c) do regulamento, o controlador de dados é obrigado a nomear um responsável pela proteção de dados. Além disso, segundo o Artigo 35 (3) (b), é exigida a realização de uma avaliação de impacto sobre a proteção de dados. Portanto, a normativa europeia não somente exige a escolha e aplicação

[21] Art. 9, GDPR: “É proibido o processamento de dados pessoais revelando origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, ou filiação sindical, e processamento de dados genéticos, dados biométricos com a finalidade de identificar unicamente uma pessoa singular, dados relativos à saúde ou dados relativos a um sexualidade ou orientação sexual de uma pessoa.”UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho.

apropriadas da base legal para o tratamento de dados sensíveis, mas também impõe deveres adicionais ao controlador de dados. Estes deveres incluem a nomeação de um responsável dedicado à proteção de dados e a realização de avaliações de impacto, visando assegurar um tratamento responsável e seguro dessas informações.

A definição de uma categoria especial de dados reflete uma preocupação quanto ao uso indevido de dados sensíveis, particularmente em áreas como bancária, financeira, seguros e saúde, onde o risco de discriminação pode ser potencializado (MULHOLLAND, 2020). O tratamento de dados sensíveis por entidades como empregadores, recrutadores, seguradoras, planos de saúde ou órgãos públicos, se realizado sem as devidas garantias, pode exacerbar cenários de violação de direitos. Esta preocupação se estende ao desenvolvimento contínuo de análises e perfis comportamentais que utilizam esses dados para direcionar e personalizar bens e serviços com alta precisão. Essa preocupação fundamenta-se na possibilidade de que os dados sensíveis, quando mal utilizados, possam contribuir para a perpetuação de desigualdades e práticas discriminatórias (RODOTÁ, 2008).

A Lei Geral de Proteção de Dados (LGPD) do Brasil define, em seu Art. 5º, inciso I, dado pessoal como “informação relacionada a pessoa natural identificada ou identificável”. Embora não defina explicitamente o que são dados pessoais sensíveis, a LGPD especifica em seu Art. 5º, inciso II[22], categorias de dados considerados como tal. Essas categorias incluem informações sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicatos ou organizações de caráter religioso, filosófico ou político. Incluem-se também na definição de dados sensíveis informações relativas à saúde ou à vida sexual, além de dados genéticos ou biométricos. Essa classificação adotada pela legislação brasileira alinha-se em grande medida com a noção europeia de dados sensíveis, como estabelecido pelo Regulamento Geral de Proteção de Dados Pessoais (GDPR).

Doneda (2010), ao discorrer sobre a categoria de dados sensíveis, ressalta que a criação desta categoria e as respectivas normativas específicas não foram

[22] Art. 5º, LGPD: “Para os fins desta Lei, considera-se: [...]II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;[...]”

isentas de críticas. Uma dessas críticas sugere que é impossível definir antecipadamente os efeitos do tratamento de uma informação, independentemente de sua natureza. Consequentemente, até mesmo dados não classificados como sensíveis podem, sob determinadas condições de tratamento, revelar aspectos da personalidade de um indivíduo e levar a práticas discriminatórias. Doneda (2010) ressalta a importância de considerar que o conceito de dados sensíveis responde à necessidade de delimitar uma área onde a probabilidade de uso discriminatório da informação é potencialmente maior. Contudo, ele também reconhece que há situações em que consequências discriminatórias podem surgir sem o uso de dados sensíveis ou que a utilização destes pode ter fins legítimos e lícitos. Cardoso (2021), porém, enfatiza que a classificação de um dado como pessoal sensível não implica necessariamente que seu uso seja discriminatório. Desta forma, a possibilidade de um dado não ser utilizado de maneira discriminatória não exclui sua potencial classificação como sensível.

Segundo Teffé (2022), a categorização dos dados sensíveis pode ser subdividida em quatro grupos principais. Primeiramente, há os dados pessoais sensíveis relacionados à origem racial ou étnica do indivíduo. Em segundo lugar, consideram-se os dados pessoais sensíveis que dizem respeito a crenças e afiliações, abrangendo informações sobre convicções religiosas, posições políticas, e a filiação a sindicatos ou organizações com orientação religiosa, filosófica ou política. A terceira categoria engloba os dados pessoais sensíveis de natureza corporal, os quais incluem informações relativas à saúde do indivíduo, dados genéticos e biométricos. Por fim, a quarta categoria mencionada por Teffé (2022) diz respeito aos dados pessoais sensíveis associados à vida sexual do sujeito.

Dados concernentes à origem racial ou étnica, crenças religiosas ou políticas, e informações relativas à vida sexual possuem uma relevância especial em virtude de uma história marcada por perseguições, discriminações e preconceitos direcionados a indivíduos pertencentes a determinados grupos raciais ou étnicos, adeptos de certas crenças, ou com uma orientação sexual específica. Paralelamente, com os avanços significativos no campo da ciência e da tecnologia, os dados corporais adquiriram uma sensibilidade crescente, refletida em suas diversas aplicações e métodos de tratamento. Atualmente, esses dados desempenham um papel crucial no alimentar de sistemas de Inteligência Artificial,

que auxiliam profissionais médicos em diagnósticos e tratamentos de saúde, contribuem para investigações criminais, e são fundamentais na implementação de tecnologias de vigilância e controle. Na era da hiperconectividade e do avanço da Internet das Coisas, os dispositivos vestíveis (wearables), incluindo neurodispositivos, estão gerando um volume cada vez maior desses tipos de informações, que são automaticamente processadas para uma variedade de propósitos (TEFFÉ; MAGRANI; STEIBEL, 2012).

Ademais, consideranado a crescente expansão do metaverso, os dispositivos vestíveis (wearables) assumirão um papel ainda mais proeminente no manejo de dados sensíveis. Esses dispositivos são fundamentais no processo de fusão dos ambientes físico e virtual, contribuindo significativamente para a experiência de realidade oferecida pelo metaverso e para a construção de uma identidade digital alternativa (FLORIDI, 2022). Como visto anteriormente, neurodispositivos apresentam-se em variadas formas e estabelecem novas interfaces entre o ser humano e a máquina ao se conectar diretamente ao corpo e a mente do usuário. Em vista da avançada tecnologia aplicada, esses aparelhos permitem a avaliação e o desenvolvimento de perfis comportamentais com base em situações específicas. Desse modo, certos tratamentos de dados originados no contexto dos neurodispositivos podem ser classificados como sensíveis, dada a natureza intrusiva e a profundidade das informações coletadas.

Considerando a conexão intrínseca entre os dados neurais e o corpo humano, torna-se pertinente uma análise aprofundada dos dados sensíveis corporais reconhecidos pelo legislador. Pela análise das informações específicas que esses dados contêm e as proteções que são efetivamente asseguradas por lei, é possível compreender a extensão da segurança legal fornecida aos dados sensíveis corporais, a qual, se aplicada extensivamente aos dados neurais, pode servir de instrumento para efetivação do direito à privacidade mental.

3.2.2 **Dados pessoais sensíveis corporais**

Dentro da esfera dos dados pessoais sensíveis relacionados ao corpo humano, são abarcadas informações que dizem respeito à integridade psicofísica do indivíduo, seu comportamento, bem como suas condições e características físicas e

mentais (TEFFÉ, 2022). Com base na tipologia estabelecida pela Lei Geral de Proteção de Dados (LGPD), são considerados dados sensíveis corporais os dados de saúde, dados biométricos e dados genéticos. Tais informações possuem a capacidade de revelar aspectos íntimos e particulares do titular, afetando, frequentemente, seus parceiros e familiares. Elas fornecem insights, de maneira direta ou indireta, sobre hábitos, comportamentos, preferências alimentares e predisposições a doenças, traçando panoramas abrangentes sobre o passado, presente e potencial futuro do sujeito. Por exemplo, um prontuário médico pode revelar soropositividade de um indivíduo, ou registros de sessões terapêuticas podem expor detalhes íntimos acerca de sua sanidade.

Como visto anteriormente, nos seus estudos sobre o “corpo eletrônico”, Rodotà (2005), ao questionar "de quem é o corpo?", indaga se o corpo pertence à pessoa diretamente interessada, aos seus familiares, a uma divindade que o teria concedido, à natureza que o deseja inviolável, a uma estrutura social que de várias maneiras o domina, a um médico ou a um magistrado que determina seu destino. Essa abordagem levanta a questão acerca das decisões relacionadas à proteção e ao manejo do corpo e dos dados que o constituem. Enfatiza-se a soberania do indivíduo sobre seu próprio corpo, opondo-se a quaisquer formas de apropriação ou controle externo, e realça-se a importância do respeito pela autonomia individual em questões relativas à corporeidade (MORAES, 2014). Contudo, é importante destacar que, conforme argumentado por Menke (2020), o direito à proteção de dados não é concebido sob a ótica de propriedade, mas sim como um arcabouço normativo que direciona o processamento da informação e as comunicações a ela relacionadas. Segundo o autor, este arcabouço estabelece critérios detalhados que determinam quais entidades, em determinados contextos e sob certas condições, estão autorizadas a manipular os dados pessoais de um indivíduo de forma específica.

No contexto atual, o princípio da liberdade individual assume uma relevância substancial para embasar e legitimar as ações das pessoas no que tange à disposição e ao tratamento de seus próprios corpos. A liberdade, neste sentido, é compreendida como a capacidade de efetuar escolhas pessoais e de expressar-se livremente, sem interferências externas (RODOTÁ, 2008). Este princípio de liberdade é a base da autonomia, a qual se define como a expressão da vontade livre e a capacidade do indivíduo de se autodeterminar, agindo em conformidade

com certos princípios éticos e jurídicos (BARROSO, 2010). A autonomia, portanto, não apenas se alinha à liberdade individual, mas também se articula com a responsabilidade de agir dentro de um quadro normativo que respeite os direitos alheios (MORAES, 2003). Em suma, a autonomia é o pilar que sustenta a capacidade do indivíduo de tomar decisões autônomas em relação ao seu corpo e à sua identidade pessoal, dentro dos limites estabelecidos pelo direito.

Ademais da liberdade individual, a integridade psicofísica do ser humano também possui importância na garantia da proteção dos direitos inerentes à personalidade. Perlingieri (2008), destaca que tanto o aspecto físico quanto o psíquico são componentes inseparáveis da constituição humana. Ele articula que a salvaguarda de um destes aspectos implica na proteção da pessoa em sua integralidade, e que as normativas que resguardam tal integridade são, por extensão, benéficas para cada uma dessas dimensões. Dessa forma, a integridade é vista como composta por duas categorias indissociáveis: o corpo e a mente. Desse modo, no âmbito jurídico, a integridade deve ser abordada sob a ótica da unidade psicofísica, reconhecendo a interdependência e a importância igualitária de ambos os aspectos para a plenitude do ser humano (MORAES, 2014).

Dentro deste contexto, os neurodispositivos e outros wearables conectados ao corpo humano desempenham um papel significativo na formatação, registro, monitoramento e análise de informações do corpo e da mente. O fenômeno da datificação consiste na conversão da experiência humana em dados digitais, que fluem através de múltiplas arquiteturas, incluindo plataformas, serviços, aplicativos, bancos de dados e dispositivos de hardware (MEJIAS; COULDRY, 2019). Esta tendência indica que cada ser humano está progressivamente desenvolvendo uma extensão e projeção digital de si mesmo, implicando que numerosos aspectos de sua vida podem ser influenciados ou determinados por essa representação eletrônica (BIONI, 2020). A consequência é a emergência de uma realidade onde a identidade e a existência física são cada vez mais complementadas e, em alguns casos, definidas por suas contrapartes digitais (RODOTÁ, 2008).

Os dados que constituem a espécie dos pessoais corporais são justamente aqueles que carregam informações sobre a existência física de um indivíduo. A LGPD ao elencar os dados pessoais sensíveis, não apenas não os classifica em espécies, mas também não traz uma definição dos três tipos que se enquadram

como corporais — dados de saúde, genéticos e biométricos — conforme a classificação proposta por Teffé (2022). No entanto, pela análise de outras fontes é possível compreender a definição desses tipos de dados sensíveis.

3.2.2.1 Dados de saúde

Conforme estabelecido pelo GDPR, dados de saúde são definidos como "dados pessoais relacionados à saúde física ou mental de uma pessoa natural, incluindo a prestação de serviços de saúde, revelando informações sobre seu estado de saúde". O Considerando nº 35 do GDPR especifica que devem ser considerados como dados pessoais relativos à saúde todos aqueles que fornecem informações sobre o estado de saúde física ou mental, passado, presente ou futuro, de um indivíduo. Isso engloba informações obtidas durante o registro ou prestação de serviços de saúde, conforme descrito na Diretiva 2011/24/UE do Parlamento Europeu. Além disso, estão inclusos nesta categoria: um número, símbolo ou sinal particular atribuído exclusivamente a uma pessoa para fins de saúde; informações provenientes de testes ou exames de uma parte do corpo ou substância corporal, incluindo dados genéticos e amostras biológicas; e quaisquer dados referentes a doenças, deficiências, risco de doença, histórico médico, tratamento clínico, ou estado fisiológico ou biomédico do titular dos dados, independentemente da fonte, seja um médico, outro profissional de saúde, hospital, dispositivo médico, ou um teste de diagnóstico *in vitro*.

Além dos tipos elencados pelo GDPR, dados de saúde podem ser compreendidos de forma ampla, englobando uma variedade de informações que vão além do mero estado de saúde física ou mental. Conforme Teffé (2022), este conceito também engloba dados pessoais que, à primeira vista, podem não parecer estar diretamente relacionados à saúde, mas que, em determinado contexto, podem fornecer inferências sobre a saúde de um indivíduo. Exemplos disso incluem informações sobre a frequência de atividades físicas, hábitos alimentares, histórico de compras em farmácias e a escolha de ser doador de órgãos.

Dados de saúde possuem a capacidade de revelar informações significativas sobre o passado, presente e futuro de um indivíduo, além de frequentemente envolverem aspectos que dizem respeito a terceiros, sendo possível analisar

doenças hereditárias por meio de determinadas informações (CÔRREA, 2006). Esta característica torna a análise desses dados particularmente sensível, persistindo essa natureza mesmo após a morte do titular. Neste contexto, Krutzinna, Taddeo e Floridi (2019) propõem uma normativa para o uso de dados de saúde post-mortem, com o consentimento prévio do titular. Eles defendem que dados médicos pessoais deveriam ser disponibilizados para pesquisa científica, incentivando e possibilitando que indivíduos doem seus registros médicos após a morte, de maneira análoga à doação de órgãos ou corpos.

O avanço científico tem potencializado um aumento substancial no número de aplicações e serviços direcionados ao setor de saúde (TOPOL, 2019). Isso inclui a utilização de inteligência artificial para diagnósticos e previsões, possibilitando por meio da coleta e análise de dados a chamada medicina de precisão (SCHULMAN; PEREIRA, 2020). A saúde, em diversos aspectos, transformou-se em um produto comercial, com táticas cada vez mais incisivas para a coleta de dados sensíveis. Um dos recursos emergentes desenvolvidos a partir do uso de dados é o conceito de "gêmeos digitais". O gêmeo digital consiste em uma representação digital, criada através de software ou outros sistemas computadorizados, de um ativo físico. O propósito principal é monitorar, visualizar, simular, prever e otimizar a tomada de decisões relacionadas a esse ativo. No campo da saúde, o gêmeo digital de um órgão ou de um paciente tem aplicação potencial na determinação de procedimentos médicos apropriados, possibilitando um tratamento mais personalizado e eficaz (RAO; MANE, 2021).

O manejo dos dados de saúde ocorre de maneira intensiva também no setor público, através de instituições responsáveis pela regulação e tratamento dessas informações. Um exemplo notável é a publicação da Resolução nº 659, em 15 de junho de 2022, pelo Conselho Nacional de Saúde. Esta resolução estabelece a Política Nacional de Informação e Informática em Saúde (PNIIS), delineando diretrizes para a gestão de dados no setor de saúde. Por sua vez, a Agência Nacional de Saúde Suplementar (ANS), como entidade reguladora, tem se dedicado a orientar o setor de saúde. Um exemplo disso é a Nota Técnica nº 3/2019, que aborda detalhadamente a proteção de dados e fornece diretrizes para a adequação da agência e da regulação da saúde suplementar à Lei Geral de Proteção de Dados (LGPD). Informações e indicadores de saúde, juntamente com orientações

científicas, são fundamentais para a formulação de políticas de saúde (SOUZA, 2008), uma vez que autoridades públicas dependem de uma estrutura de informações segura e confiável para embasar e direcionar as decisões políticas e regulatórias (ARAGÃO; SCHIOCCHET, 2020).

A expansão de bancos de dados na área da saúde evidencia a necessidade de investimentos em tecnologia e segurança da informação. Dados sensíveis em saúde têm uma vasta aplicabilidade em campos científicos, o que demanda atenção especial à sua proteção e manejo. Neste contexto, é pertinente referir-se ao artigo 13[23] da Lei Geral de Proteção de Dados (LGPD), que regulamenta o acesso de órgãos de pesquisa a bases de dados pessoais em saúde pública. Este artigo estipula que os dados devem ser tratados exclusivamente dentro do órgão, para fins de pesquisa, em ambiente controlado e seguro. Além disso, recomenda-se a adoção de práticas que incluam a anonimização ou pseudonimização dos dados e o cumprimento dos padrões éticos relacionados a estudos e pesquisas.

Conforme Martins e Soares (2020), o tratamento de dados para estudos em saúde pública deve observar restrições específicas. O princípio da finalidade exige que o tratamento dos dados se limite estritamente à finalidade do estudo. Em relação à segurança dos dados, é imperativo que o tratamento siga as práticas de segurança estipuladas por regulamentações específicas pela autoridade nacional, bem como pelas autoridades da área de saúde e sanitárias, dentro de suas competências. Além disso, a confidencialidade e o sigilo dos dados constituem princípios fundamentais da ética em saúde. Neste contexto, é relevante destacar a Lei nº 14.289, datada de 3 de janeiro de 2022, que aborda a obrigação de preservar o sigilo sobre a condição de indivíduos vivendo com infecções pelos vírus da

[23] Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas. § 1º A divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa de que trata o caput deste artigo em nenhuma hipótese poderá revelar dados pessoais. § 2º O órgão de pesquisa será o responsável pela segurança da informação prevista no caput deste artigo, não permitida, em circunstância alguma, a transferência dos dados a terceiro. § 3º O acesso aos dados de que trata este artigo será objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências. § 4º Para os efeitos deste artigo, a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

imunodeficiência humana (HIV), hepatites crônicas (HBV e HCV), hanseníase ou tuberculose. Esta legislação proíbe expressamente a divulgação, por parte de agentes públicos e privados, de informações que possibilitem a identificação de pessoas com essas condições de saúde. Ademais, o descumprimento destas disposições lei acarreta sanções ao agente infrator, conforme previsto no Art. 52[24] da LGPD, incluindo responsabilidades administrativas e a obrigação de indenizar a vítima por danos materiais e morais. As sanções estabelecidas pela lei têm um fundamento sólido, uma vez que, conforme dispõe Rodotá (2008) em relação aos dados de saúde, “a proteção especial atribuída a estes dados não se justifica somente por se referirem a fatos íntimos, mas também, e às vezes sobretudo, pelo risco que seu conhecimento possa provocar discriminações”.

3.2.2.2 Dados genéticos

Para além dos dados de saúde, a pesquisa genética tem fomentado avanços significativos na medicina. Os dados genéticos possuem relevância para o diagnóstico médico, a prevenção de doenças e os estudos de genética populacional. Devido à singularidade da herança genética de cada indivíduo, a ciência forense e o sistema judicial frequentemente recorrem a esses dados para fins de identificação. Consequentemente, observa-se um crescimento no número de bancos de dados genéticos, alguns dos quais são mantidos em âmbito nacional, como a Rede Integrada de Bancos de Perfis Genéticos (RIBPG), criada para apoiar a investigação criminal e a identificação de pessoas desaparecidas[25]. No entanto, a utilização de

[24] LGPD “Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: I - advertência, com indicação de prazo para adoção de medidas corretivas; II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; III - multa diária, observado o limite total a que se refere o inciso II; IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência; V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização; VI - eliminação dos dados pessoais a que se refere a infração; X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. [...]”

[25] A Lei nº 12.654, promulgada em 28 de maio de 2012, estabelece diretrizes rigorosas para a gestão de informações genéticas em bancos de dados de perfis genéticos. De acordo com esta legislação, é proibida a revelação de traços somáticos ou comportamentais das pessoas através desses bancos,

dados genéticos para avaliação de riscos à saúde ou para determinação de relações biológicas suscita importantes questionamentos. Estes não se limitam apenas à privacidade e à proteção dos dados de um indivíduo, mas estendem-se também a grupos sociais. Isso ocorre porque a composição genética de um indivíduo é compartilhada com outros membros de sua família, por exemplo.

Os dados genéticos armazenam características únicas que diferenciam um indivíduo dos demais, conferindo-lhe singularidade. Além disso, apresentam um aspecto probabilístico, indicando as possíveis predisposições ao desenvolvimento de enfermidades de maneira aproximada. Ademais, são geracionais, fornecendo informações sobre a herança genética do indivíduo e sua interconexão genética com seus parentes (HAMMERSCHMIDT, 2005). Contudo, os dados genéticos humanos podem levar a caracterizações sociais discriminatórias. A análise genética pode resultar na distinção de indivíduos, baseada na identificação da possibilidade de desenvolvimento de doenças genéticas, separando-os do restante da sociedade. Um exemplo plausível dessa discriminação seria o requerimento de análise genética como condição para o exercício de determinadas profissões ou para assumir certos cargos.

Em 1997, foi promulgada a Declaração Universal do Genoma Humano e dos Direitos Humanos, seguida pela Declaração Internacional sobre Dados Genéticos Humanos em 2003. Esta última destaca um status especial dos dados genéticos humanos, fundamentando-se em várias razões: (i) a capacidade de revelar predisposições genéticas de indivíduos; (ii) o potencial impacto significativo sobre a família, incluindo a descendência, que pode se estender por gerações e, em alguns casos, afetar todo o grupo ao qual o indivíduo pertence; (iii) a possibilidade de conter informações cujo significado pode não ser imediatamente aparente no momento da

---

com exceção da determinação genética de gênero. O perfil genético é gerado a partir de regiões não-codificantes do DNA, o que impede a revelação de características físicas ou de saúde, tendo como única finalidade a individualização. Os bancos de dados de perfis genéticos são mantidos sob estrita confidencialidade, com acesso restrito e controlado. O administrador desses bancos é responsável civil, penal e administrativamente por qualquer uso indevido ou não autorizado dos dados, incluindo a utilização para fins diversos dos especificados em lei ou em decisão judicial. ara assegurar a confidencialidade, são empregados dados dissociados, ou seja, informações que não são diretamente associadas a indivíduos identificáveis. (XVIII Relatório da Rede Integrada De Bancos de Perfis Genéticos (RIBPG), disponível em < https://www.gov.br/mj/pt-br/assuntos/sua-seguranca/seguranca-publica/ribpg/relatorio> Acesso em: 14 jan. 24

coleta das amostras biológicas; e (iv) o valor cultural que esses dados podem representar para pessoas ou grupos específicos.

No contexto jurídico brasileiro, ao abordar a questão da identidade genética, o Supremo Tribunal Federal (STF)[26] manifestou-se sobre a inadmissibilidade de restrições ao exercício do direito fundamental à busca da identidade genética. A Corte reconheceu que, no cerne da dignidade da pessoa humana, reside o direito fundamental à identidade pessoal do indivíduo, que engloba, entre outros aspectos, a identidade genética. Essa decisão fundamenta-se na compreensão de que a inserção e a realização do potencial de cada pessoa no mundo estão intrinsecamente ligadas à sua história pessoal, que é moldada pelos dados biológicos herdados de seus progenitores (RE 363.889 DF, 2011).

Embora a Lei Geral de Proteção de Dados (LGPD) do Brasil não forneça uma definição explícita para dados genéticos, o Decreto nº 10.046/19, em seu Artigo 2º, inciso IV, oferece uma descrição, caracterizando atributos genéticos como "características hereditárias da pessoa natural, obtidas pela análise de ácidos nucleicos ou por outras análises científicas". Essa definição, embora contribua para o entendimento da natureza dos dados genéticos, não abarca completamente todas as nuances dessa categoria de dados. Diante desta lacuna, torna-se pertinente recorrer à experiência internacional no tratamento dessa temática.

O GDPR oferece uma definição de dados genéticos. Conforme o considerando 34 do GDPR, dados genéticos são definidos como aqueles relacionados às características genéticas, sejam elas hereditárias ou adquiridas, de uma pessoa, provenientes da análise de uma amostra biológica do indivíduo. Esta análise pode incluir a avaliação de cromossomos, ácido desoxirribonucleico (ADN),

[26] STF. RE 363.889 DF, Rel. Min. Dias Toffoli, Tribunal Pleno, DJe: 16.12.2011. Trecho da ementa: "1. É dotada de repercussão geral a matéria atinente à possibilidade da repropositura de ação de investigação de paternidade, quando anterior demanda idêntica, entre as mesmas partes, foi julgada improcedente, por falta de provas, em razão da parte interessada não dispor de condições econômicas para realizar o exame de DNA e o Estado não ter custeado a produção dessa prova. 2. Deve ser relativizada a coisa julgada estabelecida em ações de investigação de paternidade em que não foi possível determinar-se a efetiva existência de vínculo genético a unir as partes, em decorrência da não realização do exame de DNA, meio de prova que pode fornecer segurança quase absoluta quanto à existência de tal vínculo. 3. Não devem ser impostos óbices de natureza processual ao exercício do direito fundamental à busca da identidade genética, como natural emanação do direito de personalidade de um ser, de forma a tornar-se igualmente efetivo o direito à igualdade entre os filhos, inclusive de qualificações, bem assim o princípio da paternidade responsável. 4. Hipótese em que não há disputa de paternidade de cunho biológico, em confronto com outra, de cunho afetivo. Busca-se o reconhecimento de paternidade com relação a pessoa identificada. (...)"

ácido ribonucleico (ARN) ou de outros elementos capazes de fornecer informações equivalentes. Adicionalmente, o Artigo 4º, item 13, do GDPR, especifica que os dados genéticos são dados pessoais associados às características genéticas, hereditárias ou adquiridas, de uma pessoa singular. Esses dados fornecem informações únicas sobre a fisiologia ou a saúde do indivíduo e são tipicamente derivados da análise de uma amostra biológica da pessoa em questão.

A medicina personalizada, empregando testes genéticos, visa oferecer um tratamento singular e adaptado às características biológicas individuais. Embora tais estudos genéticos proporcionem diagnósticos mais precisos e viabilizem práticas de medicina preventiva, o manejo inadequado do armazenamento e compartilhamento de dados genéticos pode levar a consequências preocupantes. Uma dessas implicações é a potencial categorização de riscos baseada no perfil genético do indivíduo, que pode resultar na “genetização da vida”, um fenômeno onde as informações genéticas passam a dominar a percepção e o tratamento da saúde individual (COLUSSI; SANTOS, 2018).

No contexto da proteção contra discriminações baseadas em informações genéticas, destaca-se a Lei de Não Discriminação de Informações Genéticas (GINA) dos Estados Unidos, promulgada em 2008. Esta legislação salvaguarda os cidadãos norte-americanos de práticas discriminatórias que utilizem informações genéticas, tanto no âmbito dos seguros de saúde quanto nas relações de trabalho. De acordo com a GINA, é proibida a discriminação em qualquer aspecto do emprego — incluindo contratação, demissão, remuneração, designação de tarefas, promoções, dispensas, treinamento, benefícios adicionais ou quaisquer outros termos ou condições de emprego — com base em informações genéticas (EUA, 2008). Em contraste, embora a LGPD do Brasil estabeleça o princípio da não discriminação no tratamento de dados (Art. 6º, inciso IX), observa-se que a lei não apresenta disposições específicas voltadas para a proteção de dados genéticos.

3.2.2.3 Dados biométricos

No contexto da Lei Geral de Proteção de Dados (LGPD), os dados biométricos constituem outro tipo de dado corporal reconhecida como sensível. A biometria é definida como a ciência de estabelecer a identidade de um indivíduo por

meio da medição e análise de atributos fisiológicos ou comportamentais mensuráveis (TEFFÉ, 2022). Na categoria dos atributos fisiológicos, encontram-se exemplos como impressões digitais, reconhecimento de íris, identificação por retina, características faciais, arcada dentária, geometria da mão e estatura. Por outro lado, os atributos comportamentais incluem aspectos como a maneira de digitar, andar, gestos característicos, dinâmica da assinatura, posição habitual ao segurar um celular, movimentos ao usar um mouse de computador, pressão exercida sobre teclados ou telas, e padrões de correção de texto.

Embora a Lei Geral de Proteção de Dados (LGPD) não especifique uma definição para dados biométricos, o Decreto nº 10.046/19, em seu Artigo 2º, inciso II, proporciona uma descrição. Conforme o decreto, atributos biométricos são definidos como “características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado.” O GDPR, em seu Artigo 4º, item 14, oferece uma definição de dados biométricos. Segundo este regulamento, são considerados dados biométricos aqueles "dados pessoais resultantes de um tratamento técnico específico relacionados às características físicas, fisiológicas ou comportamentais de uma pessoa singular, que permitem ou confirmam a identificação única dessa pessoa singular." Exemplos explicitamente mencionados incluem imagens faciais e dados dactiloscópicos (impressões digitais).

Dados biométricos são reconhecidos por oferecerem métodos eficientes e confiáveis para a identificação e autenticação de indivíduos. Esses dados se caracterizam por serem reconhecíveis e verificáveis, possuindo atributos únicos e específicos aos seus titulares. Neste contexto, o corpo humano assume a função de uma "senha", atuando como um meio singular e exclusivo de individualização da pessoa. Diferentemente de outros tipos de dados sensíveis, que frequentemente estão relacionados à expressão pública do indivíduo, os dados biométricos, assim como os dados genéticos, geralmente não são derivados de escolhas pessoais, estando intrinsecamente ligados à sua identidade física (DOERING; SILVA, 2020).

Informações biométricas, tradicionalmente utilizadas para fins de identificação e autenticação, têm encontrado aplicação em diversos contextos, levantando questões significativas sobre privacidade e consentimento. Um exemplo notável ocorreu em 2018 no Brasil, quando o Instituto Brasileiro de Defesa do Consumidor (Idec) e outras entidades ajuizaram uma Ação Civil Pública contra a ViaQuatro,

operadora da Linha Amarela do metrô de São Paulo, por coleta indevida de dados pessoais. O caso envolveu o projeto “Portas Digitais” da ViaQuatro, que utilizava câmeras para filmar as reações dos passageiros à publicidade exibida, analisando emoções sem o consentimento prévio dos usuários, com o intuito de otimizar a venda de anúncios. As “portas interativas” instaladas em algumas estações buscavam identificar características como gênero, faixa etária e emoções dos passageiros expostos à publicidade. Os autores da ação civil argumentaram que tal prática representava uma violação do direito à imagem dos consumidores e usuários do transporte público, além de desrespeitar a proteção especial conferida aos dados pessoais sensíveis. Eles pleitearam que a ViaQuatro fosse proibida de utilizar dados biométricos ou qualquer outro tipo de identificação sem o consentimento explícito dos usuários, e requereram indenização por danos coletivos no valor mínimo de R$ 100.000.000,00 (IDEC, 2018).

Em 07 de maio de 2021, foi proferida uma sentença de mérito sobre o caso, na qual se reconheceu que a conduta da Via Quatro violava claramente o direito à imagem dos consumidores, as normas relativas à proteção de dados pessoais sensíveis e os direitos básicos do consumidor, especialmente no que diz respeito à informação e à proteção contra práticas comerciais abusivas. O juízo acatou o pedido para que a ré se abstivesse de utilizar dados biométricos ou qualquer outra forma de identificação dos usuários do transporte público sem a devida comprovação de consentimento. A decisão judicial enfatizou que, caso a ViaQuatro desejasse retomar tais práticas, seria necessário obter consentimento prévio dos usuários, fornecendo informações claras e específicas sobre a captação e o tratamento dos dados, além de adotar as ferramentas apropriadas para tal fim (SÃO PAULO, 2021).

Dados biométricos são reconhecidos por sua capacidade de identificar indivíduos de maneira precisa e direta, sem a necessidade de múltiplos cruzamentos de informações. Nesse contexto, a Portaria nº 248, de 2 de fevereiro de 2018, do Ministério da Saúde do Brasil, estabelece uma diretriz relevante. De acordo com esta portaria, as Declarações de Nascidos Vivos (DNV) devem ser vinculadas ao registro biométrico tanto do recém-nascido quanto de sua mãe, conforme determinação conjunta das Secretarias de Vigilância em Saúde e de Atenção à Saúde. A prática de coletar e registrar dados biométricos desde o nascimento

possibilita o rastreamento, monitoramento e análise profunda dos indivíduos por setores tanto públicos quanto privados. A utilização desses dados ultrapassa a mera unificação de documentos, abrindo caminho para a implementação de sistemas sofisticados de vigilância e controle sobre a população.

Ainda no campo da biometria, tecnologias de reconhecimento de emoções faciais são empregadas para analisar sentimentos de pessoas naturais utilizando diferentes fontes, como fotos e vídeos (VEMOU; HORVATH, 2021). As expressões faciais, que constituem uma forma de comunicação não verbal, oferecem recursos para a análise das emoções humanas. A decodificação de expressões emocionais tem sido um campo de interesse no estudo da psicologia (ALMADA, 2012). A disseminação generalizada de câmeras, os avanços tecnológicos no tratamento de dados biométricos e o aumento no uso de inteligência artificial e aprendizado de máquina têm contribuído significativamente para o aprimoramento dessa tecnologia (KAVOLIŪNAITĖ-RAGAUSKIENĖ, 2024).

Ademais, a criação de bancos de dados biométricos para a identificação de cidadãos, especialmente para fins de validação de identidades e concessão de benefícios governamentais. Um marco importante nesse contexto é a Lei n° 13.444/2017, que instituiu a Identificação Civil Nacional (ICN). O propósito da ICN é cadastrar os cidadãos de forma a permitir uma identificação segura, tanto em transações com órgãos públicos quanto privados. A base de dados da ICN incluirá uma variedade de informações, destacando-se a integração com a base de dados biométricos da Justiça Eleitoral. Espera-se que, mediante a validação de dados biométricos na base da ICN, os cidadãos possam acessar serviços anteriormente disponíveis apenas presencialmente em órgãos federais, como o INSS e a Receita Federal (TSE, 2021).

Contudo, no contexto de uma possível violação ou incidente de segurança envolvendo dados biométricos, as consequências podem ser particularmente graves. Diferentemente de senhas numéricas ou outros identificadores substituíveis, as características físicas utilizadas na biometria, como impressões digitais, não podem ser alteradas ou substituídas. A natureza permanente dos dados sensíveis corporais eleva o risco associado à sua exposição indevida, tornando essencial um regime de segurança rigoroso e específico. Esta realidade sublinha a importância de uma proteção ampliada e a adoção de medidas de segurança mais robustas no

tratamento dos dados pessoais sensíveis em comparação aos demais dados pessoais.

3.2.3 **Bases legais para o tratamento de dados pessoais**

No âmbito do tratamento de dados pessoais, conforme estipulado pela Lei Geral de Proteção de Dados (LGPD), é imperativo que qualquer agente, seja ele pessoa natural ou jurídica, de direito público ou privado, inclusive nas atividades realizadas em meios digitais, fundamente suas ações em uma base legal sólida. Tal base legal refere-se às disposições estabelecidas nos artigos 7º ou 11 da LGPD, podendo ser complementada, conforme a especificidade do caso, pelas normas contidas nos artigos 14 ou 23 da mesma lei. Conforme Teffé e Viola (2022), as bases legais para o tratamento de dados são definidas de maneira abrangente e diversificada, cabendo detalhamentos e regulamentações por parte da Autoridade Nacional de Proteção de Dados, do Poder Legislativo, do Judiciário e da doutrina jurídica.

A seleção de uma base legal adequada e segura para o tratamento de dados é um aspecto crucial, especialmente quando considerado que mais de uma base legal pode ser aplicável a uma determinada operação de tratamento. Esta possibilidade de identificar múltiplas bases legais para o tratamento de dados tem encontrado suporte em algumas autoridades de proteção de dados e na doutrina. O Information Commissioner's Office (ICO) do Reino Unido (2023), interpretando a aplicação do Regulamento Geral sobre a Proteção de Dados (GDPR), manifestou: “Você pode considerar que mais de uma base se aplica, caso em que você deve identificar e documentar todas elas desde o início” (tradução nossa). Ao analisar a LGPD, Menke (2021) considera ser razoável a interpretação do caput do artigo 7º, no sentido de que é permitido o enquadramento da operação de tratamento de dados pessoais em mais de uma base legal.

A LGPD, em seu Artigo 5º, inciso X, define o conceito de tratamento de dados de maneira abrangente, incluindo uma vasta gama de operações realizadas com dados pessoais. Isso engloba atividades como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, entre outras. Essencialmente, qualquer ação que envolva dados pessoais deve estar

fundamentada em uma base legal apropriada. Teffé (2022) esclarece que as bases legais para o tratamento de dados, tanto pessoais comuns (Artigo 7º) quanto sensíveis (Artigo 11), são exaustivas na LGPD, podendo ser complementadas, quando necessário, pelos Artigos 14 e 23, que abordam, respectivamente, o tratamento de dados de crianças e adolescentes e o tratamento de dados pelo poder público.

Paralelamente, o GDPR segue uma sistemática similar no que tange à aplicação de bases legais para o tratamento de dados pessoais. O princípio do processamento lícito, estabelecido no Artigo 5, requer que toda operação de tratamento de dados pessoais possua uma base legal claramente definida, conforme especificado no Artigo 6(1). Este artigo elenca as condições sob as quais o tratamento de dados é considerado lícito. De acordo com Kotschy (2018), a lista de fundamentos legais para o tratamento de dados contida no Artigo 6(1) é exaustiva e definitiva, não sendo passível de suplementação ou alteração por meio de interpretação. Isso implica que o processamento de dados pessoais deve atender a um dos fundamentos legais especificados, além de cumprir com os demais princípios centrais estabelecidos pelo Artigo 5(1).

Existe um consenso jurídico de que as bases legais para o tratamento de dados pessoais, conforme estabelecidas no Artigo 7º, são consideradas de igual peso e relevância. Este entendimento é reforçado pelo enunciado n. 689, aprovado na IX Jornada de Direito Civil do Conselho da Justiça Federal (CJF) em maio de 2022.[27] Por outro lado, no que concerne ao Artigo 11 da LGPD, que trata especificamente do tratamento de dados pessoais sensíveis, existe uma posição minoritária na doutrina, conforme apontado por Teffé (2022), que sugere uma precedência do consentimento em relação às demais bases legais.

A tabela a seguir compara as bases legais para o tratamento de dados pessoais comuns e dados pessoais sensíveis, conforme estabelecido nos Artigos 7º e 11 da Lei Geral de Proteção de Dados (LGPD):

Tabela 1 — Comparativo das bases legais elencadas pelos Artigos 7º e 11 da LGPD

Art. 7º - Dados Pessoais	Art. 11 - Dados Pessoais Sensíveis

[27] Enunciado 689 – “Não há hierarquia entre as bases legais estabelecidas nos arts. 7º e 11 da Lei Geral de Proteção de Dados (Lei n. 13.709/2018)”

Art. 7º - Dados Pessoais	Art. 11 - Dados Pessoais Sensíveis
Consentimento do titular	Consentimento específico e destacado para finalidades específicas
Cumprimento de obrigação legal ou regulatória pelo controlador	Cumprimento de obrigação legal ou regulatória pelo controlador
Execução de políticas públicas pela administração pública	Tratamento compartilhado de dados pela administração pública para execução de políticas públicas
Realização de estudos por órgão de pesquisa	Realização de estudos por órgão de pesquisa (garantindo anonimização dos dados, sempre que possível)
Execução de contrato ou de procedimentos preliminares relacionados a contrato	Exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral
Exercício regular de direitos em processo judicial, administrativo ou arbitral	Proteção da vida ou da incolumidade física do titular ou de terceiro
Proteção da vida ou da incolumidade física do titular ou de terceiro	Tutela da saúde (em procedimento por profissionais da área da saúde)
Tutela da saúde (em procedimento por profissionais da área da saúde)	Garantia da prevenção à fraude e à segurança do titular nos processos de identificação e autenticação de cadastro em sistemas eletrônicos
Legítimo interesse do controlador ou de terceiros	
Proteção ao crédito	

Fonte: LGPD (BRASIL, 2018)..

Uma análise comparativa das bases legais para o tratamento de dados (Tabela 1), conforme apresentada nos Artigos 7º e 11 da LGPD, revela que o Artigo 11 preserva diversas bases já estabelecidas no Artigo 7º para o tratamento de dados pessoais. No entanto, observa-se que o Artigo 11 exclui expressamente do tratamento de dados sensíveis as situações relacionadas aos interesses legítimos do controlador ou de terceiros (Art. 7º, IX) e à proteção do crédito (Art. 7º, X).

Neste último ponto, conforme estabelecido na Lei do Cadastro Positivo (Lei nº 12.414/11), os bancos de dados podem conter informações relativas ao

adimplemento do cadastrado, visando a formação de um histórico de crédito, dentro das condições previstas na referida legislação. Contudo, é expressamente proibido o registro de informações sensíveis ou excessivas nesses bancos de dados (Art. 3º, §3º). Para a composição do cadastro, devem ser armazenadas apenas informações objetivas, claras, verdadeiras e de fácil entendimento, necessárias para a avaliação da situação econômica do cadastrado (Art. 3º, I a V).

Ainda neste contexto, no Recurso Especial 1.419.697, foi determinado que a avaliação do risco de crédito deve respeitar os limites impostos pelo sistema de proteção ao consumidor, notadamente no que concerne à tutela da privacidade e à transparência nas relações negociais, conforme disposto no Código de Defesa do Consumidor e na Lei 12.414/11. Em relação ao sistema de pontuação de crédito (*scoring*), foi afirmado que, embora não seja necessário o consentimento do consumidor para a consulta, devem ser fornecidos esclarecimentos, se solicitados, sobre as fontes dos dados considerados (histórico de crédito) e as informações pessoais valoradas, entendimento que motivou a Súmula 550[28] do Superior Tribunal de Justiça (STJ). Adicionalmente, a Corte destacou que o fornecedor do serviço de *credit scoring* não deve utilizar informações sensíveis, e é considerado abuso de direito o uso de informações sensíveis, excessivas, incorretas ou desatualizadas.

Mendes e Doneda (2018) argumentam que o Artigo 23 da LGPD introduz uma base legal adicional para o tratamento de dados pessoais, especificamente direcionada à execução de competências legais ou ao cumprimento das atribuições legais do serviço público. Contudo, é plausível interpretar que o tratamento de dados pessoais para essas finalidades já esteja em grande parte abarcado pelas disposições relativas ao cumprimento de uma obrigação legal (Art. 7º, II, e Art. 11, II, ‘a’), uma vez que a atuação da Administração Pública normalmente decorre de um mandato legal, bem como pelo tratamento e uso compartilhado de dados necessários à execução de políticas públicas (Art. 7º, III, e Art. 11, II, ‘b’).

Neste sentido, a inclusão do Artigo 23 na LGPD pode ser vista como estabelecendo requisitos adicionais e específicos para o tratamento de dados pessoais realizado pelo poder público, mais do que introduzir uma nova base legal

[28] A utilização de escore de crédito, método estatístico de avaliação de risco que não constitui banco de dados, dispensa o consentimento do consumidor, que terá o direito de solicitar esclarecimentos sobre as informações pessoais valoradas e as fontes dos dados considerados no respectivo cálculo. (SÚMULA 550, STJ, SEGUNDA SEÇÃO, julgado em 14/10/2015, DJe 19/10/2015)

autônoma. Esta interpretação é corroborada por orientações da Autoridade Nacional de Proteção de Dados (ANPD), que enfatiza que

"O tratamento de dados pessoais pelo Poder Público deve se amparar em uma das hipóteses previstas no art. 7º ou, no caso de dados sensíveis, no art. 11 da LGPD. Esses dispositivos devem ser interpretados em conjunto e de forma sistemática com os critérios adicionais previstos no art. 23, que complementam e auxiliam a interpretação e a aplicação prática das bases legais no âmbito do Poder Público" (ANPD, 2022).

Considerando a aplicação da Lei Geral de Proteção de Dados (LGPD) ao tratamento de dados pessoais[29], é imprescindível que o agente responsável pelo tratamento indique, de maneira preliminar, uma base legal pertinente para as ações praticadas. Conforme Teffé (2022), quando se trata de operações de processamento que envolvem uma mescla de dados pessoais sensíveis e não sensíveis, deve-se adotar um critério de rigor mais elevado. Nesse sentido, o tratamento desses dados deve estar em conformidade com as exigências de uma base legal mais estrita, conforme estipulado no Artigo 11 da LGPD. Em tais circunstâncias, a proteção conferida aos dados pessoais sensíveis deve prevalecer, orientando as práticas de tratamento de dados e estabelecendo um padrão de segurança e privacidade mais rigoroso.

Segue-se, então, uma análise das bases legais aplicáveis ao tratamento de dados pessoais sensíveis.

3.2.3.1 Consentimento do titular ou do responsável legal

[29] Conforme estabelecido no Artigo 4º da Lei Geral de Proteção de Dados (LGPD), existem circunstâncias específicas nas quais as disposições da lei não se aplicam ao tratamento de dados pessoais, incluindo os dados sensíveis. Essas exceções incluem: a) Tratamento de dados realizado por pessoa natural para fins exclusivamente particulares e não econômicos, caracterizando uma esfera privada de atuação desvinculada de atividades comerciais ou profissionais. b) Tratamento de dados para fins exclusivamente jornalísticos ou artísticos, respeitando a liberdade de expressão e criação artística, desde que observados os princípios da LGPD. c) Tratamento de dados realizado para fins exclusivamente acadêmicos, aplicando-se, nesse caso, as disposições dos Artigos 7º e 11 da LGPD. Esta exceção reconhece a importância da pesquisa acadêmica, ao mesmo tempo que impõe limites e condições para o tratamento de dados nesse contexto. d) Tratamento de dados realizado exclusivamente para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, ressaltando a relevância dessas atividades para o interesse público e a segurança nacional. e) Dados provenientes de fora do território nacional que não sejam objeto de comunicação, uso compartilhado com agentes de tratamento brasileiros ou de transferência internacional de dados para países que não ofereçam um grau de proteção de dados pessoais adequado, conforme previsto pela LGPD.

O Artigo 11 da LGPD estabelece como primeira condição autorizativa para o tratamento de dados sensíveis o consentimento do titular ou de seu responsável legal. Este consentimento deve ser manifestado de forma específica[30] e destacada[31], direcionado a finalidades claramente delimitadas. Conforme Bioni (2019), a base legal do consentimento para o tratamento de dados sensíveis deve ser compreendida "como um vetor para que haja mais assertividade do titular em relação a esses movimentos 'específicos' de seus dados". Essa concepção de consentimento aproxima-se da ideia de consentimento expresso, exigindo uma participação mais ativa do titular dos dados (TEPEDINO; TEFFÉ 2020).

Ademais, a LGPD estipula que o consentimento para o tratamento de dados pessoais deve ser informado, particularmente nos casos em que tal tratamento seja uma condição para o fornecimento de um produto, serviço ou exercício de um direito. Essa disposição visa garantir que o titular dos dados seja claramente informado sobre esta contingência e sobre os meios de exercer os direitos previstos no Artigo 18 da Lei. Tal regulamentação busca mitigar a prática das políticas de "tudo ou nada", comumente empregadas em serviços digitais, onde a aceitação integral dos termos é a única opção disponível para o usuário. Este cenário é corroborado por práticas como a implementação de "muros de rastreamento" em alguns sites, onde o acesso só é concedido mediante o consentimento ao rastreamento por terceiros. Nestas circunstâncias, muitos usuários podem sentir-se compelidos a concordar com qualquer solicitação, levantando questões sobre a efetividade do controle das pessoas sobre suas informações pessoais em situações onde o consentimento é pré-requisito para acessar serviços ou websites (BORGESIUS; KRUIKEMEIER; BOERMAN; HELBERGER, 2017).

Nesse sentido, Rodotá (2008) discorre sobre a existência de condicionantes em determinados contextos que efetivamente restringem a liberdade de escolha dos

[30] O conceito de "consentimento específico" refere-se à autorização do titular dos dados para finalidades de tratamento claramente definidas e delimitadas pelo controlador, com antecedência ao processamento dos dados. Esse consentimento destaca-se pela granularidade, permitindo ao titular escolhas detalhadas e personalizadas quanto ao uso de seus dados, possibilitando a aceitação de certos tratamentos e a recusa de outros não considerados adequados.

[31] O conceito de "consentimento destacado" implica que o titular dos dados deve ter acesso claro e completo às informações relevantes sobre o tratamento de seus dados pessoais, com as disposições pertinentes apresentadas de forma destacada no documento de consentimento. Este princípio enfatiza a necessidade de uma declaração de vontade clara e específica, vinculada a um objetivo definido, e ressalta que tal manifestação de consentimento deve ser proeminente e facilmente identificável no documento que autoriza o tratamento dos dados.

indivíduos. Segundo o jurista, esse condicionamento surge da premissa de que o acesso a certos serviços, sejam eles essenciais, importantes ou percebidos como tal, depende não apenas do fornecimento de informações específicas pelo usuário, mas também da possibilidade de que essas informações, uma vez coletadas (potencialmente sob o consentimento do titular), possam ser submetidas a tratamentos subsequentes e mais complexos. Peña e Varon (2019) observam que apenas um número limitado de indivíduos possui a habilidade ou a oportunidade real de negociar ou recusar as condições estipuladas nos termos de serviço e políticas de privacidade de plataformas digitais. Nesse contexto, a concordância com o uso dos dados pessoais frequentemente não reflete um genuíno acordo do titular dos dados, mas sim uma submissão à vontade das empresas.

Mulholland (2020) salienta que a exigência de um consentimento qualificado para o tratamento de dados sensíveis é motivada pela natureza existencial e intrínseca dos conteúdos abordados por esses dados. Para melhor desenvolver esse conceito, a autora recorre ao biodireito, que oferece uma perspectiva para delinear o que constitui um consentimento específico e destacado para finalidades bem definidas. Essa associação é pertinente, pois o biodireito, ao tratar de interesses de natureza existencial, requer uma abordagem jurídica especialmente cuidadosa, com o objetivo de assegurar a autonomia plena do indivíduo. No contexto do tratamento de dados sensíveis, essa necessidade de proteção específica é ainda mais acentuada, considerando-se que o titular desses dados é frequentemente visto como uma parte vulnerável, cujos direitos e liberdades fundamentais podem estar em risco (MARCULINO, 2021).

Nesse contexto, o Information Commissioner’s Office (ICO) (2020) fornece um exemplo sobre a validade do consentimento no contexto do tratamento de dados pessoais. No exemplo, uma academia implementa um sistema de reconhecimento facial para controlar o acesso às suas instalações, exigindo que todos os membros concordem com essa forma de identificação como condição para entrada. Neste cenário, o consentimento não é considerado válido ou livre, uma vez que os membros não possuem uma escolha real – caso não aceitem o reconhecimento facial, são impedidos de acessar a academia. Ainda que o reconhecimento facial possa apresentar vantagens em termos de segurança e conveniência, ele não é estritamente necessário para o acesso às instalações de uma academia de

ginástica. No entanto, o ICO (2020) salienta que, se a academia oferecer aos membros uma alternativa de acesso, como a utilização de um cartão de membro ou senha, ao invés do reconhecimento facial, o consentimento poderá ser considerado livre e válido.

A questão do consentimento e de sua exigência contínua nas interações digitais e as potenciais manipulações da vontade real do usuário, representa um tópico de significativa relevância. Neste contexto, o European Data Protection Board (EDPB) observa uma problemática específica relacionada ao consentimento no ambiente digital. O EDPB (2020) aponta que, no ambiente digital, muitos serviços dependem de dados pessoais para funcionar, o que leva os titulares de dados a receberem frequentes solicitações de consentimento, muitas vezes requerendo apenas um clique ou um deslize de dedo para resposta. Essa dinâmica recorrente pode gerar um fenômeno conhecido como "fadiga do consentimento", no qual a constante repetição dessas solicitações acaba por reduzir a eficácia dos mecanismos de consentimento como um alerta para o usuário (CHOI; PARK, JUNG, 2021). Este cenário apresenta um risco particular aos titulares dos dados, visto que, tipicamente, o consentimento é requerido para ações que, segundo o GDPR, seriam ilícitas na ausência de tal consentimento.

Segundo Teffé (2022), o consentimento deve ser entendido como um processo multifacetado, envolvendo ambas as partes da relação e segmentado em várias etapas, em conformidade com as qualificações estipuladas pela lei, tais como ser informado, livre, inequívoco e específico e destacado (em casos de dados sensíveis). Este entendimento enfatiza a função crucial dos agentes de tratamento de dados, responsáveis por assegurar que cada fase do processo de consentimento esteja alinhada com os requisitos legais, visando obter uma aceitação válida no final. O design é visto como uma ferramenta essencial para garantir a obtenção do consentimento destacado e, portanto, a conformidade desse procedimento com a legislação.

Por outro lado, Chatelier (2019) adverte que, embora o design possa ser empregado para reforçar os direitos dos titulares dos dados, ele também pode ser utilizado de forma enganosa, através de práticas como as interfaces maliciosas, conhecidas como "dark patterns" (padrões obscuros). Esta perspectiva sugere que o design e o consentimento estão intrinsecamente relacionados, podendo influenciar

positivamente, ao aprimorar a capacidade das pessoas de tomarem decisões informadas e conscientes, ou negativamente, ao induzi-las a escolhas desfavoráveis por meio de estratégias de design abusivas ou manipulativas.

Outro exemplo relevante sobre a importância do consentimento como base legal é a coleta e análise de dados neurais em pesquisas científicas sobre doenças neurodegenerativas (JWA; POLDRACK, 2022). Neste cenário, os participantes da pesquisa são solicitados a fornecer consentimento específico e explícito para a coleta e análise de seus dados neurais, como padrões de atividade cerebral, com o objetivo claramente definido de avançar no entendimento e tratamento de condições como Alzheimer ou Parkinson. Este consentimento é informado e destacado, assegurando que os participantes estejam plenamente cientes da natureza, finalidade e implicações da coleta de seus dados neurais sensíveis.

3.2.3.2 Cumprimento de obrigação legal ou regulatória pelo controlador

O tratamento de dados sensíveis sem consentimento é considerado lícito quando necessário para o cumprimento de obrigações legais ou regulatórias impostas ao controlador. Esse contexto inclui, por exemplo, obrigações trabalhistas e deveres decorrentes da legislação anticorrupção. Situações ilustrativas dessa prerrogativa legal são a obrigatoriedade de exames médicos conforme o artigo 168 da Consolidação das Leis do Trabalho (CLT); e a coleta de dados relativos à filiação sindical para fins de desconto da contribuição sindical, conforme os artigos 545, 578 e 579 da CLT.

Adicionalmente, essa base legal abrange obrigações oriundas de Códigos de Ética profissionais, portarias do Ministério da Justiça, e resoluções de entidades reguladoras, como conselhos profissionais ou especializados. Exemplos relevantes incluem a Resolução nº 466/2012 do Conselho Nacional de Saúde (CNS), que regula pesquisas e testes em seres humanos, e a Resolução da Diretoria Colegiada (RDC) nº 9 de 20 de fevereiro de 2015, da Agência Nacional de Vigilância Sanitária (ANVISA), que estabelece regulamentos para a realização de ensaios clínicos com medicamentos no Brasil.

Os setores de seguros, saúde e mercado financeiro encontram-se sujeitos a uma variedade de normas legais e regulatórias que, em certas circunstâncias,

exigem o tratamento de dados pessoais, incluindo dados sensíveis, de seus clientes. No contexto da saúde, por exemplo, as pessoas jurídicas de direito privado que administram planos de assistência à saúde estão subordinadas à Lei nº 9.656/98 e à regulamentação estabelecida pela Agência Nacional de Saúde (ANS), que inclui resoluções normativas relacionadas à privacidade e proteção de dados. Segundo Almeida Vicente (2019), o conhecimento do ambiente legal e regulatório, incluindo uma compreensão precisa das bases legais que autorizam o tratamento de dados, é fundamental para o desenvolvimento das atividades econômicas desses setores.

Como ilustração de uma obrigação legal específica, é pertinente mencionar o tratamento de dados contidos em prontuários médicos, que deve ocorrer em conformidade com as normativas estabelecidas pela Lei nº 13.787/18. Esta legislação regula a digitalização e o uso de sistemas informatizados para a guarda, armazenamento e manuseio de prontuários de pacientes, estabelecendo diretrizes para o tratamento desses dados sensíveis. Adicionalmente, vale destacar a Resolução nº 1.605/09 do Conselho Federal de Medicina (CFM), que proíbe médicos de revelar o conteúdo do prontuário ou ficha médica do paciente sem o seu consentimento. Esta resolução enfatiza a confidencialidade das informações médicas. Além disso, a Resolução do CFM nº 1.821/07 aprova normas técnicas relativas à digitalização e ao uso de sistemas informatizados para a guarda e manuseio de documentos de prontuários de pacientes, permitindo a eliminação do formato físico (papel) e facilitando a troca de informações identificadas no âmbito da saúde.

A discussão sobre a utilização de dados biométricos de empregados para o controle de jornada ou acesso a áreas restritas nas empresas é um tema contemporâneo relevante no âmbito da escolha da base legal adequada. Pinheiro e Bomfim (2020) argumentam que, embora outros métodos possam ser empregados para registrar a jornada de trabalho, a biometria é considerada o meio mais eficaz para assegurar a integridade e a autenticidade dos registros. A fidedignidade destes é crucial para ambas as partes envolvidas, prevenindo alegações de manipulação da jornada de trabalho e permitindo uma apuração precisa do saldo de horas. Neste contexto, o tratamento de dados biométricos para fins de controle de jornada é

justificado pelo cumprimento de uma obrigação legal[32] pelo controlador, conforme estabelecido no artigo 11, II, “a”, da LGPD.

Teffé (2022) aponta que a questão do uso de dados biométricos em ambientes corporativos, especialmente para controle de jornada e acesso, ainda não está totalmente pacificada. Uma das principais questões levantadas é a "indispensabilidade" da biometria, considerando a existência de sistemas alternativos que apresentam um caráter menos intrusivo. Exemplos de tais sistemas incluem cartões magnéticos individuais, senhas de acesso às dependências da empresa ou a implementação de medidas organizacionais de segurança. Neste contexto, a Autoridade Holandesa de Proteção de Dados impôs uma multa significativa de 725.000 euros a uma empresa por considerar excessiva a exigência de impressões digitais dos funcionários para fins de registro de presença e jornada. A decisão baseou-se na avaliação de que a empresa não estava autorizada a processar esses dados pessoais sensíveis, visto que a sua prática não se enquadrava em nenhuma das exceções legais previstas (AUTORITEIT PERSOONGEGEVENS, 2020).

Um exemplo do uso desta base legal para o tratamento de dados neurais pode ser encontrado no âmbito da regulamentação da pesquisa e desenvolvimento de novos dispositivos conectados ao corpo humano. Por exemplo, no desenvolvimento de novos neurodispositivos, as empresas desenvolvedoras podem estar legalmente obrigadas a coletar e analisar dados neurais como parte dos requisitos regulatórios para testes em humanos. Esses dados são coletados e tratados para atender às normas estabelecidas por agências reguladoras, como a FDA nos Estados Unidos, que exigem a coleta de dados específicos para avaliar a segurança e eficácia de dispositivos que se conectam, ou interpretam, sinais do corpo humano (ESTADOS UNIDOS, 2021). Neste cenário, o tratamento de dados neurais está fundamentado na necessidade de cumprir com as obrigações legais e

[32] CLT, Art. 74. O horário de trabalho será anotado em registro de empregados. §1º (Revogado). §2º Para os estabelecimentos com mais de 20 (vinte) trabalhadores será obrigatória a anotação da hora de entrada e de saída, em registro manual, mecânico ou eletrônico, conforme instruções expedidas pela Secretaria Especial de Previdência e Trabalho do Ministério da Economia, permitida a pré-assinalação do período de repouso. §3º Se o trabalho for executado fora do estabelecimento, o horário dos empregados constará do registro manual, mecânico ou eletrônico em seu poder, sem prejuízo do que dispõe o caput deste artigo. § 4º Fica permitida a utilização de registro de ponto por exceção à jornada regular de trabalho, mediante acordo individual escrito, convenção coletiva ou acordo coletivo de trabalho.

regulatórias impostas aos controladores (empresas desenvolvedoras) no processo de aprovação da disponibilização de novos dispositivos ao mercado consumidor, o que dispensa o consentimento do titular.

3.2.3.3 Tratamento de dados necessários à execução de políticas públicas

A base legal estabelecida Artigo 11, II, "b", da LGPD permite que a Administração Pública realize o tratamento compartilhado de dados pessoais que sejam essenciais à execução de políticas públicas definidas em leis ou regulamentos. Essas políticas públicas podem incluir áreas como saúde pública, prevenção de doenças, campanhas de vacinação, assistência a cidadãos em situações de vulnerabilidade ou iniciativas destinadas a combater a discriminação contra minorias (ANPD, 2022).

Contudo, Wimmer (2021) ressalta uma confusão terminológica na LGPD quanto ao termo "tratamento compartilhado" de dados. Segundo a análise, o "uso compartilhado de dados", definido no Artigo 5º, XVI, constitui uma forma de "tratamento" de dados, como explicado no Artigo 5º, X. Seria ilógico pressupor que a legislação pretendesse restringir o tratamento de dados sensíveis pelo Poder Público exclusivamente a situações de uso compartilhado. Assim, uma interpretação sistemática dos artigos relevantes sugere que o Artigo 11 abrange tanto o tratamento quanto o uso compartilhado de dados sensíveis pela Administração Pública.

Wimmer (2021) observa que o Estado executa uma ampla gama de atividades de tratamento de dados, que nem sempre podem ser enquadradas no conceito de políticas públicas. Atividades como o pagamento de salários e a gestão de servidores públicos, essenciais ao funcionamento do Estado, não são facilmente classificáveis como políticas públicas. Da mesma forma, ações de fiscalização e sancionamento podem ser entendidas como execução de políticas públicas apenas sob uma interpretação ampliada do termo. A solução para essa questão encontra-se na leitura do Artigo 23 da LGPD, que estabelece uma base legal complementar para o tratamento de dados pelo Poder Público, adicionando às previsões dos Artigos 7 e 11 o objetivo de "executar as competências legais ou cumprir as atribuições legais do serviço público".

No contexto do tratamento de dados neurais, um exemplo objetivo utilizando esta base legal envolve a implementação de programas educacionais pelo governo. Uma iniciativa governamental pode ser desenvolvida para incorporar tecnologias de *neurofeedback* em salas de aula, visando melhorar a concentração e o desempenho acadêmico de estudantes em universidades públicas. Neste programa, dispositivos de *neurofeedback* são utilizados para coletar dados neurais dos estudantes enquanto realizam atividades educacionais específicas. A análise desses dados permite aos educadores ajustarem métodos de ensino e conteúdo em tempo real, com base nas respostas neurais dos alunos, promovendo um ambiente de aprendizado mais eficaz e personalizado (KRELL; DOLECKI; TODD, 2023). Sendo necessário o tratamento desses dados para a execução da política pública educacional, a Administração Pública estaria dispensada de obter consentimento.

3.2.3.4 Realização de estudos por órgão de pesquisa

A Lei Geral de Proteção de Dados (LGPD) autoriza o tratamento de dados sensíveis para a realização de estudos por órgãos de pesquisa, abrangendo investigações de natureza histórica, estatística, tecnológica ou científica. Neste contexto, a legislação enfatiza a importância de garantir, sempre que possível, a anonimização dos dados pessoais, visando a proteção da privacidade dos indivíduos envolvidos (BARRETO; ALMEIDA; DONEDA, 2019). O termo “sempre que possível”, abre uma certa margem de discricionariedade, cabendo ao controlador definir quando a anonimização ocorrerá, o que pode gerar certa insegurança jurídica (EIGELSON; BECKER, 2020).

A LGPD define a anonimização de dados como a aplicação de “meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo” (Art. 5º, XI). A Lei considera a anonimização uma medida protetiva para os titulares dos dados, devendo ser garantida sempre que possível. Um dado é considerado anonimizado quando não identifica seu titular, eliminando qualquer relação direta ou indireta com ele. Souza (2020) esclarece que a avaliação de "esforços razoáveis" para anonimização leva em conta fatores objetivos, como o custo e o tempo necessários para reverter o processo de anonimização, em consonância com as

tecnologias disponíveis, conforme estipulado no Artigo 12, §1º, da LGPD. Além disso, fatores subjetivos também são relevantes, como a entidade responsável pela anonimização e quem tenta revertê-la. Uma vez que um dado é anonimizado, ele deixa de ser considerado pessoal segundo o Artigo 12 da LGPD. Esta interpretação está alinhada com o Considerando nº 26 do GDPR, que estabelece que os princípios de proteção de dados não se aplicam a informações anônimas, isto é, informações que não se referem a uma pessoa singular identificada ou identificável, nem a dados pessoais que foram tornados anônimos de maneira que o titular não possa ser identificado.

Não é possível, porém, presumir que a anonimização forneça um alto grau de proteção aos dados, considerando as amplas possibilidades de cruzamento de informações e o avanço contínuo das tecnologias focadas na desanonimização de bases de dados pessoais, incluindo os dados sensíveis. Ruaro e Sarlet (2021) argumentam que, diante dos processos de agregação e reidentificação de bases de dados, um dado anonimizado é, em geral, um dado pessoal. Assim, as formas de discriminação podem sofrer alterações significativas, tornando-se por vezes sutis e imperceptíveis ao cidadão comum. Os autores destacam que o termo "identificável" é frequentemente superável e foi incorporado pela LGPD em relação às formas de expressão da razoabilidade, isto é, ao nível de investimento de tempo e de dinheiro requeridos no processo de anonimização.

Conforme exposto por Mulholland (2020), a responsabilidade pela determinação da viabilidade da anonimização de dados sensíveis é atribuída aos agentes de tratamento de dados, em especial aos órgãos de pesquisa. Neste contexto, é imperativo considerar o desconhecimento e a hipossuficiência do titular dos dados em relação às técnicas de anonimização existentes, a fim de estabelecer um padrão de segurança adequado. Dessa forma, surge a necessidade de regulação por parte da Autoridade Nacional de Proteção de Dados Pessoais (ANPD) no que tange à definição do tipo de tecnologia de segurança e dos sistemas de anonimização de dados que devem ser adotados pelos agentes de tratamento.

Teffé (2022) ressalta que a utilização dessa base legal não é extensiva a todas as instituições. O Artigo 5º, XVIII, da LGPD define o conceito de órgão de pesquisa como “órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as

leis brasileiras, com sede e foro no País, que tenha em sua missão institucional ou em seu objetivo social ou estatutário a realização de pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico". Esta definição estabelece critérios claros para as entidades que se qualificam para utilizar dados sensíveis sob esta base legal, delimitando o escopo de aplicação da norma.

A restrição estabelecida pela Lei Geral de Proteção de Dados (LGPD), que limita a utilização da base legal para o tratamento de dados pessoais a pessoas jurídicas de direito privado sem fins lucrativos, impõe um parâmetro significativo. Essa condição exclui certas entidades de pesquisa privadas, como sociedades, da possibilidade de se valerem dessa base legal. A legitimidade para a utilização dessa base legal recai sobre o órgão de pesquisa como instituição, e não sobre pessoas naturais atuando individualmente, como pesquisadores, bolsistas ou estudantes. Em estudo técnico, a ANPD (2022) destaca que a responsabilidade pelo tratamento de dados pessoais, nas hipóteses previstas nos artigos 7º, IV, e 11, II, "c" da LGPD, recai exclusivamente sobre o órgão de pesquisa. Esta responsabilidade é de natureza institucional, atribuída legalmente à entidade de pesquisa.

No contexto do tratamento de dados neurais, um exemplo objetivo que utiliza esta base legal pode ser encontrado na pesquisa sobre interações humanas e aprendizado de máquina. Uma universidade ou instituição acadêmica pode iniciar um projeto de pesquisa focado no desenvolvimento de algoritmos de inteligência artificial (IA) que aprendem a partir de padrões de atividade cerebral humana, com o objetivo de melhorar interfaces cérebro-computador (BCIs) (TAKAJI; NISHIMOTO, 2020). Neste projeto, dados neurais são coletados de voluntários enquanto realizam tarefas específicas ou são expostos a diversos estímulos visuais ou auditivos. A análise desses dados busca entender como diferentes áreas do cérebro respondem a estímulos específicos, o que pode contribuir significativamente para o avanço da tecnologia de BCIs, melhorando a interação entre humanos e máquinas em diversas aplicações, como jogos eletrônicos, dispositivos de assistência a pessoas com deficiência e interfaces de realidade virtual. Nesse exemplo específico, a instituição de pesquisa controladora dos dados estaria dispensada de obter o consentimento dos titulares ao utilizar a base legal do Art. 11, II, c.

3.2.3.5 Exercício regular de direitos, inclusive em âmbito contratual ou processual

A LGPD contempla também a possibilidade de tratamento de dados sensíveis, sem a necessidade de consentimento, para o exercício regular de direitos em diferentes contextos, incluindo contratos, processos judiciais, administrativos e arbitrais. Conforme Elgenson e Becker (2020), Esta base legal alinha-se com o princípio de legalidade, expresso art. 5º, II, da CRFB/88, pelo qual “ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei”.

Nota-se, contudo, que o Artigo 11 da LGPD não reproduz integralmente a disposição do Artigo 7º, inciso V, que autoriza o tratamento de dados pessoais quando necessário para a execução de um contrato ou de procedimentos preliminares relativos a um contrato do qual o titular dos dados seja parte, a pedido deste último. Essa base legal é importante para o setor de seguros, pois permite a coleta e o tratamento de dados necessários para uma avaliação precisa do risco e para a execução eficiente das obrigações contratuais. Isto porque, este setor demanda a realização de análises preliminares detalhadas para fundamentar a contratação de seguros, processo conhecido como avaliação de risco (CNSEG, 2021).

Palhares, Prado e Vidigal (2021) enfatizam a intenção do legislador em impor um grau elevado de cautela aos agentes de tratamento de dados, conforme estipulado na LGPD. Para o tratamento de dados pessoais sensíveis, a legislação ressalta a necessidade de que o agente de tratamento identifique um direito específico emergente do contrato que justifique sua necessidade, não estando incluídos os procedimentos preliminares para sua execução. Essa abordagem legislativa é particularmente rigorosa, exigindo mais do que uma mera necessidade de tratamento de dados; ela demanda que o tratamento seja essencial. Essa exigência é evidenciada pelo uso do termo “indispensável” no inciso II do Artigo 11 da LGPD. Conforme os autores, a escolha dessa terminologia sublinha o desejo do legislador de restringir o tratamento de dados pessoais aos casos em que é absolutamente necessário para o cumprimento de direitos contratuais específicos.

No tocante ao exercício regular de direitos em contratos, é relevante mencionar situações como as dos seguros saúde ou de vida, nos quais a coleta de informações sensíveis se faz necessária. A ausência do tratamento desses dados pode inviabilizar a entrega da prestação contratualmente acordada, como por exemplo, o ressarcimento de despesas médicas em seguros saúde ou o pagamento

de indenizações em casos de invalidez decorrente de acidente ou doença (TEFFÉ, 2022). Neste contexto, argumenta-se que a seguradora não possui apenas a obrigação de cumprir com os termos do contrato, mas também detém o direito de adimpli-lo. Esse entendimento reflete a necessidade de um tratamento adequado de dados sensíveis para a efetiva execução de obrigações contratuais no setor de seguros. A coleta e o processamento de tais informações, portanto, não se restringem a uma mera formalidade operacional, mas são essenciais para o cumprimento adequado e eficaz dos compromissos assumidos no âmbito da relação contratual (CNSEG, 2021).

No âmbito do GDPR, a doutrina europeia aborda a questão do tratamento de dados sensíveis por seguradoras, especialmente no que concerne ao exercício regular de direitos decorrentes de um contrato. Neste contexto, reconhece-se que uma seguradora pode tratar dados de saúde de um segurado para verificar a regularidade de uma reclamação de indenização oriunda de um sinistro em seguros de pessoas. Ustaran (2018) postula que o uso de dados sensíveis pode ser necessário para que um controlador estabeleça, exerça ou defenda reivindicações legais. Segundo o autor, a dependência deste critério exige que o controlador estabeleça a necessidade. Ou seja, deve haver uma conexão próxima e substancial entre o processamento dos dados e os propósitos pretendidos. Um exemplo de atividade que se enquadraria neste critério é o processamento de dados médicos por uma companhia de seguros para determinar a validade de uma reivindicação de seguro médico de uma pessoa. O processamento desses dados seria necessário para a companhia de seguros considerar a reivindicação apresentada pelo reclamante sob sua apólice de seguro.

Segundo Teffé (2022), no que tange ao exercício regular de direitos ou à defesa em ações judiciais, compreende-se que esta prerrogativa não deve ser restrita exclusivamente a processos judiciais já em andamento. Esta hipótese de tratamento de dados pode ser interpretada de maneira mais abrangente, de modo a incluir procedimentos judiciais futuros. Isso se aplica tanto para o estabelecimento de uma ação quanto para a defesa em processos judiciais, desde que dentro de critérios razoáveis e com justificativa plausível. Além disso, a interpretação abrange a obtenção de orientação jurídica ou outras formas de defesa legal necessárias para o exercício de direitos.

Um exemplo do uso desta base no contexto do tratamento de dados neurais pode ser observado na indústria de tecnologia, especificamente na personalização e no aprimoramento de interfaces cérebro-computador (BCIs) por empresas especializadas. Estas empresas, ao desenvolverem BCIs que permitem aos usuários controlar dispositivos eletrônicos diretamente com seus pensamentos, podem necessitar coletar e analisar dados neurais de indivíduos para aprimorar a precisão e usabilidade de seus produtos. Neste cenário, a coleta de dados neurais é realizada sob a justificativa de exercício regular de direitos em um contexto contratual, onde os usuários das BCIs concordam, através de um contrato de consentimento informado, com a coleta e análise de seus dados neurais. No já citado caso do dispositivo Insight poderia ser aplicada para regularizar a coleta e análise de dados neurais dos usuários. A utilização dessa base legal se justificaria no contexto de um contrato estabelecido entre a Emotiv e seus usuários, onde os termos e condições do uso do Insight são claramente definidos, incluindo a natureza dos dados coletados, as finalidades específicas da coleta e análise desses dados, assim como as medidas de segurança implementadas para proteger a privacidade e a integridade dos dados pessoais sensíveis coletados.

3.2.3.6 Proteção da vida ou da incolumidade física do titular ou de terceiro

Conforme apontado por Teffé (2022), em determinadas circunstâncias, o tratamento de dados pessoais sensíveis pode ser fundamental para a proteção de interesses tanto individuais, como a vida e a integridade física do titular dos dados, quanto coletivos, como em situações humanitárias ou de interesse público. A utilização dessa base legal é particularmente adequada em casos onde o consentimento do titular dos dados é difícil de ser obtido, por exemplo, quando o indivíduo está inconsciente ou desaparecido. Segundo a autora, um exemplo elucidativo seria o caso de uma pessoa inconsciente levada a um hospital, no qual nunca foi atendida anteriormente, após sofrer um grave acidente. Neste cenário, o hospital necessitaria acessar ao menos parte do histórico médico do paciente para prover um atendimento adequado. Nesse contexto, a legislação permite que o médico responsável pelo atendimento solicite informações a outro hospital onde o

paciente tenha sido previamente tratado ou ao médico de confiança do paciente, caso essa informação esteja disponível.

No contexto do tratamento de dados neurais, uma aplicação desta base legal envolve o desenvolvimento e aplicação de sistemas avançados de segurança veicular. Empresas de tecnologia automotiva podem desenvolver sistemas de monitoramento baseados em neurotecnologia que utilizam dados neurais para detectar sinais de sonolência, perda de atenção ou incapacidade do motorista em tempo real. Neste cenário, neurodispositivos instalados no veículo coletam dados neurais do motorista para analisar padrões de atividade cerebral que indiquem fadiga ou distração (ZHANG; HAN; YI et al., 2023). Se sinais preocupantes são detectados, o sistema pode tomar medidas preventivas automáticas, como alertar o motorista, reduzir a velocidade do veículo, ou até mesmo acionar controle autônomo para parar o carro de forma segura, visando prevenir possíveis acidentes. Ao realizar o tratamento desses dados com objetivo de proteger a vida do titular e de terceiros, as empresas estariam dispensadas de obter o consentimento.

3.2.3.7 Tutela da saúde por profissionais e serviços de saúde ou autoridade sanitária

O “Código de Boas Práticas: Proteção de Dados para Prestadores Privados de Serviços em Saúde”, publicado em 2021 pela Confederação Nacional de Saúde (CNSaúde), sublinha a necessidade de cautela na aplicação da base legal para o tratamento de dados em serviços de saúde. Este documento esclarece que o conceito não se aplica indiscriminadamente a todas as etapas da prestação de serviços de saúde. Embora o setor de saúde opere, de maneira geral, em benefício da saúde do paciente, a base legal em questão é especificamente aplicável a “procedimentos realizados por profissionais de saúde, serviços de saúde ou autoridade sanitária”, e não a qualquer processamento de dados no setor de saúde.

Embora seja uma publicação brasileira, o Código de Boas Práticas da CNSaúde sugere que a utilização dessa base legal seja interpretada à luz do conceito de tutela da saúde presente no GDPR, especificamente nos Artigos 9(2)(h) e 9(3), em razão de uma ausência de definição precisa na LGPD. Estes artigos do GDPR estabelecem que o tratamento de dados é permitido quando necessário para

fins de medicina preventiva, avaliação da capacidade de trabalho, diagnóstico médico, prestação de cuidados ou tratamentos de saúde ou gestão de sistemas e serviços de saúde, ou em um contrato com um profissional de saúde. Além disso, o tratamento desses dados deve ocorrer sob a responsabilidade de um profissional obrigado ao sigilo profissional.

De acordo com Teffé (2022), diante das restrições impostas pela legislação em relação aos sujeitos autorizados a utilizar esta base legal para o tratamento de dados, torna-se evidente que os principais controladores neste contexto são os hospitais e outros agentes atuantes na área da saúde. No que concerne à autoridade sanitária, é pertinente mencionar a Lei nº 9.782/99, que estabelece o Sistema Nacional de Vigilância Sanitária e institui a Agência Nacional de Vigilância Sanitária (ANVISA). Contudo, segundo a autora, a respeito da base legal, é possível questionar quem seriam os profissionais de saúde e quais serviços seriam considerados de saúde. Conforme estabelecido pelo “Código de Boas Práticas” (CNSaúde, 2021), é imperativo verificar quais tratamentos de dados são realizados no contexto das atividades principais dos prestadores de serviços de saúde. Isso inclui medicina preventiva ou do trabalho, avaliação da capacidade de trabalho do empregado, diagnóstico médico, prestação de cuidados ou tratamentos de saúde, e se tais dados foram tratados por ou sob a responsabilidade de um profissional sujeito à obrigação de sigilo profissional.

Um exemplo da utilização desta base legal para o tratamento de dados neurais pode ser observado na utilização de neurodispositivos por profissionais de saúde para monitorar e tratar condições neurológicas. Por exemplo, em um centro de neurologia, pacientes que sofrem de epilepsia podem ser submetidos a monitoramento contínuo utilizando neurodispositivos capazes de registrar atividade cerebral em tempo real (NEUROPACE, 2023). Nesse caso, a obtenção consentimento do titular estaria dispensada, uma vez que o tratamento estaria amparado na base legal da tutela da saúde.

3.2.3.8 Garantia da prevenção à fraude e à segurança do titular

O Artigo 11, inciso II, alínea "g", da LGPD introduz uma base legal específica que visa à prevenção de fraudes e à garantia da segurança dos titulares dos dados,

vinculando-se aos interesses tanto dos titulares quanto de determinadas entidades. Esta disposição legal tem aplicabilidade particular em contextos em que a confirmação da identidade dos indivíduos é fundamental. Como ilustração prática, Teffé (2022) menciona situações em que instituições bancárias e empregadores processam dados biométricos para prevenir fraudes, sem necessidade do consentimento dos titulares. Isso ocorre, por exemplo, para assegurar que seja o empregado autorizado acessando áreas restritas da empresa ou para confirmar a identidade de um cliente realizando transações bancárias significativas. Além disso, essa base legal é aplicável na prevenção de fraudes em processos de identificação ou confirmação de identidade em aplicações móveis, como na criação de contas digitais. Similarmente, a coleta de dados biométricos de colaboradores para acesso a sistemas financeiros de uma empresa é uma aplicação pertinente dessa base legal.

Um exemplo do uso desta base no tratamento de dados neurais pode ser encontrado no setor financeiro, especificamente no desenvolvimento e implementação de sistemas de autenticação biométrica neural por bancos e instituições financeiras. Estes sistemas utilizam dados neurais coletados através de dispositivos de interface cérebro-computador (BCIs) para verificar a identidade dos clientes durante transações bancárias online, como acessos a contas, transferências de dinheiro, ou pagamentos (CHAKRABORTY, 2021). Neste contexto, os dados neurais são tratados para criar um perfil de autenticação único para cada cliente, baseado em padrões específicos de atividade cerebral que são extremamente difíceis de replicar ou forjar. O uso desses dados neurais visa prevenir fraudes, como o acesso não autorizado a contas bancárias ou a realização de transações financeiras fraudulentas. Nesse exemplo, com amparo na base legal da garantia da prevenção à fraude, as instituições estariam dispensadas da obtenção do consentimento do titular para realizar o tratamento desses dados.

Após a explanação das bases legais pertinentes ao tratamento de dados pessoais sensíveis, torna-se patente que a proteção atribuída a esses dados é mais rigorosa, refletindo uma abordagem mais cautelosa e adequada para salvaguardar a privacidade mental dos indivíduos. Diante deste panorama, surge a necessidade de examinar a viabilidade de enquadrar os dados neurais sob a mesma esfera de proteção.

4 A PROTEÇÃO DO DADO NEURAL COMO DADO PESSOAL SENSÍVEL

Nesta seção será abordada a proteção dos dados neurais como dados pessoais sensíveis sob a LGPD, explorando duas perspectivas principais. Inicialmente, examina-se a possibilidade de uma interpretação ampliativa do rol do art. 5º, II da referida lei, tratando-o como exemplificativo, o que abriria espaço para incluir os dados neurais como sensíveis. Posteriormente, considera-se a proteção desses dados não pela sua natureza genérica ou sensível, mas pelo tratamento sensível a que podem ser submetidos, que pode revelar informações sensíveis sobre o titular, de modo a atrair para si a aplicação do comando previsto no art. 11 §1º da mesma lei.

4.1 CLASSIFICAÇÃO NO ROL DO ART. 5º, II, DA LGPD

A LGPD, especificamente em seu artigo 5º, inciso II, identifica categorias de dados pessoais considerados sensíveis, abrangendo informações sobre origem racial ou étnica, convicções religiosas, opiniões políticas, filiação sindical ou a organizações de natureza religiosa, filosófica ou política, dados relativos à saúde ou à vida sexual, dados genéticos ou biométricos vinculados a indivíduos. Entretanto, a legislação não clarifica se a listagem apresentada é conclusiva ou meramente ilustrativa, podendo abarcar outras categorias tais como os dados neurais.

No âmbito jurídico, a designação de um rol como taxativo (*numerus clausus*) implica uma enumeração definitiva e restrita, precludindo interpretações que ampliem seu escopo. Por outro lado, uma listagem exemplificativa (*numerus apertus*) sugere uma apresentação não conclusiva, permitindo a inclusão de novas instâncias ou direitos compatíveis com a categoria ou lista inicialmente proposta (NERY JUNIOR, 2014). Teffé (2022) enfatiza a importância de considerar a técnica legislativa adotada, bem como a essência dos direitos envolvidos, seja em aspectos existenciais seja patrimoniais, e como a proteção conferida se alinha ao princípio da dignidade da pessoa humana.

Exemplos de rol taxativo no direito brasileiro incluem: as cláusulas pétreas na CFRB/88, o artigo 60, § 4º, estabelece um rol taxativo de matérias que não podem ser objeto de deliberação para emenda constitucional; os casos de inelegibilidade

previstos na Lei Complementar nº 64/90 (Lei das Inelegibilidades), que estabelece situações específicas nas quais um cidadão é considerado inelegível para cargos públicos eletivos; e as exceções à regra de impenhorabilidade do bem de família, o artigo 3º da Lei nº 8.009/90 estabelece um rol taxativo das hipóteses em que o bem de família pode ser penhorado.

Como exemplo de rol exemplificativo, é possível citar a desconsideração da personalidade jurídica no Código Civil, o artigo 50 prevê a possibilidade em caso de abuso, caracterizado pelo desvio de finalidade ou pela confusão patrimonial, sendo que a doutrina e a jurisprudência entendem que essas não são as únicas hipóteses possíveis, aplicando a teoria da desconsideração de forma mais ampla, conforme as circunstâncias do caso concreto; as inovações tecnológicas na Lei de Direitos Autorais (Lei nº 9.610/98), o artigo 7º, que define as obras intelectuais protegidas, apresenta uma lista que não exclui outras criações do gênero literário, artístico ou científico, ou novas modalidades de criação, sinalizando um rol exemplificativo; e os direitos da personalidade, o artigo 5º da CFRB/88 lista uma série de direitos fundamentais, dentre outros deveres e garantias, mas não se limita a eles, permitindo a interpretação de que outros direitos, embora não explicitados, também são constitucionalmente protegidos em razão do princípio da dignidade da pessoa humana.

Este último exemplo possui ligação significativa com a categoria dos dados pessoais sensíveis e pode auxiliar na classificação do rol do art. 5º, II, da LGPD como exemplificativo. A discussão sobre os direitos da personalidade é marcada por uma abordagem pluralista, como aponta Gomes (1983), que defende a existência de múltiplos direitos autônomos e distintos, agrupados devido a suas características comuns. Segundo o autor, essa visão se contrapõe à ideia de um direito geral de personalidade, argumentando que a efetiva proteção desses direitos se concretiza através de legislações específicas, reconhecendo a diversidade dos bens jurídicos protegidos.

Perlingieri (2008) contribui para essa discussão ao distinguir entre teorias que advogam por um conjunto aberto de direitos da personalidade, caracterizando a atipicidade, e aquelas que propõem um rol fechado, baseado na tipicidade. Essa contraposição reflete diferenças ideológicas e culturais profundas. O autor critica a limitação dos direitos da personalidade ao aspecto patrimonial, propondo que a

personalidade deveria ser compreendida como um valor central do ordenamento jurídico, que fundamenta "uma série aberta de situações subjetivas existenciais" necessitadas de proteção constante e adaptável.

Dessa forma, segundo Perlingieri (2008), a jurisprudência não deve negar proteção a manifestações da personalidade que, embora não estejam expressamente previstas em códigos específicos, possuem relevância jurídica e, por consequência, merecem tutela judicial. Esta concepção é corroborada no contexto brasileiro por Teffé (2016), que observa a adoção da perspectiva pluralista pelo legislador nacional, refletida tanto na CFRB/88 quanto no Código Civil. Assim, entende-se que o rol de direitos da personalidade não é exaustivo, permitindo ao intérprete a garantia de proteção às diversas manifestações existenciais da pessoa, já que estas possuem intrínseca importância no ordenamento jurídico.

Considerando os princípios fundamentais da categoria dos dados sensíveis, a proteção de dados pessoais como um direito da personalidade e sua intrínseca relação com aspectos existenciais do ser humano, pode ser interpretado que o rol de dados sensíveis previsto na LGPD deva ser compreendido de maneira exemplificativa, permitindo uma tutela abrangente e contextual (KONDER, 2019). Como direito inerente à personalidade, a proteção de dados pessoais é essencial, irrenunciável e intransferível, sustentando a necessidade de uma flexibilização do conceito de dados sensíveis para abarcar proteções atípicas que resguardem o direito à existência e o pleno desenvolvimento da vida em sociedade (PERLINGIERI, 2008).

Uma delimitação exaustiva de dados sensíveis poderia excluir demandas e manifestações individuais que, diante do avanço social e tecnológico, requeiram proteção ampliada, conforme argumenta Teffé (2022). Nesta linha, Mulholland (2020) enfatiza que a definição contida no Art. 5º, II, da LGPD não deve ser interpretada como taxativa, mas sim como exemplificativa, sem limitar a possibilidade de inclusão de novas hipóteses que demandem proteção jurídica. Neste contexto de inovação tecnológica, enquadra-se o tratamento de dados neurais, que possibilita novos cenários de acesso a informações sensíveis dos titulares dos dados.

Negri e Korkmaz (2019) argumentam que o regime de proteção aos dados pessoais sensíveis estabelecido pela LGPD é rigoroso, mas o artigo 5º, inciso II, não

abrange todas as circunstâncias potenciais de discriminação e desigualdade, devido ao seu enfoque em um modelo específico de situações jurídicas. Tal limitação poderia comprometer a isonomia ao excluir de proteção específica dados que, por sua natureza, se enquadram na categoria de sensíveis, ainda que não listados explicitamente. Assim, uma proteção efetiva no contexto das sociedades da informação exige uma abordagem ampla no tratamento normativo dos dados sensíveis.

Miragem e Petersen (2020) corroboram essa visão, destacando que os dados pessoais identificados como sensíveis merecem um nível de proteção superior, mediante a imposição de regras mais estritas para seu tratamento. Essa necessidade decorre tanto da privacidade intensificada que tais dados representam quanto do potencial discriminatório de seu uso indevido. A regulamentação dos dados sensíveis está intrinsicamente relacionada ao princípio da não discriminação, visando prevenir abusos por meio de disposições específicas. Ressaltam, ainda, que o conceito de dados sensíveis na LGPD não é fixo, permitindo a inclusão de novas categorias de dados que, embora não previstos inicialmente, apresentem riscos significativos de discriminação ao titular (art. 11, §1º, da LGPD), evidenciando que dados considerados comuns podem adquirir status de sensíveis diante de contextos discriminatórios, conforme será visto na próxima subseção.

Teffé (2022) destaca que a fundamentação para a instituição da categoria de dados sensíveis na legislação, particularmente na proteção de dados, deriva da necessidade de resguardar informações suscetíveis a serem empregadas em contextos de discriminação ilícita ou abusiva. Dessa forma, o escopo de proteção desses dados sensíveis pode ser expandido para abarcar, dependendo do contexto e da aplicação, informações relativas à orientação sexual, nacionalidade, condições socioeconômicas do indivíduo, bem como dados sobre antecedentes e condenações criminais, entre outros.

A Lei do Cadastro Positivo (Lei nº 12.414/11), em seu artigo 3º, § 3º, proíbe expressamente o registro de informações consideradas sensíveis, tais como aquelas referentes à origem social e étnica, saúde, genética, orientação sexual, e convicções políticas, religiosas e filosóficas. A inclusão da categoria "origem social" na legislação do Cadastro Positivo, embora ausente na LGPD, sublinha a necessidade de uma proteção mais abrangente para informações que possam ser empregadas

de maneira discriminatória, conforme apontam Knopp e Collares (2019). Decisões do Superior Tribunal de Justiça (STJ)[33] sobre os limites da prática de *credit scoring* e a aplicação da Lei do Cadastro Positivo reiteram a restrição ao uso de dados sensíveis para prevenir práticas discriminatórias e citam, além da origem social, a categoria "orientação sexual", também ausente na LGPD. Desse modo, considerando-se taxativo o rol do art. 5º, II, da LGPD, algumas categorias de notória sensibilidade ficariam de fora do regime específico destinado aos dados pessoais sensíveis, impactando na forma de tratamento desses dados (KORKMAZ, 2019).

Ao defender a inclusão dos dados de pessoas com deficiência como dados pessoais sensíveis, Lopes (2023) evidencia a complexidade na categorização de determinados tipos de dados na LGPD. Dados relativos à deficiência, assim como os dados neurais, podem ser interpretados como sendo da espécie "dados de saúde", explicitamente mencionada na LGPD. No entanto, Lopes (2023) argumenta que as deficiências apresentam desafios multifacetados que transcendem uma simples classificação como questões de saúde, pois nem todas as deficiências são resultado de doenças. Analogamente, os dados neurais, apesar de poderem ser considerados dados de saúde em certos contextos, têm aplicações que vão além do âmbito da saúde, como entretenimento, educação e marketing, conforme abordado na subseção 2.1. Portanto, uma interpretação restritiva do rol de dados sensíveis na LGPD poderia excluir injustamente os dados neurais dessa categoria, limitando assim a proteção desses dados.

Bobbio (1992) argumenta que "os direitos constituem uma classe variável" e que, "no futuro, poderão surgir novas pretensões que no momento sequer podemos imaginar". Nesse sentido, Negri e Korkmaz (2019) defendem a aplicação de uma possível cláusula geral aos dados pessoais sensíveis, oxigenando o ordenamento jurídico "mediante princípios valorativos e elementos extrajurídicos, permitindo a adaptação do direito à dinâmica social". Esta proposta encontra especial relevância no contexto das neurotecnologias, uma vez que os dados neurais, derivados de atividades cerebrais, apresentam um potencial significativo para revelar informações profundas e pessoais sobre um indivíduo. Como visto anteriormente, tais dados, por sua natureza intrínseca, podem revelar aspectos íntimos da personalidade,

[33] REsp 1.419.697 – RS e Resp 1.457.199 – RS.

preferências, predisposições e, até mesmo, intenções futuras do titular dos dados. A aplicação de uma cláusula geral, conforme sugerido por Negri e Korkmaz (2019), permitiria ao ordenamento jurídico absorver e regular de forma eficaz os desafios emergentes trazidos pelo avanço das neurotecnologias.

Nesse cenário, o já mencionado dispositivo *Insight*, desenvolvido pela empresa Emotiv, exemplifica a necessidade de o direito adaptar-se às novas realidades sociais impostas pelas neurotecnologias. A Emotiv descreve o *Insight* como equipado com cinco sensores EEG e dois de referência, sendo capaz de fornecer análises detalhadas sobre a atividade cerebral do usuário. As medições baseiam-se em seis métricas cognitivas e emocionais chave: foco, estresse, excitação, relaxamento, interesse e engajamento (EMOTIV, 2024). Estas métricas permitem o monitoramento do estado cognitivo e do bem-estar de um indivíduo. Desse modo, os dados neurais coletados pelo *Insight* têm o potencial de revelar informações pessoais e íntimas sobre um indivíduo, semelhantes às categorias de dados pessoais sensíveis definidas pela LGPD. Essas informações podem incluir, mas não se limitam a, predisposições psicológicas, estados emocionais, níveis de estresse e foco, e outras características que refletem a personalidade e a condição mental do titular dos dados. Consequentemente, a classificação desses dados como sensíveis sob a LGPD pode ser justificada pela sua natureza íntima e pelo potencial de afetar os direitos da personalidade, como a privacidade mental e a autodeterminação. A semelhança entre as informações potencialmente reveladas pelo tratamento de dados neurais e aquelas reveladas pelas categorias de dados pessoais sensíveis corporais listadas na LGPD, como os dados genéticos[34], reforça a argumentação de que os dados neurais poderiam ser enquadrados nessa categoria.

Como abordado na subseção 2.2, o direito à privacidade mental é um dos cinco neurodireitos propostos pela Neurorigths Foundation. A classificação de dados neurais sob a categoria dos dados pessoais sensíveis poderia reforçar a proteção dessa dimensão da privacidade, considerando o potencial discriminatório e os riscos

[34] Há uma preocupação real de que pessoas com certos marcadores genéticos possam enfrentar discriminação, seja em termos de empregabilidade ou de cobertura de seguro, baseada na predisposição genética para determinadas doenças ou comportamentos, mesmo quando essas predisposições não garantem o desenvolvimento da condição (ABNEURO, 2022), de modo similar ao que pode ser revelado pela identidade neural de um indivíduo.

à dignidade humana que seu tratamento inadequado pode acarretar (LIGTART et al, 2023). A proposição dos neurodireitos, portanto, não só responde às questões emergentes trazidas pelas neurotecnologias, mas também aponta para a necessidade de adaptar o direito à dinâmica social, em linha com as reflexões de Bobbio (1992) sobre a variabilidade dos direitos e a proposta de Negri e Korkmaz (2019) para uma cláusula geral que permita a adaptação do direito à sociedade.

Por outro lado, conforme Teffé (2022), parte da doutrina sustenta que o rol de dados sensíveis na LGPD deveria ser interpretado de forma taxativa, argumentando que a especificidade e as restrições impostas ao seu tratamento justificam uma definição limitada e precisa desses dados. Nessa perspectiva, o Art. 5º, II, da LGPD não seria interpretado como um conceito aberto com elementos exemplificativos, mas como uma definição que delimita um rol fechado e específico de dados sensíveis (LEONARDI, 2019). Gusmão (2024) argumenta que a taxatividade proporcionaria maior segurança jurídica para as partes envolvidas e facilitaria o tratamento de grandes volumes de dados sensíveis. Nesse sentido, atualmente está em discussão na Câmara dos Deputados o Projeto de Lei 522/22 [35]que propõe inserir no rol 5º, II, da LGPD a espécie dos dados neurais.

Contudo, a preferência por uma interpretação taxativa do rol de dados sensíveis na LGPD não impede que dados pessoais não listados explicitamente na Lei sejam tratados com a mesma cautela dedicada aos dados sensíveis, particularmente em contextos em que estes possam revelar informações de caráter sensível. Esta abordagem é corroborada pelo parágrafo 1º do Art. 11, que será discutido em detalhes na próxima subseção.

4.2 POTENCIAL DE REVELAÇÃO DE DADOS SENSÍVEIS CONFORME ART. 11, §1º, DA LGPD

Mullholand (2020) enfatiza que a determinação da sensibilidade de um dado não deve se restringir exclusivamente à sua natureza intrínseca ou ao seu conteúdo específico, mas sim à sua potencialidade para promover discriminação no âmbito do tratamento de dados pessoais. A restrição ao tratamento desses dados emerge da

[35] PROJETO DE LEI Nº 522, DE 2022 (Do Dep. Carlos Henrique Gaguim). Modifica a Lei n° 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), a fim de conceituar dado neural e regulamentar a sua proteção.

necessidade de evitar seu emprego de forma a resultar em discriminação, abuso ou desigualdade. Portanto, além da análise da característica estrutural do dado, é imperativo reconhecer que certos dados podem ser considerados sensíveis com base nas implicações do seu uso no processo de tratamento de dados, ampliando a concepção do que pode ser entendido como dado sensível de acordo com o contexto de sua aplicação.

Para assegurar a proteção dos direitos fundamentais da pessoa, o parágrafo primeiro do artigo 11 da LGPD estabelece que as normas atinentes aos dados sensíveis são extensíveis a quaisquer dados pessoais cujo tratamento possa revelar aspectos sensíveis do titular, expondo-o a potenciais prejuízos. Conforme Rodrigues e Hibner (2020), todos os dados considerados sensíveis compartilham a vulnerabilidade à utilização discriminatória, implicando que a definição de tais dados não pode ser concebida de maneira limitada. Nesse contexto, Rodotà (2008) esclarece que a formação de perfis baseada em dados pessoais propicia a ocorrência de discriminação sob diversas circunstâncias: dados inicialmente percebidos como não sensíveis podem adquirir tal característica mediante tratamento, possibilitando a identificação do indivíduo e de aspectos íntimos como hábitos, relações sociais, preferências e convicções; além disso, o processamento de dados que resulta na identificação de grupos estigmatizados atribui-lhes conotações negativas.

De acordo com Palhares, Parado e Vidigal (2021), a sensibilidade não reside nos dados em si, mas na inferência ou interpretação derivada deles, que, dependendo dos propósitos de tratamento, podem demandar a aplicação de medidas restritivas conforme o Artigo 11, parágrafo 1º, da LGPD, ainda que não sejam inicialmente classificados como dados sensíveis. Teffé (2022) complementa essa visão, indicando que a determinação da sensibilidade de uma informação deve levar em conta o contexto do tratamento, a finalidade, o uso efetivo da informação, seu potencial discriminatório quando combinada com outros dados, e a própria definição de "dado pessoal". Essa interpretação é reforçada pelo enunciado n. 690[36], validado na IX Jornada de Direito Civil do Conselho da Justiça Federal (CJF) em

[36] “A proteção ampliada conferida pela LGPD aos dados sensíveis deverá ser também aplicada aos casos em que houver tratamento sensível de dados pessoais, tal como observado no §1º do art. 11 da LGPD.”

maio de 2022, que sugere que a proteção reforçada aos dados sensíveis estipulada pela LGPD também se estenda a situações em que o tratamento de dados pessoais seja considerado sensível, conforme exemplificado pelo parágrafo 1º do Artigo 11.

Segundo Doneda (2020), as evoluções na tecnologia e ciência ampliam as formas de tratamento de dados pessoais, sugerindo a necessidade de novas classificações, categorias e mecanismos de proteção. Atualmente, informações pessoais anteriormente não consideradas sensíveis podem, devido a avanços tecnológicos e científicos, estar sujeitas a tratamento discriminatório ilícito ou abusivo ou ser utilizadas para deduzir ou inferir dados sensíveis. Doneda e Monteiro (2015) investigaram a solicitação de dados sobre nacionalidade na Universidade Federal de Santa Maria, evidenciando a complexidade da coleta de informações potencialmente discriminatórias. A requisição, motivada por um pedido de acesso à informação de entidades externas, incluía dados sobre a presença de indivíduos israelenses entre alunos e professores. O caso suscita preocupações quanto à possibilidade de uso discriminatório dessas informações, embora a nacionalidade, por si só, não figure tipicamente como dado sensível. O exemplo ilustra como informações aparentemente neutras podem adquirir caráter sensível dependendo de seu tratamento e finalidade.

Em análises recentes, identificou-se uma prática discriminatória, no Reino Unido, em que motoristas com nomes percebidos como não ingleses enfrentavam cotações de seguros de carro superiores às de indivíduos com nomes de ressonância inglesa, uma vez que grandes seguradoras praticavam diferenciação tarifária baseada no nome do motorista (LEO, 2018). Paralelamente, observou-se a recusa de concessão de crédito a indivíduos cujos nomes são estatisticamente mais comuns entre comunidades afrodescendentes dos Estados Unidos (TEPEDINO, 2019). Esses exemplos ilustram como o nome de uma pessoa, um dado pessoal genérico, dependendo do contexto de seu uso, pode adquirir a natureza de dado sensível, em virtude de tratamentos que potencializam discriminação ou estigmatização.

Wachter e Mittelstadt (2019) analisam a questão das inferências derivadas de dados pessoais e se estas, dependendo do conteúdo revelado, poderiam ser consideradas sensíveis no contexto normativo europeu. Destacam que informações como gênero, idade, situação financeira, geolocalização e perfis pessoais não são

classificadas como dados sensíveis sob o Artigo 9 do GDPR, apesar de frequentemente servirem como base para discriminação. Conforme o Regulamento Europeu, existe uma proibição geral ao processamento de dados sensíveis, com exceções incluindo consentimento explícito, propósitos científicos ou estatísticos, e quando "o processamento se relaciona a dados pessoais que são manifestamente tornados públicos pelo titular dos dados". As preocupações sobre inferências são implícitas na definição das "categorias especiais de dados pessoais". A expressão "dados pessoais revelando" sugere que a definição visa cobrir dados que divulgam direta ou indiretamente atributos protegidos.

Nesse contexto, em diretrizes sobre perfilamento, o Grupo de Trabalho do Artigo 29[37] (2017) observou que atividades de perfilamento podem criar dados sensíveis "por inferência de dados que não são, por si só, categorias especiais de dados, mas tornam-se ao ser combinados com outros dados". Um estudo acadêmico (KOSINSKI; STILWELL; GRAEPEL, 2017) combinou 'curtidas' no Facebook com informações limitadas de pesquisa e descobriu que os pesquisadores previram corretamente a orientação sexual de usuários do sexo masculino 88% das vezes; a origem étnica de um usuário 95% das vezes; e se um usuário era cristão ou muçulmano 82% das vezes. Diante desse cenário, o Grupo de Trabalho do Artigo 29 (2017) entende que dados que não são sensíveis por natureza devem ser tratados como tal se "revelam indiretamente" ou podem ser usados para inferir atributos sensíveis.

Conforme Lopes (2021), a análise do § 1º do art. 11 da LGPD revela uma abertura normativa que permite a aplicação das restrições de tratamento de dados sensíveis a quaisquer dados pessoais que, ao serem tratados, possam revelar informações sensíveis ou causar dano ao titular. Essa disposição amplia o espectro de proteção além dos casos explicitamente mencionados no rol do art. 5º, II, da LGPD. Nesse sentido, embora os dados neurais não estejam explicitamente listados

[37] O Grupo de Trabalho do Artigo 29 (Art. 29 WP) era um órgão consultivo independente europeu sobre proteção de dados e privacidade, estabelecido sob a Diretiva de Proteção de Dados da União Europeia 95/46/EC. Era composto por representantes das autoridades nacionais de proteção de dados de cada Estado-Membro da UE, do Supervisor Europeu de Proteção de Dados (EDPS), e da Comissão Europeia. O grupo fornecia pareceres sobre questões de proteção de dados para promover a aplicação uniforme da Diretiva em toda a UE. Com a entrada em vigor do Regulamento Geral sobre a Proteção de Dados (GDPR) em 25 de maio de 2018, o Art. 29 WP foi substituído pelo Comitê Europeu de Proteção de Dados (EDPB), que possui uma estrutura e mandato semelhantes, mas com capacidade legal reforçada para garantir a conformidade com o GDPR em toda a União Europeia.

como sensíveis na LGPD, a natureza íntima e a capacidade de revelar informações profundas sobre a personalidade, preferências, condições de saúde mental e até predisposições comportamentais do indivíduo pode justificar uma proteção equivalente à dos dados sensíveis.

Ao analisar novamente o uso do dispositivo *Insight* da Emotiv, observa-se que, independentemente da natureza inicialmente genérica dos dados coletados, o tratamento desses dados pode desvendar informações sensíveis, encaixando-se no âmbito do art. 11, §1º da LGPD. Este neurodispositivo, ao acessar informações neurais, pode permitir análises e inferências sobre aspectos profundos da personalidade do usuário, como suas reações emocionais a conteúdos específicos, podendo revelar indiretamente suas crenças religiosas ou opiniões políticas através do registro de estímulos neurais (BUBLITZ, 2023). Como visto anteriormente, as categorias de dados pessoais consideradas sensíveis sob a LGPD incluem opiniões políticas e crenças religiosas, quando vinculadas a uma pessoa natural. Além disso, os dados neurais coletados pelo *Insight*, ao refletirem aspectos cognitivos e emocionais, como foco e estresse, oferecem uma janela para a condição psicológica do indivíduo, assemelhando-se, nesse aspecto, aos dados genéticos e biométricos, que também podem expor predisposições a certas condições ou características pessoais intrínsecas.

Nesse sentido, a norma do art. 11 §1º da LGPD pode ser vista como um instrumento legal que contribui para a efetivação do direito à privacidade mental ao permitir que os dados neurais, pelo seu potencial de revelar informações sensíveis ou causar dano ao titular, sejam tratados com as mesmas restrições aplicadas aos dados sensíveis explicitamente listados pela lei (SILVA, 2022). Essa perspectiva se alinha com as preocupações e recomendações levantadas pelos pesquisadores e cientistas que propõem os neurodireitos, oferecendo um caminho para a proteção jurídica dos dados neurais e, por extensão, da privacidade mental frente aos desafios impostos pelo avanço das neurotecnologias (AZEVEDO, 2021).

5 **CONCLUSÃO**

A investigação realizada sobre a classificação dos dados neurais como dados pessoais sensíveis, em conformidade com a LGPD, revelou a necessidade de uma tutela jurídica que contemple as especificidades e potenciais riscos associados ao tratamento desses dados. A análise multidisciplinar permitiu uma compreensão ampliada sobre a matéria, corroborando a hipótese inicial de que: os dados neurais requerem o mesmo nível de proteção atribuído aos dados pessoais sensíveis em razão de 1) sua natureza sensível ou 2) de sua capacidade de revelar informações sensíveis sobre os indivíduos ao serem tratados.

A pesquisa concluiu que o tratamento de dados neurais, devido à sua capacidade de revelar aspectos sensíveis do indivíduo, demanda o mesmo nível de proteção atribuída aos dados pessoais sensíveis, nos moldes do art. 11, §1º da LGPD. Além disso, foi evidenciado que os dados neurais, pela sua natureza semelhante às espécies tipificadas como sensíveis, podem sim ser considerados como tal, ao considerar-se o rol do art. 5º, II, da LGPD como exemplificativo.

A pesquisa atingiu seus objetivos, oferecendo uma análise que englobou desde a caracterização dos dados neurais, passando pela legislação pertinente, até as implicações e precedentes internacionais. Entende-se que a legislação brasileira, apesar de avançada, necessita de atualizações para abordar os desafios emergentes trazidos pelas neurotecnologias. Esta necessidade inclui a possibilidade de uma inclusão explícita dos dados neurais no rol do art. 5º, II, da LGPD, assegurando que a proteção à privacidade e aos dados pessoais se mantenha resiliente frente aos avanços tecnológicos. Essa inclusão não apenas alinharia a legislação brasileira com as demandas impostas pelo avanço tecnológico, mas também reforçaria o compromisso do Brasil com a proteção da privacidade e dos dados pessoais em um cenário global.

A pesquisa enfrentou limitações decorrentes da rápida evolução das neurotecnologias e da escassez de precedentes legais e doutrinários específicos sobre o tratamento de dados neurais. Essa dinâmica impõe desafios para uma análise conclusiva sobre a aplicabilidade da LGPD aos dados neurais, sugerindo a necessidade de estudos contínuos e atualizados à medida que novas tecnologias e aplicações surgem.

Futuramente, vislumbra-se a possibilidade de pesquisar abordagens para o consentimento informado no uso de neurotecnologias, considerando os desafios únicos apresentados pela natureza potencialmente invasiva e pela complexidade dessas tecnologias. A capacidade de acesso a informações sensíveis através do tratamento de dados neurais pode não ser totalmente compreendida no momento do consentimento, tanto pelos titulares dos dados quanto pelos controladores. Informações não previstas podem ser descobertas ou utilizadas de maneiras não consentidas inicialmente. A realização do primeiro implante de um dispositivo da Neuralink em humanos representa um marco crucial na aplicação de neurotecnologias, ressaltando a urgência de explorar abordagens robustas para o consentimento informado.

Além disso, também se mostra pertinente monitorar como outros países estão regulamentando os dados neurais e neurotecnologias, com o objetivo de identificar melhores práticas e abordagens regulatórias que possam ser adaptadas ao contexto brasileiro.

Este trabalho reforça a importância de uma abordagem proativa e reflexiva sobre a proteção da privacidade mental e da integridade dos indivíduos na era digital, especialmente no que tange aos avanços nas neurotecnologias e ao tratamento de dados neurais. A pesquisa aponta para a necessidade de um diálogo contínuo entre legisladores, acadêmicos, profissionais da área de tecnologia e a sociedade, para assegurar que os direitos à privacidade e proteção de dados pessoais sejam preservados diante dos desafios tecnológicos contemporâneos.

REFERÊNCIAS

ABNEURO - ACADEMIA BRASILEIRA DE NEUROLOGIA. **Consequências de fatores genéticos e ambientais na doença de Parkinson**. 2021. Disponível em: https://abneuro.org.br/2022/01/13/consequencias-de-fatores-geneticos-e-ambientais-na-doenca-de-parkinson/. Acesso em: 6 fev. 2024.

AGARWAL, Sharad; DUTTA, Tanusree. **Neuromarketing and consumer neuroscience**: current understanding and the way forward. 2015. Disponível em: https://doi.org/10.1007/s40622-015-0113-1. Acesso em: 11 nov. 2023.

AGOSTINHO, Santo; OLIVEIRA, Nair de Assis (Org.). **O Livre Arbítrio**. São Paulo: Paulus, v. 8, 1995.

ALEMANHA. Bundesverfassungsgericht (Tribunal Constitucional Federal). Volkszählungsurteil. **Diário Oficial da União**, 15 de dezembro de 1983. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html. Acesso em: 13 nov. 2023.

ALLEN, Anita L.. **Privacy-as-Data Control**: Conceptual, Practical, and Moral Limits of the Paradigm . 2000. Disponível em: https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1789&context=faculty_scholarship. Acesso em: 12 nov. 2023.

ALMADA, Leonardo Ferreira. Percepção Emocional e Processamento de Informações Emocionais no Reconhecimento de Expressões Faciais: origens psicológicas do julgamento social. **Dois pontos: Revista dos Departamentos de Filosofia da UFPR e da UFSCar**, v. 9, n. 2, 02 dez. 2012. Disponível em: http://dx.doi.org/10.5380/dp.v9i2.26594. Acesso em: 14 jan. 2024.

ANPD. **Guia Orientativo**: Tratamento de Dados Pessoais pelo Poder Público. 2022. Disponível em: https://www.gov.br/anpd/ptbr/assuntos/noticias/no-dia-internacional-da-protecao-de-dados-anpd-publicaguia-orientativo-sobre-tratamento-de-dados-pessoais-pelo-poder-publico. Acesso em: 25 jan. 2024.

ARAGÃO, Suéllyn Mattos de; SCHIOCCHET, Taysa. Lei Geral de Proteção de Dados: desafio do Sistema Único de Saúde. **RECIIS – Revista Eletrônica de Comunicação, Informação e Inovação em Saúde**, Rio de Janeirro, v. 14, jul./set. 2020.

ARISTÓTELES; PESSANHA, José Américo Motta (Org.). **Ética a Nicômaco**: Poética. 4 ed. São Paulo: Nova Cultural, v. 2, 1991.

ARTICLE 29 WORKING PARTY. **Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679**. 2018. Disponível em: https://ec.europa.eu/newsroom/article29/items/612053/en. Acesso em: 25 jan. 2024.

ARTICLE 29 WORKING PARTY. **Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS)**. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/610171. Acesso em: 25 jan. 2024.

ASHER-SCHAPIRO, Avi; BAPTISTA, Diana. **Hands off my brainwaves:**: Latin America in race for 'neurorights'. Reuters. 2023. Disponível em: https://www.reuters.com/article/tech-privacy-brainwaves-idUSL8N3AH6D6/. Acesso em: 12 nov. 2023.

AUTORITEIT PERSOONSGEGEVENS. **Company fined for processing employees' fingerprint data**. 2020. Disponível em: https://www.autoriteitpersoonsgegevens.nl/en/current/company-fined-for-processing-employees-fingerprint-data. Acesso em: 25 jan. 2024.

BARROSO, Luís Roberto. **A dignidade da pessoa humana no direito constitucional contemporâneo**: natureza jurídica, conteúdos mínimos e critérios de aplicação.. 2010. Disponível em: http://www.luisrobertobarroso.com.br/wpcontent/uploads/2010/12/Dignidade_texto-base_11dez2010.pdf. Acesso em: 15 jan. 2024.

BAYNES, Chris. **Chinese schools scanning children's brains to see if they are concentrating**. The Independent. 2019. Disponível em: https://www.independent.co.uk/tech/china-schools-scan-brains-concentration-headbands-children-brainco-focus-a8728951.html. Acesso em: 18 nov. 2023.

BECHTEL, William. **Mental Mechanisms**: Philosophical Perspectives on Cognitive Neuroscience. 1 ed. Routledge, 2007.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: A Função e os Limites do Consentimento. 3 ed. Forense, 2021.

BOONE , Worth ; PICCININI, Gualtiero . The cognitive neuroscience revolution. **Synthese**, v. 193, mai. 2016. Special Issue on Neuroscience and its Philosophy.

BORGATTI, Stephen P. Centrality and network flow. **Social Networks**, v. 27, n. 1, jan. 2005.

BORGESIUS, Frederik J Zuiderveen *et al*. **Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation**. European Data Protection Law Review. 2017. Disponível em: https://www.ivir.nl/publicaties/download/EDPL_2017_03.pdf. Acesso em: 25 jan. 2024.

BOSTROM, Nick. Are We Living in a Computer Simulation?. **The Philosophical Quarterly**, v. 53, n. 211, apr. 2023. Disponível em: https://doi.org/10.1111/1467-9213.00309. Acesso em: 12 nov. 2023.

BRASIL, Marcus Vinícius. **Paraplégico chuta bola na abertura da Copa com suporte de exoesqueleto**. Exame. 2014. Disponível em: https://exame.com/ciencia/paraplegico-chuta-bola-na-abertura-da-copa-com-suporte-de-exoesqueleto/. Acesso em: 18 nov. 2023.

BRASIL. Altera as Leis nºs 12.037, de 1º de outubro de 2009, e 7.210, de 11 de julho de 1984 - Lei de Execução Penal, para prever a coleta de perfil genético como forma de identificação criminal, e dá outras providências. Lei n. 12654, de 27 de maio de 2012. Disponível em: https://planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12654.htm. Acesso em: 25 nov. 2023.

BRASIL. Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. Lei n. 9610, de 18 de fevereiro de 1998. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9610.htm. Acesso em: 22 nov. 2023.

BRASIL. **Constituição**. República Federativa do Brasil de 1988. Brasília, DF. Senado Federal, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/ConstituicaoCompilado.htm. Acesso em: 11 nov. 2023.

BRASIL. Câmara dos Deputados. Projeto de Lei n. 522/22, de 08 de março de 2023. Disponível em: https://www.camara.leg.br/propostas-legislativas/2317524. Acesso em: 26 nov. 2023.

BRASIL. Código Civil. Lei n. 10406, de 09 de janeiro de 2002. **Diário Oficial da União**. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 11 nov. 2023.

BRASIL. Define o Sistema Nacional de Vigilância Sanitária, cria a Agência Nacional de Vigilância Sanitária, e dá outras providências. Lei n. 9782, de 25 de janeiro de 1999. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9782.htm#:~:text=LEI%20N%C2%BA%209.782%2C%20DE%2026%20DE%20JANEIRO%20DE%201999.&text=Define%20o%

20Sistema%20Nacional%20de,Sanit%C3%A1ria%2C%20e%20d%C3%A1%20outras%20provid%C3%AAncias.&text=CAP%C3%8DTULO%20I-,Art.,6%C2%BA%20e%20pelos%20arts.. Acesso em: 20 nov. 2023.

BRASIL. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Lei n. 12414, de 08 de junho de 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 23 nov. 2023.

BRASIL. Dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente. Lei n. 13787, de 26 de dezembro de 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13787.htm. Acesso em: 19 nov. 2023.

BRASIL. Dispõe sobre a Identificação Civil Nacional (ICN). Lei n. 13444, de 10 de maio de 2017. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13444.htm. Acesso em: 16 nov. 2023.

BRASIL. Dispõe sobre a impenhorabilidade do bem de família. Lei n. 8009, de 28 de março de 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8009.htm. Acesso em: 21 nov. 2023.

BRASIL. Dispõe sobre a proteção do consumidor e dá outras providências. Lei n. 8078, de 10 de setembro de 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 12 nov. 2023.

BRASIL. Dispõe sobre a remoção de órgãos, tecidos e partes do corpo humano para fins de transplante e tratamento e dá outras providências. Lei n. 9434, de 03 de fevereiro de 1997. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9434.htm. Acesso em: 24 nov. 2023.

BRASIL. Dispõe sobre os planos e seguros privados de assistência à saúde. Lei n. 9656, de 02 de junho de 1998. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9656.htm. Acesso em: 18 nov. 2023.

BRASIL. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.. Lei n. 12965, de 22 de abril de 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 13 nov. 2023.

BRASIL. Lei Geral de Proteção de Dados Pessoais (LGPD). Lei n. 13.709, de 13 de agosto de 2018, Brasília, 14 de agosto de 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 11 nov. 2023.

BRASIL. Lei n. 12527, de 17 de novembro de 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 14 nov. 2023.

BRASIL. Lei n. 14289, de 02 de janeiro de 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/L14289.htm#:~:text=L14289&text=Torna%20obrigat%C3%B3ria%20a%20preserva%C3%A7%C3%A3o%20do,30%20de%20outubro%20de%201975.. Acesso em: 15 nov. 2023.

BUBLITZ, Jan-Christoph. Privacy Concerns in Brain–Computer Interfaces. **AJOB Neuroscience**, v. 10, n. 1, 2019. Disponível em: https://doi.org/10.1080/21507740.2019.1595783. Acesso em: 11 nov. 2023.

BUBLITZ, Jan-Christoph. What an International Declaration on Neurotechnologies and Human Rights Could Look like: Ideas, Suggestions, Desiderata. **AJOB Neuroscience**, 2023. Disponível em: 10.1080/21507740.2023.2270512. Acesso em: 6 fev. 2024.

BUBLITZ, Jan-Christoph; HILDT, Elisabeth; FRANCKE, Andreas . My mind is mine!? Cognitive liberty as a legal concept. **Cognitive enhancement**, v. 1, 2013. Trends in Augmentation of Human Performance. Disponível em: https://doi.org/10.1007/978-94-007-6253-4_19. Acesso em: 11 nov. 2023.

BULL, Hans Peter. **Informationelle Selbstbestimmung - Vision oder Illusion?**: Datenschutz im Spannungsverhältnis von Freiheit und Sicherheit. 2 ed. Mohr Siebeck, 2011.

BUOLAMWINI, Joy; GEBRU, Timnit. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. **Proceedings of Machine Learning Research**, v. 81, 2018. Disponível em: https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf. Acesso em: 12 nov. 2023.

CACHAPUZ, Maria Claudia Mercio. Transparência e Informação: entre o público e o privado. **Revista Eletrônica do TCE-RS**, 2019. Edicão Especial, 30 Anos da Constituição Estadual.. Disponível em: http://www.bibliotecadigital.ufrgs.br/da.php?nrb=001097778&loc=2019&l=ad3480966dee6bcc. Acesso em: 12 nov. 2023.

CACHAPUZ, Maria Claudia Mercio. Tratamento à informação, dados nominativos e a interpretação possível à lei de acesso à informação*. In:* ANDRADE, Francisco António Carneiro Pacheco de (Coord.); CELLA, José Renato Gaziero (Coord.); FREITAS, Pedro Miguel Fernandes (Coord.). **Direito, governança e novas tecnologias**: VII Encontro Internacional do CONPEDI. Florianópolis, 2017. Disponível em: http://www.bibliotecadigital.ufrgs.br/da.php?nrb=001059285&loc=2019&l=f274930a0be5478e. Acesso em: 12 nov. 2023.

CADWALLADR, Carole; GRAHAM-HARRISON, Emma. **Cambridge Analytica and Facebook**: The Scandal and the Fallout So Far. The Guardian. 2018. Disponível em: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. Acesso em: 27 nov. 2023.

CARDOSO, Oscar Valente. A proteção dos dados pessoais sensíveis em situações não discriminatórias. **Revista de Direito e as Novas Tecnologias**, São Paulo, v. 13, out./dez. 2021.

CARRUTHERS, Peter . **The Architecture of the Mind**. 1 ed. Clarendon Press, 2006.

CATTAN, Grégoire. The Use of Brain–Computer Interfaces in Games Is Not Ready for the General Public. **Frontiers in Computer Science**, v. 3, 24 mar. 2021. Sec. Human-Media Interaction. Disponível em: https://doi.org/10.3389/fcomp.2021.628773. Acesso em: 11 nov. 2023.

CHAKRABORTY, Chiranjib. **Brain-Computer Interface**: Banking, Finance & Emotional. Linkedin. 2021. Disponível em: https://www.linkedin.com/pulse/brain-computer-interface-banking-finance-emotional-chakraborty. Acesso em: 31 jan. 2024.

CHIESA, Patricia Andrea *et al*. Brain activity induced by implicit processing of others' pain and pleasure. **Human Brain Mapping**, v. 38, n. 11, nov. 2017. Disponível em: 10.1002/hbm.23749. Acesso em: 11 nov. 2023.

CHILE. Senado. Proyecto de Ley: Sobre protección de los neuroderechos y la integridad mental, y el desarrollo de la investigación y las neurotecnologías n. 13828-19, ano 2020.

CHOI, Hanbyul; PARK, Jonghwa; JUNG, Yoonhyuk. The role of privacy fatigue in online privacy behavior. **Computers in Human Behavior**, v. 81, abr. 2018. Disponível em: https://doi.org/10.1016/j.chb.2017.12.001. Acesso em: 25 jan. 2024.

CINEL, Caterina; VALERIANI, Davide; POLI, Riccardo. Neurotechnologies for Human Cognitive Augmentation: Current State of the Art and Future Prospects. **Frontiers in Human Neuroscience**, v. 13, 2019. Sec. Cognitive Neuroscience. Disponível em: https://doi.org/10.3389/fnhum.2019.00013. Acesso em: 15 nov. 2023.

CLARK, Andy; CHALMERS, David . The Extended Mind. **Analysis**, v. 58, n. 1, jan. 1998. Disponível em: https://www.jstor.org/stable/i366412. Acesso em: 15 nov. 2023.

CNSEG - Confederação Nacional das Seguradoras. **Guia de boas práticas do mercado segurador brasileiro sobre a proteção de dados**. Disponível em: https://cnseg.org.br/publicacoes/guia-de-boas-praticas-do-mercado-segurador-brasileiro-sobre-a-protecao-de-dados-pessoais.html. Acesso em: 25 jan. 2024.

COLUSSI, Fernando Augusto Melo; SANTOS, Tomlyta Luz Velasquez dos. Novas tecnologias e liberdade de expressão na pesquisa científica: uma análise sobre a proteção de dados genéticos e de saúde. **Revista de Biodireito e Direito dos Animais**, Porto Alegre, v. 4, n. 2, jul./dez. 2018.

CORRÊA, Adriana Espíndola. O corpo digitalizado: um novo objeto para o direito. **Revista da Faculdade de Direito (UFPR)**, v. 44, 2006.

COULTER, Martin; SANDLE, Paul. **AI summit a start but global agreement a distant hope**. Reuters. 2023. Disponível em: https://www.reuters.com/technology/ai-summit-start-global-agreement-distant-hope-2023-11-03/. Acesso em: 27 nov. 2023.

COX, David D; SAVOY, Robert L. Functional magnetic resonance imaging (fMRI) “brain reading”: detecting and classifying distributed patterns of fMRI activity in human visual cortex. **NeuroImage**, v. 19, n. 2, jun. 2003. Disponível em: https://doi.org/10.1016/S1053-8119%2803%2900049-1. Acesso em: 13 nov. 2023.

CRANE, Leah. **Elon Musk demonstrated a Neuralink brain implant in a live pig**. New Scientist. 2020. Disponível em: https://www.newscientist.com/article/2253274-elon-musk-demonstrated-a-neuralink-brain-implant-in-a-live-pig/. Acesso em: 11 nov. 2023.

CRAVER , Carl F. **Explaining the Brain**: Mechanisms and the Mosaic Unity of Neuroscience. 1 ed. Oxford University Press, 2009.

DANKS, David; LONDON, Alex John. Algorithmic Bias in Autonomous Systems. **Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence**, 2017. AI and autonomy track. Disponível em: https://doi.org/10.24963/ijcai.2017/654. Acesso em: 13 fev. 2024.

DEUTSCHE WELLE. **A prótese controlada pelo pensamento**. 2021. Disponível em: https://www.dw.com/pt-br/a-pr%C3%B3tese-controlada-pelo-pensamento/a-57108721. Acesso em: 11 nov. 2023.

DOERING, Victor *et al*. **O tratamento de dados biométricos na LGPD: dilemas jurídicos e políticos de seu processamento**: Direito público digital. São Paulo: Thomson Reuters Brasil, 2020.

DONEDA, Danilo. **A proteção de dados pessoais nas relações de consumo**: para além da informação credíticia . Brasília: SDE/DPDC, 2010. Disponível em: https://www.vidaedinheiro.gov.br/wp-content/uploads/2017/04/SENACON_Caderno_ProtecaoDadosPessoais.pdf. Acesso em: 15 dez. 2023.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 3 ed. São Paulo: Thomson Reuters, 2021.

DONEDA, Danilo; MENDES, Laura Schertel. Marco jurídico para a cidadania digital: uma análise do projeto de lei 5276/2016. **Revista de Direito Civil Contemporâneo**, v. 9, 2016.

DONEDA, Danilo; MONTEIRO, Marília. **Acesso à informação e privacidade no caso da Universidade Federal de Santa Maria**. Jota. 2015. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/acesso-a-informacao-e-privacidade-no-caso-da-universidade-federal-de-santa-maria-02072015. Acesso em: 5 fev. 2024.

DORFMAN, Peter. **2 Heads—and a Brain-Computer Interface—Are Making Waves in the Art World**. Autodesk. 2018. Disponível em: https://www.autodesk.com/design-make/articles/brain-computer-interface. Acesso em: 18 nov. 2023.

EIGELSON, Bruno (Coord.); BECKER, Daniel (Coord.). **Comentários à Lei Geral de Proteção de Dados**: Lei 13.709/2018. São Paulo: Revista dos Tribunais, 2020.

EMOTIV. **Insight**. 2023. Disponível em: https://www.emotiv.com/insight. Acesso em: 6 fev. 2024.

EMOTIV. **Rac Mind Over Motor**. 2023. Disponível em: https://www.emotiv.com/news/rac-mind-over-motor/. Acesso em: 18 nov. 2023.

ESTADOS UNIDOS. FDA - Food and Drug Administration. Regulatory Overview of Neurological Devices, de 03 de agosto de 2021. Disponível em: https://www.fda.gov/medical-devices/neurological-devices/regulatory-overview-neurological-devices. Acesso em: 31 jan. 2024.

EUROPA. EDPD - European Data Proction Board. Diretrizes relativas ao consentimento na acepção do Regulamento 2016/679 n. 05/2020, de 03 de maio de 2020. Disponível em: https://edpb.europa.eu/our-worktools/our-documents/guidelines/guidelines-052020-consent-under-regulation2016679_en. Acesso em: 25 jan. 2024.

EUROPA. Parlamento Europeu. Diretriz relativa ao exercício dos direitos dos doentes em matéria de cuidados de saúde transfronteiriços n. 2011/24/UE, 09 de março de 2011. Disponível em: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:088:0045:0065:pt:PDF. Acesso em: 15 jan. 2024.

EUROPA. Parlamento Europeu. General Data Protection Regulation (GDPR). Regulamento (UE) n. 2016/679, de 26 de abril de 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 11 nov. 2023.

EXAME. **Implante cerebral para restaurar memória é desenvolvido**. 2014. Disponível em: https://exame.com/ciencia/implante-cerebral-para-restaurar-memoria-e-desenvolvido. Acesso em: 20 nov. 2023.

FARAHANY , Nita A. **The Battle for Your Brain**: Defending the Right to Think Freely in the Age of Neurotechnology. St. Martin's Press, 2023.

FODOR, Jerry A. **The Modularity of Mind**: Essay on Faculty Psychology. MIT Press, 1983.

FRANCK, Georg. The economy of attention. **Journal of Sociology**, v. 55, n. 1, mar. 2019. Disponível em: https://journals.sagepub.com/doi/full/10.1177/1440783318811778. Acesso em: 9 jan. 2024.

FUKUYAMA, Fracis. **Our Posthuman Future**: Consequences of the Biotechnology Revolution. Profile Books, 2003.

GOERING, Sara ; YUSTE, Rafael. On the Necessity of Ethical Guidelines for Novel Neurotechnologies. **Cell**, v. 167, n. 4, 03 nov. 2016. Disponível em: https://doi.org/10.1016/j.cell.2016.10.029. Acesso em: 13 nov. 2023.

GOERING, Sara *et al*. Recommendations for Responsible Development and Application of Neurotechnologies. **Neuroethics**, v. 14, 29 abr. 2021. Disponível em: https://link.springer.com/article/10.1007/s12152-021-09468-6. Acesso em: 11 nov. 2023.

GOERING, Sara; KLEIN, Eran. **The Oxford Handbook of Philosophy and Disability**: Neurotechnologies and Justice by, with, and for Disabled People. Oxford University Press, 2019. Disponível em: http://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780190622879.001.0001/oxfordhb-9780190622879-e-33. Acesso em: 15 nov. 2023.

GOLDHABER, Michael H. The attention economy and the Net. **First Monday**, v. 2, n. 4, 07 abr. 1997. Disponível em: https://firstmonday.org/ojs/index.php/fm/article/view/519. Acesso em: 9 jan. 2024.

GOMES, Orlando. Direitos da personalidade e responsabilidade civil. **Revista de direito comparado luso-brasileiro**, Rio de Janeiro, v. 2, 1983.

GRANDCHAMP, Romain; DELORME, Arnaud. The Brainarium: An Interactive Immersive Tool for Brain Education, Art, and Neurotherapy. **Computational Intelligence and Neuroscience**, 06 set. 2016. Disponível em: https://pubmed.ncbi.nlm.nih.gov/27698660/. Acesso em: 11 nov. 2023.

GREELY, Henry T. Mind Reading*. In:* MORSE, Stephen J; ROSKIES, Adina L. **A Primer on Criminal Law and Neuroscience**: A contribution of the Law and Neuroscience Project, supported by the MacArthur Foundation. Nova Iorque: Oxford University Press, 2013.

GUIDI, Guilherme. **Modelos regulatórios para proteção de dados pessoais**. 2017. Disponível em: https://itsrio.org/wp-content/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf. Acesso em: 13 jan. 2024.

GUO, Christine. **Why Wearable DHTs are Bringing More Meaningful Data Collection to Patient-Centric Clinical Trials**. Applied Clinical Trials. 2023. Disponível em: https://www.appliedclinicaltrialsonline.com/view/why-wearable-dhts-are-bringing-more-meaningful-data-collection-to-patient-centric-clinical-trials. Acesso em: 31 jan. 2024.

GUPTA, Ankur; VARDALAKIS, Nikolaos; WAGNER, Fabien B. Neuroprosthetics: from sensorimotor to cognitive disorders. **Communications Biology**, v. 6, n. 1, 06 jan. 2023. Disponível em: https://pubmed.ncbi.nlm.nih.gov/36609559/. Acesso em: 11 nov. 2023.

GUSMÃO, André Simoni e. **Sobre a taxatividade do rol de dados pessoais sensíveis**. Consultor Jurídico. 2024. Disponível em: https://www.conjur.com.br/2024-jan-13/sobre-a-taxatividade-do-rol-de-dados-pessoais-sensiveis/. Acesso em: 5 fev. 2024.

GUZMÁN, Lorena. **Chile**: Pioneering the protection of neurorights. UNESCO. 2022. Disponível em: https://en.unesco.org/courier/2022-1/chile-pioneering-protection-neurorights. Acesso em: 20 nov. 2023.

HARARI, Yuval Noah. **21 lições para o século 21**. 1 ed. Companhia das Letras, 2018.

HARAWAY, Donna. A Cyborg Manifesto: Science, Technology, and Socialist Feminism in the Late Twentieth Century*. In:* HARAWAY, Donna. **Simians, Cyborgs, and Women**: The Reinvention of Nature. 1 ed. Routledge, 1990.

HARRIS, Sam. **Free Will**. 1 ed. Free Press, 2012.

HAYLES, N. Katherine. **How We Became Posthuman**: Virtual Bodies in Cybernetics, Literature, and Informatics. 1 ed. University of Chicago Press Journals, 1999.

HE, Jia; VAN DE VIJVER, Fos. **Bias and Equivalence in Cross-Cultural Research**. 2012. Disponível em: https://scholarworks.gvsu.edu/orpc/vol2/iss2/8/. Acesso em: 12 nov. 2023.

HORNUNG, Gerrit; SCHNABEL, Christoph. Data protection in Germany I:: The population census decision and the right to informational self-determination. **Computer Law & Security Review**, v. 25, n. 1, 2009. Disponível em: https://doi.org/10.1016/j.clsr.2008.11.002. Acesso em: 13 nov. 2023.

ICO - Information Commissioner's Office. **What are the conditions for processing?**. 2023. Disponível em: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/criminal-offence-data/what-are-the-conditions-for-processing/. Acesso em: 25 jan. 2024.

IDEC - Instituto Brasileiro de Defesa do Consumidor. **Idec vai à Justiça contra coleta de dados de emoções de passageiros em linha do metrô de São Paulo**. 2018. Disponível em: https://idec.org.br/release/idec-vai-justica-contra-coleta-de-dados-de-emocoes-de-passageiros-em-linha-do-metro-de-sao. Acesso em: 15 jan. 2024.

IENCA, Marcello; ANDORNO, Roberto. Towards new human rights in the age of neuroscience and neurotechnology. **Life Sciences, Society and Policy**, v. 13, 2017. Disponível em: https://doi.org/10.1186/s40504-017-0050-1. Acesso em: 12 nov. 2023.

IENCA, Marcello; HASELAGER, Pim. Hacking the brain: brain–computer interfacing technology and the ethics of neurosecurity. **Ethics and Information Technology**, v.

18, 2016. Disponível em: https://link.springer.com/article/10.1007/s10676-016-9398-9. Acesso em: 12 nov. 2023.

IENCA, Marcello; JOTTERAND, Fabrice; ELGER, Bernice S. From Healthcare to Warfare and Reverse: How Should We Regulate Dual-Use Neurotechnology?. **Neuron**, v. 97, n. 2, 17 jan. 2018. Disponível em: 10.1016/j.neuron.2017.12.017. Acesso em: 12 nov. 2023.

INCEPTION. Christopher Nolan. Emma Thomas e Cristopher Nolan. EUA/Reino Unido: Warner Bros. Pictures, 2010 (148min).

IWRY, Jonathan; YADEN, David B; NEWBERG, Andrew B. Noninvasive Brain Stimulation and Personal Identity: Ethical Considerations. **Frontiers in Human Neuroscience**, v. 11, n. 281, 07 jun. 2017. Disponível em: https://pubmed.ncbi.nlm.nih.gov/28638327/. Acesso em: 18 nov. 2023.

IZMAILOVA, Elena S; WAGNER, John A; PERAKSLIS, Eric D. Wearable Devices in Clinical Trials: Hype and Hypothesis. **Clinical Pharmacology & Therapeutics**, jul. 2018. Disponível em: https://pubmed.ncbi.nlm.nih.gov/29205294/. Acesso em: 31 jan. 2024.

JOAN is Awful In: Black Mirror. Ally Pankiw. Charlie Brooker. Reino Unido: Netflix, 2023 (56min).

JWA, Anita S; POLDRACK, Russell A. Addressing privacy risk in neuroscience data: from data protection to harm prevention. **Journal of Law and the Biosciences**, v. 9, n. 2, jul./dez. 2022. Disponível em: https://doi.org/10.1093/jlb/lsac025. Acesso em: 31 jan. 2024.

KANE, Robert. **The Oxford Handbook of Free Will**. 2 ed. Oxford University Press, 2011.

KANG, Jiawen *et al*. Reliable Federated Learning for Mobile Networks. **IEEE Wireless Communications**, v. 27, n. 2, abr. 2020. Disponível em: https://ieeexplore.ieee.org/document/8994206. Acesso em: 13 nov. 2023.

KAVOLIŪNAITĖ-RAGAUSKIENĖ, Eglė. Right to Privacy and Data Protection Concerns Raised by the Development and Usage of Face Recognition Technologies in the European Union. **Journal of Human Rights Practice**, 11 jan. 2024. Disponível em: https://doi.org/10.1093/jhuman/huad065. Acesso em: 15 jan. 2024.

KHALSA, Sahib S; LAPIDUS, Rachel C. Can Interoception Improve the Pragmatic Search for Biomarkers in Psychiatry?. **Frontiers in Psychiatry**, v. 7, n. 121, 25 jul. 2016. Disponível em: 10.3389/fpsyt.2016.00121. Acesso em: 15 nov. 2023.

KHEDR, Alhassan; GULAK, Glenn. SecureMed: Secure Medical Computation Using GPU-Accelerated Homomorphic Encryption Scheme. **IEEE Journal of Biomedical and Health Informatics**, v. 22, n. 2, mar. 2018. Disponível em: 10.1109/JBHI.2017.2657458. Acesso em: 13 nov. 2023.

KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. **Dados Sensíveis na Lei Geral de Proteção de Dados Pessoais**: mecanismos de tutela para o livre desenvolvimento da personalidade Dissertação (Mestrado em Direito) - Universidade Federal de Juiz de Fora, Juiz de Fora, 2019. Disponível em: https://bit.ly/3kHzLxS. Acesso em: 5 fev. 2024.

KOTSCHY, Waltraut. Article 6 Lawfulness of processing. *In:* KUNER, Christopher *et al*. **The EU General Data Protection Regulation (GDPR)**: A Commentary. Oxford University Press, 2020. Disponível em: https://academic.oup.com/book/41324. Acesso em: 25 jan. 2024.

KRELL, Jason; DOLECKI, Patrick K; TODD, Anderson. School-Based Neurofeedback Training for Sustained Attention. **Journal of Attention Disorders**, v. 27, n. 10, 25 abr. 2023. Disponível em: https://doi.org/10.1177/10870547231168430. Acesso em: 31 jan. 2024.

KRUTZINNA, Jenny; TADDEO, Mariarosaria; FLORIDI, Luciano. Enabling Posthumous Medical Data Donation: A Plea for the Ethical Utilisation of Personal Health Data. *In:* KRUTZINNA, Jenny; FLORIDI, Luciano. **The Ethics of Medical Data Donation**. Springer, 2019. cap. 11. Disponível em: 10.1007/978-3-030-04363-6_11. Acesso em: 13 nov. 2023.

LAURIE, Graeme *et al*. Managing Access to Biobanks: How Can We Reconcile Individual Privacy and Public Interests in Genetic Research?. **Medical Law International**, v. 10, n. 4, 12 fev. 2017. Disponível em: https://doi.org/10.1177/096853321001000404. Acesso em: 15 nov. 2023.

LAVAZZA, Andrea. Freedom of Thought and Mental Integrity: The Moral Requirements for Any Neural Prosthesis. **Frontiers in Neuroscience**, v. 12, n. 82, 19 fev. 2018. Disponível em: 10.3389/fnins.2018.00082. Acesso em: 11 nov. 2023.

LEO, Ben. **Motorists fork out £1,000 more to insure their cars if their name is Mohammed**. The Sun. 2018. Disponível em: https://www.thesun.co.uk/motors/5393978/insurance-race-row-john-mohammed/. Acesso em: 5 fev. 2024.

LEONARDI, Marcel. Principais bases legais de tratamento de dados pessoais no setor privado. *In:* SOUZA, Carlos Affonso Pereira de (Coord.); MAGRANI, Eduardo (Coord.); SILVA, Priscilla (Coord.). **Caderno especial**: Lei geral

de produção de dados (LGPD). São Paulo: Revista dos Tribunais, 2019. Disponível em: https://bibliotecadigital.tse.jus.br/xmlui/handle/bdtse/6380. Acesso em: 13 nov. 2023.

LIBET, Benjamin *et al*. Time of conscious intention to act in relation to onset of cerebral activity (readiness-potential): the unconscious initiation of a freely voluntary act. **Brain**, v. 106, n. 3, 11 set. 1983. Disponível em: https://doi.org/10.1093/brain/106.3.623. Acesso em: 15 nov. 2023.

LIGTHART, Sjors *et al*. Minding Rights: Mapping Ethical and Legal Foundations of 'Neurorights'. **Cambridge Quarterly of Healthcare Ethics**, v. 1, n. 21, 15 mai 2023. Disponível em: 10.1017/S0963180123000245. Acesso em: 15 nov. 2023.

LIU, Yizhi; HABIBNEZHAD, Mahmoud; JEBELLI, Houtan. Brain-computer interface for hands-free teleoperation of construction robots. **Automation in Construction**, v. 123, mar. 2021. Disponível em: https://doi.org/10.1016/j.autcon.2020.103523. Acesso em: 11 nov. 2023.

LOPES, Laís de Figueirêdo; MARGONARI, Carolina Elisa; COSTA, Vinicius Fidelis. **Dados de pessoas com deficiência são dados pessoais sensíveis?**. Migalhas. 2023. Disponível em: https://www.migalhas.com.br/depeso/380682/dados-de-pessoas-com-deficiencia-sao-dados-pessoais-sensiveis. Acesso em: 13 jan. 2024.

LÓPEZ-SILVA, Pablo; MADRID, Raúl . Sobre la conveniencia de incluir los neuroderechos en la Constitución o en la ley. **Revista Chilena de Derecho y Tecnología**, v. 10, n. 1, Primer semestre 2021. Disponível em: https://doi.org/10.5354/0719-2584.2021.56317. Acesso em: 12 nov. 2023.

MACKENZIE, Catriona; WALKER, Mary. Neurotechnologies, Personal Identity, and the Ethics of Authenticity*. In:* CLAUSEN, Jens; LEVY, Neil. **Handbook of Neuroethics**. Springer, 2015. Disponível em: https://link.springer.com/referencework/10.1007/978-94-007-4707-4. Acesso em: 11 nov. 2023.

MARCULINO, Karoline Silveira. **Vulnerabilidade do titular de dados pessoais e a responsabilidade dos agentes de tratamento** Trabalho de Conclusão de Curso (Direito) - Universidade Federal do Rio Grande do Sul, Porto Alegre, 2021. Disponível em: https://lume.ufrgs.br/handle/10183/237640. Acesso em: 11 nov. 2023.

MARINA, Nephtali *et al*. Brain metabolic sensing and metabolic signaling at the level of an astrocyte. **Glia**, jun. 2018. Disponível em: 10.1002/glia.23283. Acesso em: 15 nov. 2023.

MASSAI, Leonardo. **Dealing with "Consensus" at the UN Climate Talks**. Climalia. 2019. Disponível em: http://www.climalia.eu/dealing-consensus-un-climate-talks/. Acesso em: 27 nov. 2023.

MCKENNA, Michael; PEREBOOM, Derk. **Free Will**: A Contemporary Introduction. 1 ed. Routledge, 2016.

MCTI - Ministério da Ciência, Tecnologia, Inovações e Comunicações. **Estratégia Brasileira para a Transformação Digital**. Brasília, 2018. Disponível em: https://www.gov.br/mcti/pt-br/centrais-de-conteudo/comunicados-mcti/estrategia-digital-brasileira/estrategiadigital.pdf. Acesso em: 13 jan. 2024.

MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. **Pensar**, Fortaleza, v. 25, n. 4, out./dez. 2020. Disponível em: https://doi.org/10.5020/2317-2150.2020.10828. Acesso em: 11 nov. 2023.

MENDES, Laura Schertel; DONEDA, Danilo. Comentário à Nova Lei de Proteção de Dados (Lei 13.709/2018): O Novo Paradigma da Proteção de Dados. **Revista de Direito do Consumidor**, v. 110, 2018.

MENDES, Luciana A *et al*. Motor neuroprosthesis for promoting recovery of function after stroke. **Cochrane Database of Systematic Reviews**, 14 jan. 2020. Disponível em: 10.1002/14651858.CD012991.pub2. Acesso em: 11 nov. 2023.

MENKE, Fabiano. **A possibilidade de cumulação de bases legais nas operações de tratamento de dados pessoais**. Menke Advogados. 2021. Disponível em: https://menkeadvogados.com.br/wp-content/uploads/2021/02/artigo_Menke_bases_legais.pdf. Acesso em: 3 fev. 2024.

MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão*. In:* MENDES, Gilmar Ferreira (Coord.); SARLET, Ingo Wolfgang (Coord.); COELHO, Alexandre Zavaglia P (Coord.). **Direito, inovação e tecnologia**. São Paulo: Saraiva, 2015. Disponível em: https://www.cidp.pt/revistas/rjlb/2019/1/2019_01_0781_0809.pdf. Acesso em: 13 nov. 2023.

MENKE, Fabiano. **As origens alemãs e o significado da autodeterminação informativa**. Migalhas. 2020. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/335735/as-origens-alemas-e-o-significado-da-autodeterminacao-informativa. Acesso em: 13 nov. 2023.

MILKOWSKI, Marcin. **Explaining the Computational Mind**. MIT Press, 2013.

MIRAGEM, Bruno; PETERSEN, Luiza. O contrato de seguro e a lei geral de proteção de dados. **Revista dos Tribunais**, n. 1018, ago. 2020.

MIRANDA, Felipe Arady. O direito fundamental ao livre desenvolvimento da personalidade. **Revista do Instituto do Direito Brasileiro**, v. 10, 2013.

MOLINARO, Carlos Alberto; SARLET, Gabrielle Bezerra Sales. Questões tecnológicas, éticas e normativas da proteção de dados pessoais na área da saúde em um contexto de big data. **Direitos Fundamentais & Justiça**, v. 13, n. 41, 2019. Disponível em: https://doi.org/10.30899/dfj.v13i41.811. Acesso em: 12 nov. 2023.

MONTGOMERY, Jonathan. Data Sharing and the Idea of Ownership. **The New Bioethics**, v. 23, n. 1, abr. 2017. Disponível em: 10.1080/20502877.2017.1314893. Acesso em: 11 nov. 2023.

MORAES, Maria Celina Bodin de. **A tutela da pessoa humana no Brasil**. Civilistica. 2014. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/175. Acesso em: 15 dez. 2023.

MORAES, Maria Celina Bodin de. **Na Medida Da Pessoa Humana**: Estudos de Direito Civil-Constitucional. 1 ed. Rio de Janeiro: Processo, 2019.

MORAES, Maria Celina Bodin de; CASTRO, Thamis Dalsenter . **A autonomia existencial nos atos de disposição do próprio corpo**. 2014. Disponível em: https://ojs.unifor.br/rpen/article/download/3433/pdf_1/11176#:~:text=A%20autodetermina%C3%A7%C3%A3o%20corporal%20%C3%A9%20uma,%E2%80%9D%2C%20compat%C3%ADvel%20com%20a%20Constitui%C3%A7%C3%A3o.. Acesso em: 15 dez. 2023.

MOREIRA, Rodrigo Pereira. **Direito ao Livre Desenvolvimento da Personalidade**: Proteção e Promoção da Pessoa Humana. Curitiba: Juruá, 2016.

MULHOLLAND, Caitlin. **Dados pessoais sensíveis e consentimento na Lei Geral de Proteção de Dados Pessoais**. Migalhas. 2020. Disponível em: https://migalhas.uol.com.br/coluna/migalhas-devulnerabilidade/329261/dados-pessoais-sensiveis-e-consentimento-na-lei-geralde-protecao-de-dados-pessoais. Acesso em: 9 jan. 2024.

MULHOLLAND, Caitlin. O tratamento de dados pessoais sensíveis. *In:* MULHOLLAND, Caitlin (Org.). **LGPD e o novo marco normativo no Brasil**. Porto Alegre: Arquipélago, 2020.

MULHOLLAND, Caitlin. Os contratos de seguro e a proteção dos dados pessoais sensíveis*. In:* GOLDBERG, Ilan (Coord.); JUNQUEIRA, Thiago (Coord.). **Temas Atuais de Direito dos Seguros**: Tomo I. São Paulo: Thomson Reuters, 2020.

MUSK, Elon. **The first human received an implant from @Neuralink yesterday and is recovering well. Initial results show promising neuron spike detection**. Twitter: @elonmusk. 2024. Disponível em: https://twitter.com/elonmusk/status/1752098683024220632. Acesso em: 31 jan. 2024.

MUÑOZ, José M. Chile - right to free will needs definition. **Nature**, v. 574, n. 7780, Out. 2019. Disponível em: 10.1038/d41586-019-03295-9. Acesso em: 11 nov. 2023.

MUÑOZ, José Manuel. Hacia una sistematización de la relación entre determinismo y libertad. **Daimon: revista internacional de filosofía**, n. 56, 2012. Disponível em: https://revistas.um.es/daimon/article/view/141761. Acesso em: 11 nov. 2023.

NATURE. **Why the UK-led global AI summit is missing the point**. 2023. Disponível em: https://www.nature.com/articles/d41586-023-03333-7. Acesso em: 27 nov. 2023.

NEGRI, Sérgio Marcos Carvalho de Ávila; KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. A normatividade dos dados sensíveis na Lei Geral de Proteção de dados: ampliação conceitual e proteção da pessoa humana. **Revista de Direito, Governança e Novas Tecnologias**, Goiânia, v. 5, n. 1, 2019. Disponível em: http://dx.doi.org/10.26668/IndexLawJournals/2526-0049/2019.v5i1.5479. Acesso em: 12 nov. 2023.

NERY JUNIOR, Nelson. Questões de Ordem Pública e Seu Julgamento Ex Officio: Considerações sobre o verbete 'STJ 381' da Súmula da jurisprudência predominante no STJ. **Revista de Direito Privado**, v. 60, 2014.

NEURAL EXPERIENCE. **Check Out The Companies Using Neuromarketing to Boost Sales**. 2021. Disponível em: https://www.neuralexperience.io/what-companies-use-neuromarketing. Acesso em: 18 nov. 2023.

NEURALINK. **First Clinical Trial Open For Recruitment**. 2023. Disponível em: https://neuralink.com/blog/first-clinical-trial-open-for-recruitment/. Acesso em: 18 nov. 2023.

NEUROPACE. **NeuroPace Privacy Statement**. 2023. Disponível em: https://www.neuropace.com/privacy/. Acesso em: 31 jan. 2024.

NEWMAN, Ehren L *et al*. Revealing the Dynamics of Neural Information Processing with Multivariate Information Decomposition. **Entropy**, v. 24, n. 7, 05 jul. 2022. Disponível em: 10.3390/e24070930. Acesso em: 5 fev. 2024.

NICOLELIS, Miguel A L; LEBEDEV, Mikhail A. Principles of neural ensemble physiology underlying the operation of brain-machine interfaces. **Nature Reviews Neuroscience**, v. 10, n. 7, 2009. Disponível em: 10.1038/nrn2653. Acesso em: 11 nov. 2023.

NOWAK, Michael; ECKLES, Dean. **Determining user personality characteristics from social networking system communications and characteristics**. United States Patent US8825764B2. 2014. Disponível em: https://patents.google.com/patent/US8825764B2/en. Acesso em: 27 nov. 2023.

O'CONNOR, Timothy; FRANKLIN, Cristopher. **Free will**. Stanford Encyclopedia Of Philosophy. 2020. Disponível em: https://plato.stanford.edu/entries/freewill/. Acesso em: 27 nov. 2023.

O'NEIL , Cathy. **Weapons of Math Destruction**: How Big Data Increases Inequality and Threatens Democracy. 1 ed. Crown, 2016.

OLSON, S. **International Summit on Human Gene Editing**: A Global Discussion. National Library of Medicine. 2015. Disponível em: https://www.ncbi.nlm.nih.gov/books/NBK343651/. Acesso em: 21 nov. 2023.

O'BROLCHÁIN, Fiachra; GORDIJN , Bert. Ethics of Brain–Computer Interfaces for Enhancement Purposes*. In:* CLAUSEN, Jens; LEVY, Neil. **Handbook of Neuroethics**. Springer, 2015. Disponível em: https://link.springer.com/referencework/10.1007/978-94-007-4707-4. Acesso em: 12 nov. 2023.

PALHARES, Felipe; PRADO, Luis Fernando; VIDIGAL, Paulo Oliveira Piedade. **Compliance Digital e LGPD**: volume 5. Revista dos Tribunais, 2021.

PASQUALE, Frank. **The Black Box Society**: The Secret Algorithms That Control Money and Information. Harvard University Press, 2016.

PAZ, Abel Wajnerman. Is Your Neural Data Part of Your Mind?: Exploring the Conceptual Basis of Mental Privacy. **Minds and Machines**, v. 32, 2022. Disponível em: https://doi.org/10.1007/s11023-021-09574-7. Acesso em: 11 nov. 2023.

PEPPERELL, Julian. **The Posthuman Condition**: Consciousness Beyond the Brain. Intellect Ltd, 2009.

PEREBOOM, Derk. **Living Without Free Will**. Cambridge University Press, 2001.

PERLINGIERI, Pietro; CICCO, Maria Cristina de (Org.). **O Direito Civil na Legalidade Constitucional**. 1 ed. Renovar, 2008.

PEÑA, Paz; VARON, Joana. **O poder de dizer NÃO na Internet**. Coding Rights. 2019. Disponível em: https://medium.com/codingrights/o-poder-de-dizer-nãona-internet-17d6e9889d4a. Acesso em: 25 jan. 2024.

PICCININI, Gualtiero. **Physical Computation**: A Mechanistic Account. Oxford University Press, 2015.

PICCININI, Gualtiero; BAHAR, Sonya. Neural computation and the computational theory of cognition. **Cognitive Science**, v. 37, n. 3, abr. 2013. Disponível em: 10.1111/cogs.12012. Acesso em: 12 nov. 2023.

PINHEIRO, Iuri; BOMFIM, Vólia. Aspectos gerais da lei geral de proteção de dados e seus impactos nas relações de trabalho*. In:* SILVA, Fabrício Lima (Org.); PINHEIRO, Iuri (Coord.); BOMFIM, Vólia (Coord.). **LGPD nas Relações de Trabalho**. Venturoli, 2020.

PINTO, Paulo Mota. Notas sobre o direito ao livre desenvolvimento da personalidade e os direitos da personalidade no direito português*. In:* SARLET, Ingo Wolfgang (Org.). **A Constituição concretizada**: construindo pontes com o público e o privado. Porto Alegre: Livraria do Advogado, 2000.

PLATÃO. **A República — Platão**: Introdução, tradução e notas de Maria Helena da Rocha Pereira. Lisboa: Fundação Calouste Gulbenkian, 1972.

PUTNAM, Hilary. Psychological predicates*. In:* CAPITAN, W. H.; MERRILL, D. D. **Art, Mind, and Religion**. University of Pittsburgh Press, 1967.

PYLYSHYN, Zenon W. Cognitive architecture*. In:* CRAIG, Edward. **Routledge Encyclopedia of Philosophy Online**. Routledge , 1998. Disponível em: https://www.rep.routledge.com/. Acesso em: 11 nov. 2023.

QUINN, Paul; MALGIERI, Gianclaudio. The Difficulty of Defining Sensitive Data: The Concept of Sensitive Data in the EU Data Protection Framework. **German Law Journal**, 16 nov. 2020. Disponível em: https://dx.doi.org/10.2139/ssrn.3713134. Acesso em: 15 jan. 2024.

RACINE, Eric; VAN DER LOOS, H Z Adriaan; ILLES, Judy. Internet marketing of neuroproducts: new practices and healthcare policy challenges. **Cambridge**

Quarterly of Healthcare Ethics, v. 16, n. 2, 2007. Disponível em: 10.1017/s096318010707020x. Acesso em: 13 nov. 2023.

RAMÍREZ-MORENO, Mauricio A. *et al*. EEG-Based Tool for Prediction of University Students' Cognitive Performance in the Classroom. **Brain Sciences**, v. 11, n. 6, 26 mai. 2021. Disponível em: https://doi.org/10.3390/brainsci11060698. Acesso em: 11 nov. 2023.

RAO, Dattaraj Jagdish; MANE, Shraddha. **Digital Twin approach to Clinical DSS with Explainable AI**. 2019. Disponível em: https://doi.org/10.48550/arXiv.1910.13520. Acesso em: 15 jan. 2024.

REINER, Peter Bart; NAGEL, Saskia. Technologies of the Extended Mind: Defining the Issues*. In:* ILLES, Judy. **Neuroethics**: Anticipating the future. Oxford University Press, 2017. Disponível em: https://doi.org/10.1093/oso/9780198786832.001.0001. Acesso em: 13 nov. 2023.

REINO UNIDO. **Chair's Summary of the AI Safety Summit 2023, Bletchley Park**. 2023. Disponível em: https://www.gov.uk/government/publications/ai-safety-summit-2023-chairs-statement-2-november/chairs-summary-of-the-ai-safety-summit-2023-bletchley-park. Acesso em: 27 nov. 2023.

ROBBINS, Philip. **Modularity of Mind**. The Stanford Encyclopedia of Philosophy. 2017. Disponível em: https://plato.stanford.edu/archives/win2017/entries/modularity-mind/. Acesso em: 5 dez. 2023.

RODOTÀ, Stefano. **Costruzione del corpo, XXI Secolo**. Treccani. 2009. Disponível em: http://www.treccani.it/enciclopedia/costruzione-del-corpo_(XXI_Secolo) . Acesso em: 15 jan. 2024.

RODOTÀ, Stefano. **Il mondo nella rete**: Quali i diritti, quali i vincoli. Laterza, 2014.

RODOTÀ, Stefano. **Salviamo il corpo**: Stralcio dell'intervento al convegno su "Trasformazioni del corpo e dignità della persona". Privacy.it. 2005. Disponível em: https://www.privacy.it/archivio/rodo20050504.html. Acesso em: 11 nov. 2023.

RODOTÀ, Stefano; CONTI, Paulo. **Intervista su privacy e libertà**. Laterza, 2005.

RODRIGUES, Marco Antonio dos Santos; HIBNER, Davi Amaral. Parâmetros para a proteção de dados pessoais em tempos de pandemia. **. Revista de Direito e as Novas Tecnologias**, v. 8, jul./set. 2020.

RUARO, Regina Linden; SARLET, Gabrielle Bezerra Sales. O direito fundamental à proteção de dados sensíveis no sistema normativo brasileiro: uma análise acerca

das hipóteses de tratamento e da obrigatoriedade do consentimento livre, esclarecido e informado sob o enfoque da lei geral de proteção de dados (LGPD) – Lei 13.709/2018*. In:* BIONI, Bruno (Org) *et al*. **Tratado de Proteção de dados pessoais**. 1 ed. Rio de Janeiro: Forense, 2021.

SALLES, Arleen *et al*. **Opinion and Action Plan on 'Data Protection and Privacy'**. 2017. Disponível em: https://www.researchgate.net/publication/359792266_Opinion_and_Action_Plan_on_'Data_Protection_and_Privacy'_Human_Brain_Project_Human_Brain_Project_Authors. Acesso em: 15 nov. 2023.

SAMUEL, Sigal. **Brain-reading tech is coming. The law is not ready to protect us.**. Vox. 2019. Disponível em: https://www.vox.com/2019/8/30/20835137/facebook-zuckerberg-elon-musk-brain-mind-reading-neuroethics. Acesso em: 12 nov. 2023.

SAMUELS, Richard. Massively modular minds: Evolutionary psychology and cognitive architecture*. In:* CARRUTHERS, Peter; CHAMBERLAIN, Andrew. **Evolution and the Human Mind**: Modularity, Language and Meta-Cognition. Cambridge University Press, 2000. Disponível em: https://philpapers.org/rec/CAREAT-20. Acesso em: 15 nov. 2023.

SARLET, Ingo. Breves notas acerca da proteção de dados pessoais como direito fundamental na constituição federal brasileira de 1988: fundamentos e âmbito de proteção autônomo. **Direitos Fundamentais & Justiça**, Belo Horizonte, 2020. Disponível em: https://www.mpgo.mp.br/revista/pdfs_42/4-Ingo%20Wolfgang%20Sarlet.pdf. Acesso em: 11 nov. 2023.

SELLERS, Eric W; RYAN, David B; HAUSER, Christopher K . Noninvasive brain-computer interface enables communication after brainstem stroke. **Science Translational Medicine**, v. 6, n. 257, 08 out. 2014. Disponível em: 10.1126/scitranslmed.3007801. Acesso em: 11 nov. 2023.

SHEN, Francis X. Neuroscience, Mental Privacy, and the Law. **Harvard Journal of Law & Public Policy**, v. 36, n. 2, mar. 2013. Disponível em: https://journals.law.harvard.edu/jlpp/wp-content/uploads/sites/90/2013/04/36_2_653_Shen.pdf. Acesso em: 11 nov. 2023.

SOUZA, Maria de Fátima Marinho de. Dos dados a política: a importância da informação em saúde. **Epidemiologia e Serviços de Saúde**, v. 17, n. 1, mar. 2008. Disponível em: http://dx.doi.org/10.5123/S1679-49742008000100001 . Acesso em: 15 jan. 2024.

SULLIVAN, Laura Specker *et al*. Keeping Disability in Mind: A Case Study in Implantable Brain-Computer Interface Research. **Science and Engineering Ethics**,

v. 24, n. 2, abr. 2018. Disponível em: 10.1007/s11948-017-9928-9. Acesso em: 15 nov. 2023.

SÃO PAULO. Tribunal de Justiça. 37ª Vara Cível do Foro Central Cível da Comarca de São Paulo. Processo n. 1090663-42.2018.8.26.0100. Diário Judicial Eletrônico. Sentença, 07 de maio de 2021.

TAKAGI, Yu; NISHIMOTO, Shinji. **High-resolution image reconstruction with latent diffusion models from human brain activity**. 2023. Disponível em: https://doi.org/10.1101/2022.11.18.517004. Acesso em: 13 fev. 2024.

TEFFÉ, Chiara Spadaccini de. **Dados Pessoais Sensíveis**: Qualificação, Tratamento e Boas Práticas. 1 ed. Foco, 2022.

TEFFÉ, Chiara Antonia Spadaccini de. **A tutela da imagem da pessoa humana na internet**: da identificação do dano à sua compensação Dissertação (Mestrado em Direito Civil) - Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2016. Disponível em: https://www.bdtd.uerj.br:8443/handle/1/16842. Acesso em: 11 nov. 2023.

TEFFÉ, Chiara Spadaccini de; MAGRANI, Eduardo; STEIBEL, Fabro. Juguetes conectados y tutela de la privacidad de niños y adolescentes: explorando beneficios y desafíos*. In:* GARAVAGLIA, Lionel Ricardo Brossi (Org.); ROJAS, Tomás Dodds (Org.); PASSERON, Ezequiel (Org.). **Inteligencia artificial y bienestar de las juventudes en América Latina**. LOM Ediciones, 2019. Disponível em: https://dialnet.unirioja.es/servlet/libro?codigo=853510. Acesso em: 15 nov. 2024.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mário. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11*. In:* BIONI, Bruno (Org) *et al*. **Tratado de Proteção de dados pessoais**. 2 ed. Rio de Janeiro: Forense, 2022.

TEPEDINO, Gustavo. **As tecnologias e a renovação do Direito Civil**. OAB/RJ. 2019. Disponível em: https://www.oabrj.org.br/colunistas/gustavo-tepedino/as-tecnologias-renovacao-direito-civil. Acesso em: 5 fev. 2024.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. O consentimento na circulação de dados pessoais. **Revista Brasileira de Direito Civil** , Belo Horizonte, v. 25, jul./set. 2020. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/view/521. Acesso em: 12 nov. 2023.

TOPOL, Eric J. High-performance medicine: the convergence of human and artificial intelligence. **Nature Medicine**, v. 25, n. 1, jan. 2019. Disponível em: 10.1038/s41591-018-0300-7. Acesso em: 11 nov. 2023.

TRANFORMAÇÃO DIGITAL. **O que o futuro da Neurotecnologia nos guarda?**. 2022. Disponível em: https://transformacaodigital.com/tecnologia/o-que-o-futuro-da-neurotecnologia-nos-guarda. Acesso em: 20 nov. 2023.

TSE - TRIBUNAL SUPERIOR ELEITORAL. **Em 2021, TSE ampliou ações para implementar a Identificação Civil Nacional (ICN)**. 2021. Disponível em: https://www.tse.jus.br/imprensa/noticias-tse/2021/Dezembro/em-2021-tseampliou-acoes-para-implementar-a-identificacao-civil-nacional-icn. Acesso em: 15 jan. 2024.

USTARAN, Eduardo. **European Data Protection Law and Practice**. International Association of Privacy Professionals, 2018.

VAN INWAGEN, Peter. **Thinking about Free Will**. Cambridge University Press, 2017. Disponível em: https://www.cambridge.org/core/books/thinking-about-free-will/226A22FCC21EBA9685D1FCA35F559BE8. Acesso em: 11 nov. 2023.

VEMOU, Konstantina; HORVATH, Anna. **TechDispatch #1/2021**: Facial Emotion Recognition. European Data Protection Supervisor. 2021. Disponível em: https://edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-12021-facial-emotion-recognition_en. Acesso em: 15 jan. 2024.

VICENTE, Anamaria de Almeida. **Lei Geral Proteção de Dados Pessoais e atividades do setor da saúde**. Consultor Jurídico. 2019. Disponível em: https://www.conjur.com.br/2019-nov-12/lei-geral-protecao-dados-pessoais-atividades-setor-saude/. Acesso em: 25 jan. 2024.

WACHTER, Sandra; MITTELSTADT, Brent. A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI. **Columbia Business Law Review**, v. 2, 2019. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829. Acesso em: 12 nov. 2023.

WALTZ, Emily. **From Passwords to Passthoughts:**: Logging In to Your Devices With Your Mind. IEEE Spectrum. 2016. Disponível em: https://spectrum.ieee.org/logging-into-your-devices-with-your-mind. Acesso em: 20 nov. 2023.

WIMMER, Miriam. O regime jurídico do tratamento de dados pessoais pelo poder público*. In:* BIONI, Bruno (Org) *et al*. **Tratado de Proteção de dados pessoais**. 1 ed. Rio de Janeiro: Forense, 2021.

YEH, Malcolm. Digital EEG*. In:* YAMADA , Thoru; MENG, Elizabeth. **Practical Guide for Clinical Neurophysiologic Testing**: EEG. 2 ed. Wolters Kluwer Health, 2017.

YUSTE, Rafael *et al*. Four ethical priorities for neurotechnologies and AI. **Nature**, v. 551, n. 7679, 08 nov. 2017. Disponível em: 10.1038/551159a. Acesso em: 12 nov. 2023.

ZHANG, Zhao *et al*. A Brain-Controlled Vehicle System Based on Steady State Visual Evoked Potentials. **Cognitive Computation**, v. 15, 10 set. 2022. Disponível em: https://doi.org/10.1007/s12559-022-10051-1. Acesso em: 15 nov. 2023.

ZIMMERMANN, Raquel. **Neuromarketing político**: a chave do sucesso das campanhas políticas. Blog Neuro & Marketing. 2021. Disponível em: https://aprendaneuromarketing.com.br/blog/neuromarketing-politico-politica/. Acesso em: 20 nov. 2023.

ZUBOFF, Shoshana. **The Age of Surveillance Capitalism**: The Fight for a Human Future at the New Frontier of Power. 1 ed. PublicAffairs, 2019.