

ANÁLISE COMPARATIVA DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) E DO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS (GDPR): IMPACTOS NA REGULAÇÃO DA INTELIGÊNCIA ARTIFICIAL E NA PROTEÇÃO DA PRIVACIDADE DOS USUÁRIOS ¹

Maycon Rodrigues de Souza Lima²

RESUMO: O presente artigo visa analisar o tratamento de dados pessoais na Lei Geral de Proteção de Dados brasileira (LGPD - Lei nº 13.709/18) de forma comparativa ao Regulamento Geral de Proteção de Dados (GDPR - 2016/679). Diante da necessidade, como regra, de se enquadrar todo tratamento de dados em uma base legal determinada, mostra-se relevante estudar os impactos frente às novas tecnologia, especialmente as Inteligências Artificiais, com máquinas e modelos computacionais disruptivos, verifica-se aqui, a busca pelo equilíbrio do desenvolvimento tecnológico e o respeito aos Direitos dos titulares, especialmente o de privacidade; nesse sentido, busca-se entender e discutir a aplicação de requisitos básicos das legislações para garantir segurança nas relações e evitar que os direitos e liberdades dos titulares sejam ameaçados ou sofram danos. Para tanto, o presente artigo terá como norte a pesquisa exploratória de Direito comparado, cujas fontes bibliográficas e/ou documentais terão como base o Google Acadêmico e a Biblioteca Virtual da UFU. Os dados documentais serão extraídos de leis, doutrinas, fontes históricas e noticiários contemporâneos. O presente artigo também será composto por meio de análise qualitativa, com revisão sistematizada.

PALAVRAS-CHAVE: Dados Pessoais; Privacidade; Proteção de dados; Lei Geral de Proteção de Dados; Regulamento Geral de Proteção de Dados; Inteligência Artificial.

SUMÁRIO: 1. Autoridade Nacional de Proteção de Dados: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta lei em todo o território nacional; 2. Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada; 3.

¹ Trabalho de Conclusão de Curso apresentado à Faculdade de Direito Prof. Jacy de Assis, da Universidade Federal de Uberlândia, como requisito para obtenção do título de bacharel em direito. Orientador: Prof. Dr. João Hagenbeck Parizzi.

² Aluno do curso de Direito da Faculdade Professor Jacy de Assis da Universidade Federal de Uberlândia.

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; 4. Dado pessoal: qualquer informação relacionada a uma pessoa natural identificada ou identificável; 5. 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.

1. Introdução

A inteligência artificial (IA)³ é uma tecnologia emergente que tem o potencial de transformar diversos setores da sociedade, incluindo o mercado de trabalho. No entanto, seu uso também pode gerar riscos relacionados à privacidade, como o tratamento indevido de dados pessoais. O tratamento corresponde a qualquer interação feita com os dados pessoais; seja coleta, transmissão, armazenamento, uso, classificação, exclusão, entre outras.⁴ Nesse sentido, com o advento da IA, esses dados são usados para alimentar algoritmos e sistemas que podem aprender, prever e tomar decisões, levantando questões significativas sobre a privacidade e os direitos dos indivíduos.

Atualmente, a Lei 13709/18, conhecida como Lei Geral de Proteção de Dados (LGPD) no Brasil e o Regulamento Geral de Proteção de Dados (GDPR), também conhecido como Regulamento Europeu 2016/679, na União Europeia; criaram regulamentações similares, com o objetivo de assegurar os direitos fundamentais⁵ dos cidadãos sobre seus dados pessoais e estabelecer diretrizes seguras no tratamento. Dessarte, com o avanço tecnológico e o desenfreado uso de dados surge o inevitável debate sobre a importância da segurança da informação e o seu processamento pela IA, grande consumidora de dados. Conforme o *Social Good Brasil* - SGB, o volume de dados criado nos últimos anos é maior do que a quantidade produzida em toda a história da humanidade, com uma geração de dados que dobra a cada dois anos.⁶

³ Inteligência Artificial: o que é e como funciona. PUC, 2024. Disponível em: <<https://online.pucrs.br/blog/inteligencia-artificial>>. Acesso em 31 de out. de 2024.

⁴ Artigo 5, X da Lei 13.709/18

⁵ EMENDA CONSTITUCIONAL Nº 115, DE 2022. Disponível em: <<https://www2.camara.leg.br/legin/fed/emecon/2022/emendaconstitucional-115-10-fevereiro-2022-792285-norma-pl.html>>. Acesso em 31 de out. de 2024.

⁶ Empresas utilizam Big Data para obtenção de informações sobre negócios e ter impacto positivo no mercado. Terra, São Paulo, 6 de julho de 2024. Disponível em <https://www.terra.com.br/noticias/empresas-utilizam-big-data-para-obtencao-de-informacoes-sobre-negocios-e-ter-impacto-positivo-no-mercado_d07f7431108cfd4789f76fe4fb3bb82e21j1qy9.html?utm_source=clipboard>. Acesso em 31 de out. de 2024.

Nesse contexto, além do uso dos dados operacionais para o funcionamento das máquinas, são geradas combinações variáveis de informações de identificação pessoal, extraídas por vezes de uma pequena base de dados. Portanto, diante desse contexto, o presente artigo busca realizar, por meio comparativo com técnica bibliográfica, uma análise entre a LGPD e a GDPR na regulação da IA. Através de uma análise comparativa dessas duas leis será possível investigar como essas regulações estão moldando o respeito à privacidade, aos Direitos Fundamentais no campo da IA, desafios éticos/jurídicos e oportunidades que elas apresentam de avanços no campo da Governança de Dados.⁷

Considerando as atuais discussões sobre os impactos na Regulação das Inteligências Artificiais (IAs), o estudo comparativo entre a Lei Geral de Proteção de Dados (LGPD) do Brasil e o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia é crucial para a busca da proteção de dados em um cenário de crescente disrupção tecnológica.⁸ É nítido no cotidiano que essas tecnologias são cada vez mais imprescindíveis, seja para locomoção, por meio dos serviços de aplicativo como Uber que oferece experiência personalizada, com deslocamento em tempo real, seja para a medicina, por meio de diagnósticos cada vez mais sofisticados com resultados rápidos, como os testes de COVID-19, cujo resultado sai em menos de 10 minutos; ou até mesmo a Netflix, que foi capaz de revolucionar uma indústria de filmes e séries, superando as TVs por assinatura e o cinema. Já os smartphones substituíram os celulares convencionais, trazendo uma nova era de comunicação. inclusive no tratamento de dados neurais. Como resposta, muitos países da Europa optaram pela modificação de suas legislações, com a inserção da Proteção de Dados como um Direito Fundamental.⁹ Em paralelo, o Brasil com a LGPD também seguiu o conceito trazido pelo GDPR da União Europeia¹⁰ e, internamente, expandiu sua camada de proteção em alguns estados.

⁷ BARBIERI (2019) define Governança de Dados como um conjunto de práticas, dispostas em um framework, com o objetivo de organizar o uso e o controle adequado dos dados como um ativo organizacional. UFLA, Lavras, 2022. Disponível em <<https://kb.ufla.br/books/termos-e-definicoes-governanca-de-dados/page/governanca-de-dados>>. Acesso em 31 de out. de 2024.

⁸ Disrupção tecnológica ocorre quando uma tecnologia altera as regras do jogo de um mercado, a vida das pessoas ou uma sociedade inteira. Iberdrola. Disponível em <<https://www.iberdrola.com/inovacao/disrupcao-tecnologica#:~:text=O%20que%20significa%20a%20disrup%C3%A7%C3%A3o,pessoas%20ou%20uma%20sociedade%20inteira>>. Acesso em 31 de out. de 2024.

⁹ Artigo 16.º do Tratado sobre o Funcionamento da União Europeia (TFUE); Artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia.

¹⁰ Fichas temáticas. Parlamento europeu, Europa, maio de 2024. Disponível em <<https://www.europarl.europa.eu/factsheets/pt/sheet/157/pt/157/protecao-dos-dados-pessoais>>. Acesso em 31 de out. de 2024.

Portanto, será explanado o conceito de privacidade e sua importância, bem como a evolução da regulação da privacidade e proteção de dados na Europa e consequentemente no Brasil. Com o passar do tempo, mesmo com a criação de legislações como GDPR e LGPD, notou-se a urgência de discutir a regulação de novas tecnologias e o surgimento de novos direitos; contudo, embora a proteção dessas ferramentas sejam importantes, encontra-se o entrave do equilíbrio entre a restrição excessiva e o desenvolvimento mais eficiente das máquinas.

2. Privacidade

O conceito de privacidade ganhou força após a consolidação das Revoluções Burguesas. Inicialmente, o ideal de privacidade tinha como defesa as liberdades individuais voltadas principalmente à defesa da propriedade privada. Contudo, com o avanço tecnológico e a complexidade social, a privacidade passou a ser compreendida para além do âmbito da propriedade, inserindo-se como um direito à personalidade.

Nesse sentido, no contexto brasileiro, a Constituição Federal de 1988, em seu artigo 5º, passou a assegurar diversos direitos de personalidade. Ressalta-se o inciso X, que garante especificamente o direito à vida privada e à intimidade. Os incisos subsequentes, XI e XII, garantem a inviolabilidade do domicílio e o sigilo das comunicações pessoais, incluindo correspondência, dados e telefonemas. Esses princípios são, também, assegurados pela Declaração Universal dos Direitos Humanos de 1948, em seu artigo 12, reconhecendo e protegendo esses direitos fundamentais, evidenciando sua importância universal na preservação da dignidade humana

O doutrinador Tércio Sampaio Ferraz Jr., no resumo do seu artigo sobre sigilo de dados pessoais define: “a privacidade é regida pelo princípio da exclusividade, cujos atributos principais são a solidão (o estar-só), o segredo, a autonomia. Na intimidade protege-se sobretudo o estar-só; na vida privada, o segredo; em relação à imagem e à honra, a autonomia”.¹¹ O autor classifica o direito à privacidade como um direito subjetivo fundamental, estruturado em sujeito, conteúdo e objeto.

O sujeito é o titular do direito. (...) é toda e qualquer pessoa, física ou jurídica, brasileira ou estrangeira, residente (ou transeunte [...]) no País (art. 5º, caput). O

¹¹ FERRAZ JR., Tércio Sampaio. Sigilo de dados: O direito à privacidade e os limites à função fiscalizadora do Estado. Revista da FD-USP, v. 88, 1993, p. 439.

conteúdo é a faculdade específica atribuída ao sujeito, que pode ser a faculdade de constranger os outros ou de resistir-lhes (caso dos direitos pessoais) ou de dispor, gozar, usufruir (caso dos direitos reais). A privacidade, como direito, tem por conteúdo a faculdade de constranger os outros ao respeito e de resistir à violação do que lhe é próprio, isto é, das situações vitais que, por dizerem a ele só respeito, deseja manter para si, ao abrigo de sua única e discricionária decisão. O objeto é o bem protegido, que pode ser uma res (uma coisa, não necessariamente física, no caso de direitos reais) ou um interesse (no caso dos direitos pessoais). No direito à privacidade, o objeto é, sinteticamente, a integridade moral do sujeito.¹²

No âmbito da privacidade e intimidade, é crucial compreender o conceito de privacidade como a "qualidade do que é privado, do que diz respeito a alguém em particular". A intimidade, frequentemente utilizada como sinônimo, é definida como "caráter do que é íntimo, secreto".¹³

Dessarte, com respaldo doutrinário e influências da LGPD, GDPR e de legislações de proteção de dados ao redor do mundo, o uso do termo "privacidade" como sinônimo de "íntimo" é comum, embora nem sempre preciso. Assim, expressões como "invasão de privacidade" ilustram essa tendência, ainda que o termo mais adequado seja intimidade em alguns casos.

3. Regulação da Privacidade na Europa no contexto da internet

Na Europa, a norma atual é o Regulamento (UE) 2016/679, conhecido como Regulamento Geral de Proteção de Dados (GDPR ou RGPD), que entrou em vigor em 25.05.2018. Este regulamento substitui a Diretiva 1995/46, em vigor desde 4.05.2016, com o objetivo de adaptar suas legislações. Dado o avanço tecnológico significativo na última década, que transformou as relações entre indivíduos e Estados, a atualização normativa foi essencial para assegurar melhor proteção dos dados pessoais dos europeus.

Nesse sentido, o artigo 3º do GDPR estabelece que suas regras se aplicam ao tratamento de dados pessoais realizado em diferentes contextos no território da UE, independentemente de ocorrer dentro ou fora da União, estende-se aos indivíduos. Nesse contexto, Lemoalle e Carboni destacam que o RGPD pode ser aplicado também ao:

¹² FERRAZ JR., Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado, p. 440.

¹³ PRIVACIDADE. In: DICIO, Dicionário Online de Português. Porto: Graus, 2024.

[...] tratamento de dados pessoais de titulares residentes no território da União Europeia, estejam estes localizados fisicamente dentro ou fora da União, que venha a ser feito por alguém que não esteja localizado na União, quando as atividades de tratamento estiverem relacionadas à oferta de bens ou serviços a esses titulares de dados pessoais, tais como, vendas online por meio de uma plataforma de e-commerce, direcionamento de anúncios publicitários veiculados em uma rede social, prestação de serviço de cloud computing e uma infinidade de atividades proporcionadas, sobretudo, por aplicações de Internet.¹⁴

O novo GDPR trouxe mudanças importantes. Primeiramente, estabeleceu regras mais rigorosas sobre o exercício dos direitos dos titulares de dados e ampliou as garantias a eles oferecidas. Nesse sentido, a obtenção do consentimento dos titulares como base legal para o tratamento de dados passou a ser revisada de forma com mais cuidado, com novas condições. Assim, em caso de inconformidade na obtenção do consentimento anterior, pelo RGPD, será necessário obtê-lo novamente, especialmente no caso de menores, que exige um grau de cuidado e atenção às exigências diferenciadas.

Assim, o conceito de dados sensíveis foi ampliado; os contratos de subcontratação também passaram a ser revisados para garantir o cumprimento das novas exigências do regulamento. O encarregado da proteção de dados ganha destaque e o regulamento define medidas técnicas e organizativas para garantir a segurança dos dados, prevenindo acessos não autorizados, destruição ou modificações indevidas. Outras mudanças incluem a proteção de dados desde o início do tratamento, avaliações de impacto e a obrigação de notificação em caso de violações de segurança.¹⁵

O RGPD introduziu a avaliação obrigatória de impacto sobre a privacidade (Privacy Impact Assessments) e exigiu que empresas adotem os princípios de privacy by default e privacy by design¹⁶ em seus processos, garantindo maior proteção aos dados pessoais. Além disso, criou incentivos, como selos e certificações, para empresas que se destacarem na aplicação dessas medidas de proteção. Nesse sentido, no contexto de dados

¹⁴ LEMOALLE, Edouard; CARBONI, Guilherme. Lei Europeia de Proteção de Dados Pessoais (GDPR) e seus efeitos no Brasil.

¹⁵ COMISSÃO Nacional de Proteção de Dados. 10 medidas para preparar a aplicação do Regulamento Europeu de Proteção de Dados. [S.l.], 28.01.2017. Disponível em:

<https://www.cnpd.pt/bin/rgpd/10_Medidas_para_preparar_RGPD_CNPD.pdf>. Acesso em: 19 Out. 2024.

¹⁶ Diz respeito ao emprego de meios para se preservar a privacidade durante todo o ciclo de vida dos dados pessoais. O que é privacy by design e privacy by default? 10.2024. Disponível em:

<<https://www.terracap.df.gov.br/index.php/listagem-faq/78-lgpd-lei-geral-de-protecao-de-dados-pessoais/196-53-o-que-e-privacy-by-design-e-privacy-by-default>>. Acesso em: 19 Out. 2024.

automatizados, principalmente gerados pelas IAs, as máquinas, embora sem uma regulação específica vigente UE, passaram a receber tratamentos mais rigorosos, se comparados ao processamento de informações operacionais simples, como cadastro, por exemplo.

3.1 Regulação da Privacidade no Brasil no contexto da internet

Lei Carolina Dieckmann¹⁷

A Internet trouxe inúmeros benefícios, gerando impactos sociais positivos. No entanto, também gerou novas práticas ilícitas, com os crimes cibernéticos evoluindo à medida que o uso da tecnologia cresceu; com a globalização, o ciberespaço passou a ser habitado por pessoas de diferentes perfis, inclusive de criminosos. Nesse contexto, no ano de 2012, a atriz Carolina Dieckman foi vítima de um ataque cibercriminoso que culminou em um vazamento de fotos íntimas; diante da fragilidade legal para proteger a privacidade da população e a repercussão que o caso gerou, a ex-presidente, Dilma Rousseff sancionou duas leis que alteraram o Código Penal, adicionando os crimes virtuais e possíveis sanções.

As Leis Carolina Dieckmann (12.737/2012) e Azeredo (12.735/2012) passaram a vigorar em 2 de abril de 2013, no Código Penal Brasileiro, com o objetivo de tipificar crimes no ambiente virtual. A lei incorporou ao Código Penal os crimes informáticos, incluindo o artigo 154-A, que pune a vazamento ou divulgação de dados pessoais de terceiros sem consentimento; também foi possível estabelecer sanções para casos de invasão de dispositivos, alteração de dados ou vulnerabilidade com intuito de obter vantagem ilícita. Além disso, ressalta-se o artigo 298, que aborda a falsificação de cartões. De acordo com a Lei Carolina Dieckmann (Lei nº 12.737/2012), que alterou o Código Penal Brasileiro, os seguintes atos são punidos:

Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita: [\(Redação dada pela Lei nº 14.155, de 2021\)](#)

Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. [\(Redação dada pela Lei nº 14.155, de 2021\)](#)

¹⁷ Lei 12.737/2012

§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput. [\(Incluído pela Lei nº 12.737, de 2012\)](#) [Vigência](#)

§ 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico. [\(Redação dada pela Lei nº 14.155, de 2021\)](#)

§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: [\(Incluído pela Lei nº 12.737, de 2012\)](#) [Vigência](#)

Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa. [\(Redação dada pela Lei nº 14.155, de 2021\)](#)

§ 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos. [\(Incluído pela Lei nº 12.737, de 2012\)](#) [Vigência](#)

É importante notar que a Lei Carolina Dieckmann é uma lei que protege a privacidade das pessoas e estabelece sanções para quem viola essa privacidade. A lei não é específica para a inteligência artificial (IA), mas sim para a proteção de dados pessoais em geral. Contudo, apesar do avanço, ainda não havia uma legislação específica para punir a violação de dados pessoais no ambiente digital.

Marco Civil da Internet

O Legislativo percebeu que as leis existentes, a Constituição Federal, o Código Civil e o Código de Defesa do Consumidor, não eram suficientes para proteger os dados pessoais no ambiente digital. Por isso, criou a Lei do Marco Civil da Internet (Lei nº 12.965/2014)¹⁸, que estabeleceu o acesso à internet como direito básico e trouxe garantias como a inviolabilidade da privacidade, sigilo das comunicações e o direito à não suspensão do acesso, exceto por inadimplência. O Marco Civil regulamentou as relações digitais entre consumidores e provedores, incluindo princípios como a proteção da privacidade e dados pessoais.

Lei nº 12.965, de 23 de abril de 2014 - Marco civil da internet.

¹⁸ BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.html>. Acesso em: 18 Out. 2024

Art. 1º Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.

Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:

I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;

II - proteção da privacidade;

III - proteção dos dados pessoais, na forma da lei;

IV - preservação e garantia da neutralidade de rede;

V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;

VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;

VII - preservação da natureza participativa da rede;

VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.

Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

O Novo Marco da Internet abriu espaço para novos debates sobre a neutralidade de rede, armazenamento de dados, privacidade, responsabilidade por conteúdos infratores e armazenamento de dados no Brasil. A nova lei trouxe maior clareza sobre a privacidade dos usuários da internet, abordando direitos constitucionais como a inviolabilidade da intimidade e da vida privada (art. 7º, I), além do sigilo das informações e direito à informação (art. 7º, II e VI), assegurando que esses direitos também se aplicam no ambiente virtual. O Capítulo II da lei detalha os direitos e garantias dos usuários, incluindo a proteção da privacidade.

Art. 8º - A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.

Parágrafo único. São nulas de pleno direito as cláusulas contratuais que violem o disposto no caput, tais como aquelas que:

I – impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet; ou

II – em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil.

Embora a nova Lei nº 12.965/2014 tenha apresentado um bom avanço, o Marco demonstrou diversas limitações na abordagem de incidentes com dados pessoais, principalmente os de larga escala, com limitadas ações de mitigação de riscos e sanções brandas nas possíveis violações de dados pessoais. A título de exemplo, no ano de 2018 houve um debate no Brasil e nos EUA sobre o ataque direto à privacidade de mais de 50 milhões de usuários¹⁹; na ocasião, uma organização de consultoria política britânica chamada Cambridge Analytica²⁰ foi acusada e posteriormente declarada culpada por obter informações de usuários do Facebook, mesmo tendo sido declarado pelo aplicativo que informações sobre os perfis não seriam compartilhadas com terceiros.

Ocorre, porém, que na prática esses dados foram utilizados indevidamente, inclusive na campanha de Donald Trump à presidência dos Estados Unidos em 2016, influenciando votos dos eleitores no período eleitoral; na ocasião, cerca de 443 mil brasileiros tiveram seus dados vazados. Com a perda do consentimento e outras utilizações indevidas dos dados, o Facebook por meio da decisão do Ministério da Justiça e Segurança Pública aplicou uma multa de 6,6 milhões de reais.²¹ O fato supracitado, combinado com outros exemplos de

¹⁹ ROSENBERG, Matthew. How Trump consultants Exploited the Facebook Data of Millions. The New York Times, March 17, 2018. Disponível em: <<https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>>. Acesso disponível em 28 de out de 2024.

²⁰ Para informações completas sobre o caso consultar: DEMARTINI, Felipe. Campanha de Trump usou dados de 50 milhões de usuários do Facebook. Canaltech, 19 de Março de 2018. Disponível em: <<https://canaltech.com.br/redes-sociais/campanha-de-trump-usou-dados-de-50-milhoes-de-usuarios-do-fac...>>. Acesso: 23/10/24

²¹ Brasil multa Facebook em 6.6 milhões de reais pelo vazamento de dados no caso Cambridge. El País, Brasil, 30 de dezembro de 2019. Disponível em: <https://brasil.elpais.com/tecnologia/2019-12-30/brasil-multa-facebook-em-66-milhoes-de-reais-pelo-vazamento-de-dados-no-caso-cambridge-analytica.html#?prm=copy_link>. Acesso: 23/10/24

violações complexas aos direitos dos titulares resultaram na criação da Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018), inspirada também no GDPR, com a adoção de medidas mais severas na proteção de dados pessoais e punição de infrações.

4. Regulação da Lei Geral de Proteção de Dados (LGPD)

Como supracitado, a LGPD foi inspirada em leis semelhantes e surgiu após os escândalos de uso indevido de dados, especialmente pelas redes sociais como o Facebook. A lei entrou em vigor em setembro de 2020, tornando obrigatório que todas as empresas e organizações no Brasil se adequem às regras da lei. A lei brasileira foi criada após a aprovação da lei europeia GDPR.

A regulação é resultado de um movimento tecnológico, econômico e social. Ela foi promulgada para inserir o Brasil em um cenário de economia informacional; atualmente, a LGPD possui 10 princípios²² e com ela foram estabelecidas também 10 bases legais para a coleta, processamento e tratamento de dados no sentido geral.

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - mediante o fornecimento de consentimento pelo titular;

II - para o cumprimento de obrigação legal ou regulatória pelo controlador;

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

²² GOVERNO DO BRASIL. Conheça os 10 princípios da Lei Geral de Proteção de Dados Pessoais. Disponível em:

<<https://www.gov.br/lncc/pt-br/centrais-de-conteudo/campanhas-de-conscientizacao/campanha-lgpd/conheca-os-10-principios-da-lei-geral-de-protecao-de-dados-pessoais>>. Acesso em: 01 nov. 2024.

VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da [Lei nº 9.307, de 23 de setembro de 1996 \(Lei de Arbitragem\)](#);

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;

VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; [\(Redação dada pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente

Com a chegada da LGPD, houve uma preocupação na densificação do direito fundamental à inviolabilidade de dados, por meio de lei. A nova lei de Privacidade busca o equilíbrio entre as instituições e o indivíduo, tendo como fundamento jurídico a privacidade, a autodeterminação informacional, o consentimento e sobretudo a segurança dos dados pessoais, ao mesmo tempo em que respeita outros fundamentos como o da livre iniciativa, o desenvolvimento econômico e tecnológico.

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios. [\(Incluído pela Lei nº 13.853, de 2019\)](#) [Vigência](#)

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:

I - o respeito à privacidade;

II - a autodeterminação informativa;

III - a liberdade de expressão, de informação, de comunicação e de opinião;

IV - a inviolabilidade da intimidade, da honra e da imagem;

V - o desenvolvimento econômico e tecnológico e a inovação;

VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

4.1 Conceito de dados Pessoais

No contexto brasileiro, com a nova Lei de Proteção de Dados, a classificação de dados pessoais fica dividida entre Dados Pessoais e Dados Pessoais Sensíveis. Dados pessoais é o conjunto de informações distintas que podem levar à identificação de uma determinada pessoa. A LGPD não especifica o que é "identificável", mas com base no GDPR²³ considera como tal uma pessoa que pode ser identificada por um nome, número, características, códigos ou localização; portanto, o conceito de dado pessoal é amplo e inclui informações diretas ou indiretas sobre um indivíduo.

Por outro lado, os dados pessoais sensíveis são aqueles que a LGPD protege de maneira mais rigorosa, pois estão diretamente ligados aos aspectos mais íntimos da identidade de um indivíduo. Esses dados incluem informações sobre origem racial ou étnica, crenças religiosas, opiniões políticas, associação a sindicatos ou organizações religiosas, filosóficas ou políticas, bem como dados relacionados à saúde, vida sexual, informações genéticas ou biométricas quando conectadas a uma pessoa específica.

Art. 5º Para os fins desta Lei, considera-se:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

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;

Ocorre que, com o avanço tecnológico e a crescente "mineração de dados"²⁴, os dados que anteriormente eram considerados não sensíveis, mesmo que de conhecimento

²³ EUROPA. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. General Data Protection Regulation (GDPR). Art. 26. Disponível em: <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>>. Acesso em: 02 nov. 2024.

²⁴ O processo de minerar dados visa descobrir conexões escondidas e prever tendências futuras (...) o termo "mineração" só foi cunhado nos anos 1990, mas sua base compreende três disciplinas científicas interligadas: a estatística (o estudo numérico das relações entre dados), a inteligência artificial (inteligência exibida por softwares e/ou máquinas, que se assemelha à humana) e a machine learning (algoritmos que podem aprender com dados para realizar previsões) (MELO, 2019, p. 116)

público, como a chave pix com CPF, por exemplo, podem ser utilizados de forma indevida por terceiros, causando danos à pessoa, mesmo sem o conhecimento do titular desses dados.

Com o avanço da tecnologia e a mineração de dados pessoais, a combinação de informações pode gerar impactos significativos para o titular, mesmo que as informações individuais não sejam consideradas sensíveis em si mesmas. A complexidade resultante pode levar a consequências importantes para a vida pessoal de um indivíduo tornando necessário um tratamento mais cuidadoso e transparente dos dados pessoais. Assim, "mesmo dados considerados não sensíveis podem, sob certos tratamentos, revelar aspectos da personalidade de um indivíduo e levar a práticas discriminatórias." ²⁵Portanto, dada a interconexão tecnológica atual, é claro que limitar-se apenas ao conceito de *Dado Pessoal Sensível* para o tratamento especial e proteção reforçada, não é a abordagem mais eficaz quando o objetivo é a conformidade na governança dos dados.

Portanto, tendo em vista os conceitos e contextos supracitados, a LGPD buscou fortalecer o poder de defesa do titular e expandir as obrigações legais dos Operadores e Controladores ²⁶dos dados. Para isso, ao tratar dados, o controlador e/ou operador deve obedecer os requisitos do artigo 7º, I e seguintes, como supracitado.

4.2 Da Privacidade dos usuários e o tratamento de dados com alto risco

Além disso, ao tratar dados automatizados ou de larga escala que possam violar Direitos Fundamentais, mesmo não estando na categoria de dados sensíveis, deverão controladores e/ou operadores realizar:

Art. 5º XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a

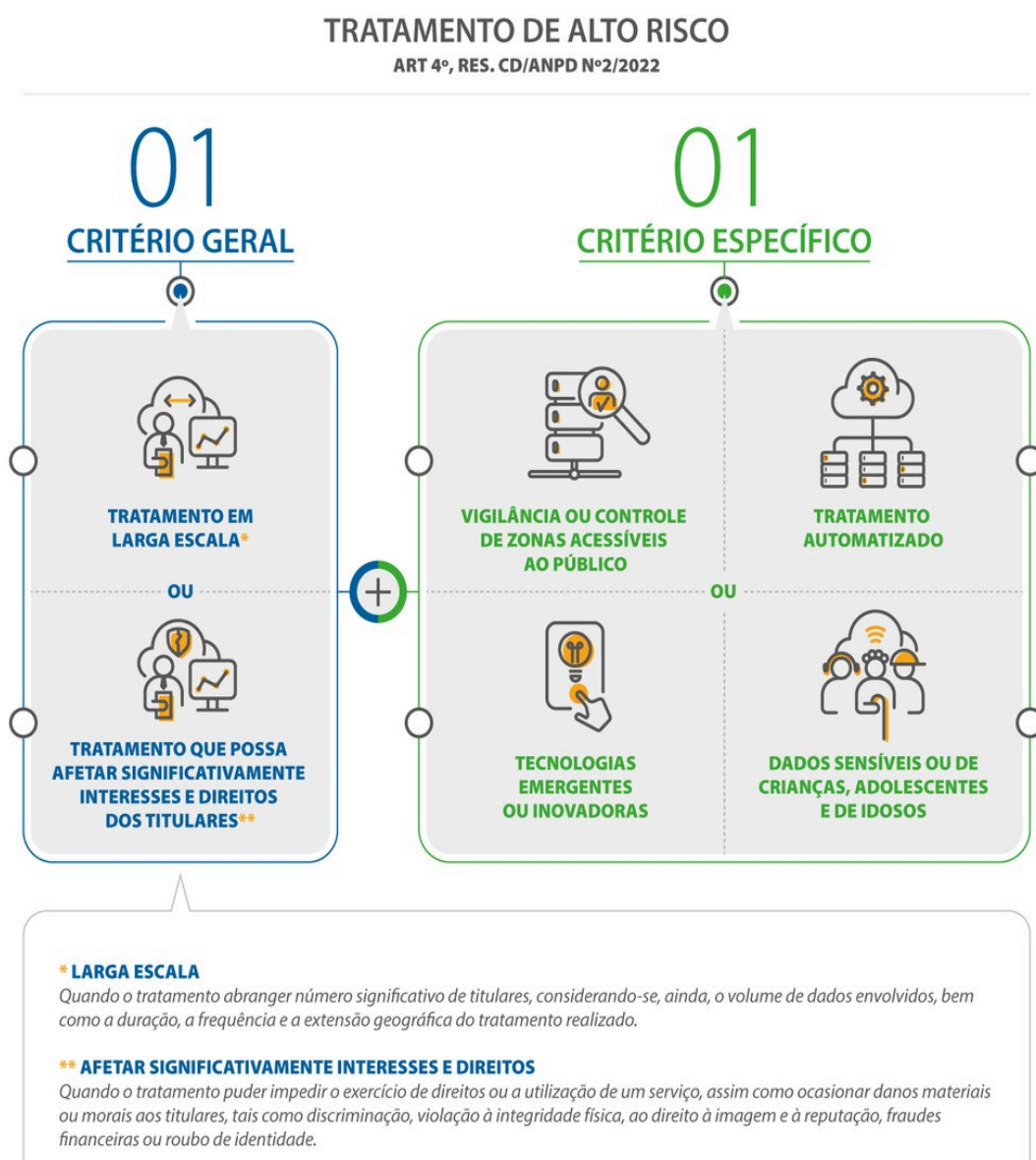
²⁵ DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006, p.162.

²⁶ BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e dá outras providências. Art. 5º, V e VI. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2018/L13709.htm>. Acesso em: 02 nov. 2024.

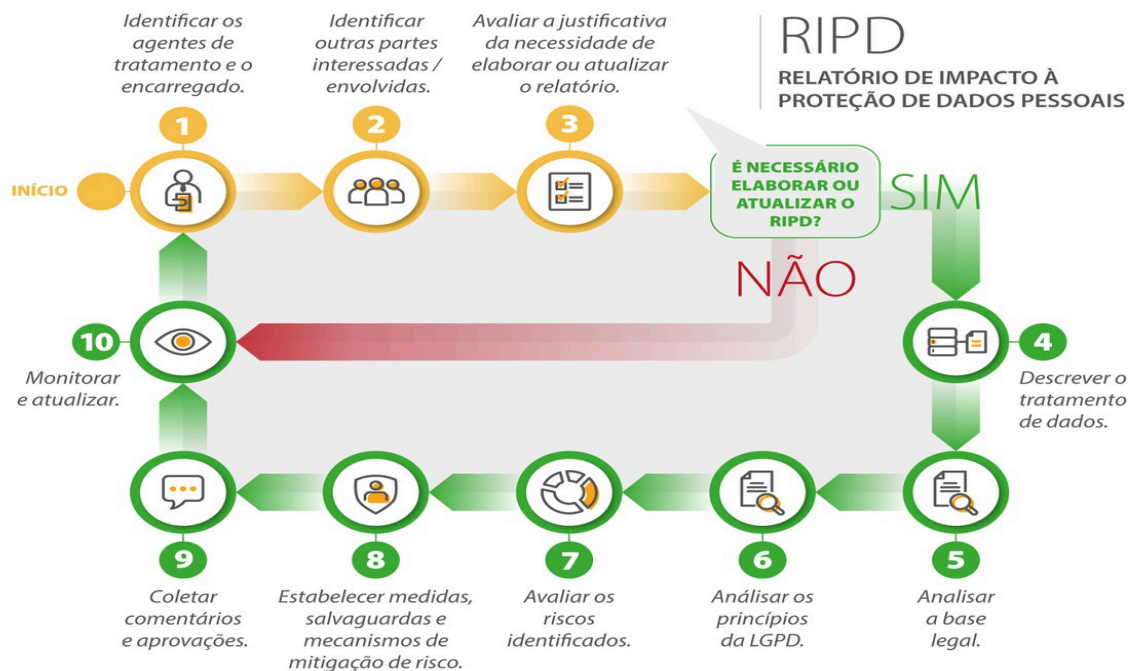
suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

Figura 1: Organograma de tratamento de Alto Risco conforme art. 4º da Resolução CD/ANPD nº 2/2022



Em suma, a jornada do RIPD funciona nos seguintes moldes:



Imagens retiradas do guia RIPD - ANPD²⁷

Ter essas delimitações em mente é fundamental para a discussão sobre a criação de novas tecnologias disruptivas que surgem com a evolução das inteligências artificiais. Embora não tenha uma regulação direta de IAs no Brasil, há diretrizes, ainda que generalistas, que podem dar um norte no tratamento de informações pessoais, enquanto uma regulação específica não entra em vigor. Essas delimitações, portanto, seguirão os princípios do artigo 6º, I e seguintes.

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

²⁷ ROSSI, Amanda. O que a farmácia sabe sobre mim? Disponível em: <https://noticias.uol.com.br/reportagens-especiais/o-que-a-farmacia-sabe-sobre-mim/#cover>. Acesso: em 03.09.2023.

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

5. Do Tratamento Automatizado de Dados Pessoais

5.1 Na LGPD

A LGPD não aborda regulações de IAs, mas estabelece regras e direitos para o tratamento de dados automatizados, também usados em processamento de dados computacionais. No seu artigo 20, a Lei Geral de Proteção de Dados empodera os titulares com o direito de não serem sujeitos a decisões baseadas exclusivamente em processos automatizados que possam afetar seus direitos de forma significativa, assegurando ao titular a possibilidade de contestação e revisão humana de tais decisões, especialmente em processos

de concessão de crédito, negociações comerciais ou outras situações que possam prejudicar diretamente o indivíduo.

Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

A lei também exige que os controladores, empresas ou entidades devem garantir que as decisões automatizadas sejam baseadas em critérios objetivos e transparentes, e que os titulares tenham acesso a informações sobre como as decisões foram tomadas

Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

§ 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial

É válido ressaltar que o tratamento de dados pessoais deve estar amparado por uma *base legal* adequada, como o consentimento, a execução de contrato, o cumprimento de obrigação legal ou regulatória. Isso significa que, para o uso de dados em decisões automatizadas, as empresas devem garantir que a coleta e o processamento desses dados estão de acordo com uma das bases legais já supracitadas, observando sempre a minimização dos dados utilizados.

5.2 Na GDPR

Já a GDPR, por outro lado, aborda a automatização de Dados no artigo 22

1. O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar.

Para isso, será necessário obedecer alguns requisitos, como:

- a) Existência de decisão: A decisão deve ser baseada no processamento de dados pessoais e afetar um indivíduo específico (BYGRAVE, 2020, p. 398).²⁸
- b) Automatização: A decisão deve ser baseada exclusivamente em processamento automatizado, sem envolvimento significativo de um ser humano (SILVA; OLIVEIRA, 2021). O Comitê Europeu de Proteção de Dados (EDPB) esclareceu que não se deve realizar uma interpretação restritiva do termo "unicamente" (EDPB/WP29, 2019, p. 20-21).²⁹
- c) Efeitos significativos: A decisão automatizada deve ter efeitos jurídicos ou de impacto significativo, como afetar os direitos ou status jurídico de um indivíduo, influenciar seu comportamento ou causar discriminação (EDPB/WP29, 2019, p. 21). Exemplos incluem a denegação de crédito ou recrutamento eletrônico sem intervenção humana significativa (Considerando 71 do GDPR).

Cabe ressaltar, aqui, a manifestação do Comitê Europeu de Proteção de Dados (EDPB) em 2018 (EDPB/WP29, 2019):

O termo direito no Regulamento Geral Europeu de Proteção de dados não quer dizer que o Artigo 22(1) apenas se aplica quando o titular dos dados pessoais o invoca ativamente. O Artigo 22(1) estabelece uma proibição geral para uma tomada de decisão baseada em um processo de automatização. Essa proibição aplica-se quer o titular dos dados adote alguma ação, quer não, no que se refere ao processamento de seus dados pessoais. (Tradução livre)³⁰

6. Inteligência Artificial e Privacidade

O termo Inteligência Artificial (IA) se refere à capacidade de programas de computador em realizar funções e raciocínios típicos da mente humana. a princípio, não existe uma precisa definição acadêmica do que vem a ser uma IA, contudo, esse campo é debatido por cientistas e filósofos, que discutem não só as questões teóricas, mas também os

²⁸ EDPB/WP29. Guidelines on Automated individual decision-making and profiling for the purposes of Regulation 2016/679 (WP251rev.01), Brussels: EU, 2018, p. 19.

²⁹ SILVA, Rafael Meira; OLIVEIRA, Cristina Godoy Bernardo de. Inteligência Artificial e proteção de dados: definição de perfil e desafios. Migalhas de Proteção de Dados, 22 jan. 2021. Disponível aqui. Acessado em 30 de outubro de 2024.

³⁰ EDPB/WP29. Guidelines on Automated individual decision-making and profiling for the purposes of Regulation 2016/679 (WP251rev.01), Brussels: EU, 2018, p. 19.

aspectos práticos, como a relação entre mente e cérebro, consciência e cognição. A IA, em suas diversas etapas de desenvolvimento, é impulsionada pela necessidade de imitar o funcionamento do cérebro humano, sendo moldada por demandas que buscam replicar suas capacidades cognitivas.

Assim, a IA tem como objetivo central o desenvolvimento de teorias e modelos de capacidade cognitiva para implementar sistemas computacionais autônomos, que simulem o comportamento inteligente humano, tais sistemas são baseados em computadores digitais, com a finalidade de realizar tarefas complexas e engajar em programas de IA.³¹

6.1 Inteligência Artificial e implicações éticas

Justamente pelos vieses do comportamento humano, a IA pode apresentar diversos preconceitos; a título de exemplo, a³² Apple Card, lançada em 2019, utilizou algoritmos para calcular os limites de crédito dos usuários. De acordo com a análise dos dados estruturados (TESSAROLO; MAGALHÃES, 2015), os algoritmos identificaram que as mulheres apresentavam um risco financeiro maior em situações idênticas, em comparação com os homens, que tinham limites de crédito 10 a 20 vezes maiores (FORBES, 2019). Nesse caso, observa-se a criação de perfis de risco baseados em estereótipos de gênero.

Além disso, com a escalada do uso dessas inteligências, inevitavelmente acentua-se a preocupação e discussão sobre as consequências de escolhas discriminatórias, como no julgamento de concursos de beleza³³, por exemplo. É importante ressaltar que a inteligência não tem consciência, portanto ela não tem intenções discriminatórias; porém, aqueles que criam e governam, são responsáveis pelo viés que é reproduzido, assim, na regulamentação, é necessário focar nas ações de prevenção de atitudes ilegais ou preconceituosas de indivíduos.

Outra problemática associada aos entraves éticos é o fornecimento de CPF em farmácias para obter descontos em produtos. Embora pareça inócua à primeira vista, na

³¹ BITTENCOURT, G. Inteligência artificial: ferramentas e teorias. 2. ed. Florianópolis: Editora da UFSC, 2001, p.16.

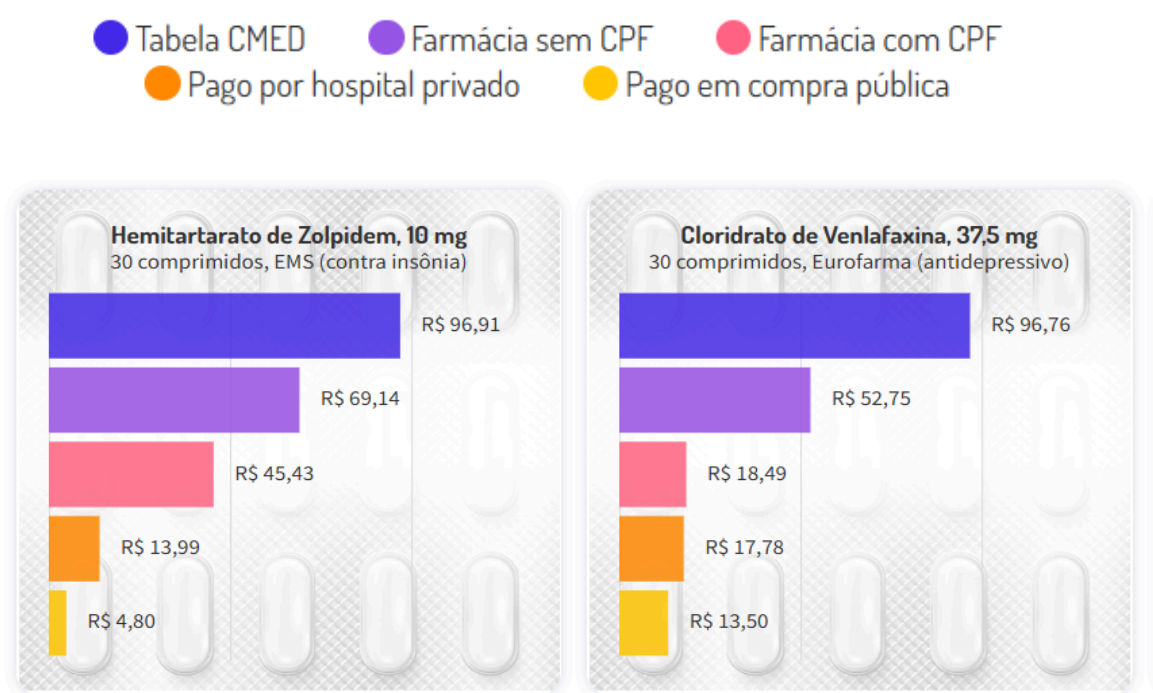
³² RIBEIRO, Ana. Discriminação em algoritmos de inteligência artificial: uma análise acerca da LGPD como instrumento normativo mitigador de vieses discriminatórios. 2023.

³³ GAZETA DO POVO. Algoritmo racista: sistema exclui pessoas de pele escura de concurso de beleza. Disponível em: <<https://www.gazetadopovo.com.br/economia/inteligencia-artificial/algoritmo-racista-sistema-exclui-pessoas-de-pele-escura-de-concurso-de-beleza-ao64d50xmcfehmh468x9cvxrh/>>. Acesso em: 01 nov. 2024.

prática,³⁴ com diversas investigações e denúncias, observa-se que grande parte das redes de farmácias utilizam sistemas automatizados e de IAs para reter e negociar dados de clientes de forma lucrativa, à custa da intimidade dos titulares. Conforme Caroline Miranda, pesquisadora da Universidade Federal do Rio de Janeiro, as farmácias se beneficiam dos altos valores da tabela da CMED, que são, na verdade, fictícios. Elas oferecem descontos sobre esses preços inflacionados, criando a ilusão de que os consumidores estão pagando muito menos. Em troca, as redes de farmácia compartilham os dados com terceiros e estes terceiros comercializam produtos³⁵ com base no histórico de cada compra ou movimento rastreado.

Na prática, nota-se uma relação desigual, que força principalmente a população mais vulnerável economicamente, sem poder de resistência, a vender seus dados, mesmo que de forma velada e inconsciente, conforme os dados a seguir:

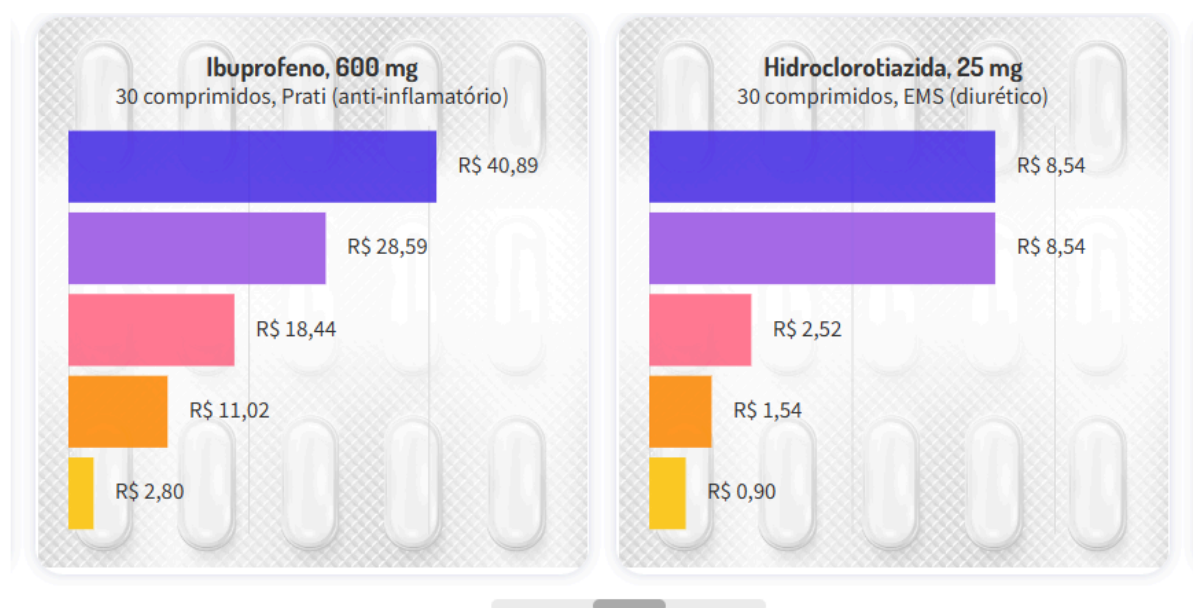
Quanto custam os medicamentos?



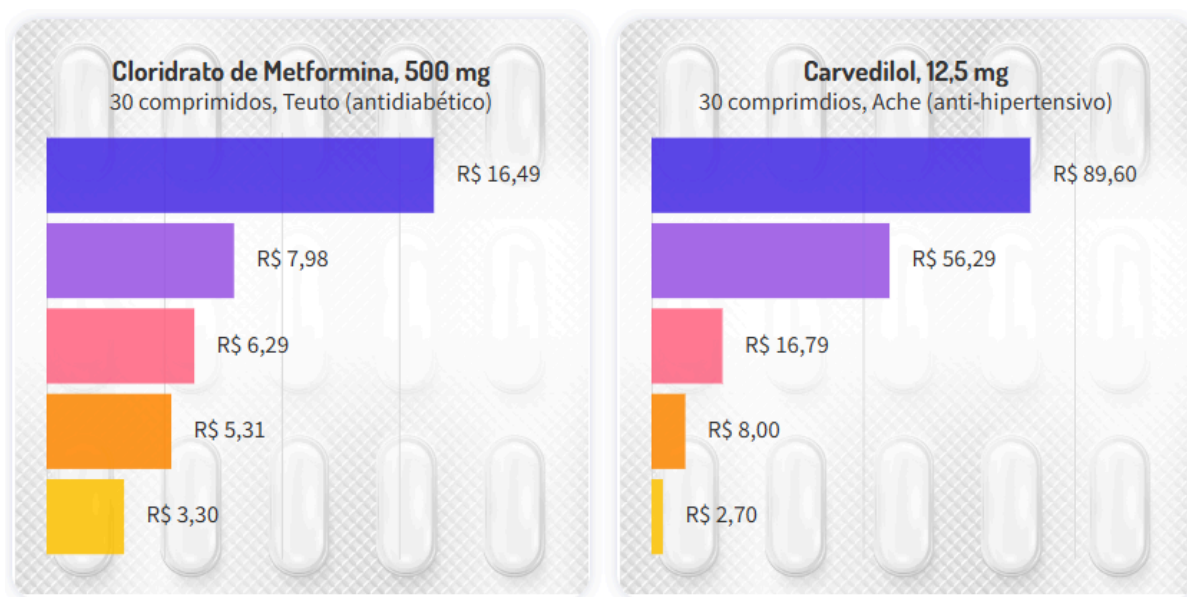
³⁴ CONJUR. Garantias de consumo: CPF em farmácias e a obtenção de descontos fictícios. Disponível em: <<https://www.conjur.com.br/2023-out-11/garantias-consumo-cpf-farmacias-obtencao-descontos-ficticios/>>.

Acesso em: 01 nov. 2024.

³⁵ UOL NOTÍCIAS. Remédio para engravidar pode direcionar até propaganda de carro. Disponível em: <<https://noticias.uol.com.br/saude/ultimas-noticias/redacao/2023/09/01/remedio-para-engravidar-pode-direcionar-ate-propaganda-de-carro.htm>>. Acesso em: 01 nov. 2024.



Preço máximo autorizado pela Cmed em SP e MG - há variações estaduais devido ao ICMS;
Preço com e sem CPF nas farmácias da RaiaDrogasil em 22/08/2023;
Menor valor pago em compras públicas em 2022 (últimos dados disponíveis);



Portanto, sob perspectiva de futuro, será necessário regular com mais rigor e eficiência que a ANPD tem demonstrado até o momento, uma vez que o uso dessas tecnologias impactam profundamente a vida dos titulares, sobretudo a intimidade. Urge-se, portanto, a padronização da fiscalização dos possíveis abusos de empresas, controladores e/ou operadores; para a nova regulação, o papel da atual ANPD será imprescindível, tendo o seu próprio meio de poder de polícia, com investigação, educação e sanção em casos de

processamento de grandes volumes de dados em tempo real, muitas vezes trata sem o conhecimento ou o controle do titular, como ainda é comum atualmente. Embora previsto já na LGPD, a autodeterminação informativa e liberdade dos titulares precisam ser um dos focos futuros.

7. Neurodireitos e os desafios regulatórios das IAs

Pensando em uma perspectiva de futuro, será imprescindível trazer maior robustez nos órgãos auxiliares à ANPD, prevista na Lei 13.709, artigo 55 C, da aplicação da proteção de dados que já possuímos, seja na linha de pesquisa, seja na linha de desenvolvimento de novos direitos que possam surgir. No artigo intitulado "*Quatro prioridades éticas para neurotecnologias e IA*", publicado na edição de novembro de 2017 da revista Nature, os autores enfatizam quatro áreas de preocupação relacionadas à neurotecnologia que também se aplicam à inteligência artificial: (1) a garantia da privacidade e do consentimento em relação aos dados neurais das pessoas, (2) a proteção da autodeterminação e do senso de identidade dos indivíduos, (3) o uso da neurotecnologia para a ampliação artificial das capacidades humanas e (4) o combate ao preconceito.

Sob o prisma da proteção da autodeterminação e do senso de identidade dos indivíduos, em face da manipulação de sua vontade e de seus valores morais, éticos e de responsabilidade, os cientistas sugerem a criação de neurodireitos.³⁶ Dessarte, com a aprovação da Lei nº 21.383, o Chile se tornou o primeiro país do mundo a instituir proteção legal aos neurodireitos. Com o intuito de adequação ao cenário disruptivo contemporâneo, o estado do Rio Grande do Sul ³⁷por meio da pela PEC 298 de 203 alterou o parágrafo único do artigo 235 de sua Constituição, estabelecendo que todo indivíduo tem o direito à integridade mental, protegendo-se contra a manipulação resultante dos avanços da neurociência e da neurotecnologia. A mudança garante que qualquer pesquisa que afete o cérebro e suas atividades só pode ser realizada com o consentimento do indivíduo.

Portanto, na nova regulação das IAs aqui no Brasil, será imprescindível absorver os princípios e bases legais que já existem na LGPD e na própria GDPR e evoluir na previsão da criação de novas formas de direitos, bem como as diversas maneiras de violação à intimidade que já existem e não estão completamente sanados ou os que passarão a surgir. A

³⁶ YUSTE, R., GOERING, S., ARCAS, B. et al. Four ethical priorities for neurotechnologies and AI. Nature 551, 159–163 (2017). Disponível em: <https://doi.org/10.1038/551159a>. Acesso em: 20 fev. 2022.

³⁷ CONJUR. A proteção ao neurodireito e a integridade mental na Constituição do RS. Disponível em: <https://www.conjur.com.br/2024-jan-05/protecao-ao-neurodireito-a-integridade-mental-na-constituicao-do-rs/>. Acesso em: 01 nov. 2024.

nova regulação das IAs diante da perspectiva dos neurodireitos deverá observar o equilíbrio textual para que o texto legal não seja restritivo a ponto de ser incapaz de promover garantias de formas eficazes, mesmo com a celeridade do tempo; observando o contexto social vigente e as tendências tecnológicas globais.

8. Artificial Intelligence Act (AI Act)

Por fim, ressalta-se a evolução regulatória das IAs na Europa. Como evolução à GDPR, o Parlamento Europeu aprovou, por maioria, um conjunto de medidas para regular o uso da IA na União Europeia, chamado AI Act. A decisão estabelece uma metodologia de análise de riscos que classifica sistemas de IA em diferentes níveis de risco. Essa abordagem é semelhante ao PL 2.338/2023, que busca regulamentar a IA no Brasil. O projeto brasileiro reflete a tendência global de legislar sobre IA, garantindo transparência e direitos dos cidadãos, e sugere que a legislação brasileira será próxima à da UE. Desde 2020, a IA tem sido discutida no Brasil, e o PL 2.338/2023 é o mais avançado e tem sido objeto de análises em comissões.

Contudo, legislar sobre o tema não é tão simples. Enquanto muitos reconhecem a necessidade de um marco regulatório claro para guiar o uso da tecnologia, há preocupações de que uma legislação excessivamente rigorosa possa inibir seu desenvolvimento, a competitividade e os avanços socioeconômicos como frisa o Senador Marcos Pontes:

— Lembrando que, quando falamos de regulação da inteligência artificial, existe um pequeno erro aí. Na verdade, é a regulação do uso da inteligência artificial, porque não há a possibilidade de você regular uma tecnologia, como é o caso da inteligência artificial. Uma legislação como essa deve conter, no seu texto, itens que, daqui a cinco anos ou dez anos, estejam ainda válidos, para que nós não tenhamos de ficar modificando essa legislação, atualizando-a à medida que a tecnologia evolui. Ela evolui, eu diria, a cada minuto. Portanto, esse é um primeiro cuidado que, idealmente, uma legislação como essa precisa ter.

Fonte: Agência Senado

Atualmente, questões sobre o uso da IA no Brasil estão sendo analisadas com base em leis existentes, como o Código de Defesa do Consumidor e a LGPD, que não foram especificamente formuladas para o contexto da IA.

A União Europeia aprovou uma lei que estabelece parâmetros para a inteligência artificial (IA), incluindo definições, categorias de risco e requisitos mínimos. A lei também

proíbe o uso de IA para manipular comportamentos humanos. A tendência é que outros países, incluindo o Brasil, sigam o exemplo e regulamentem a IA. Já é possível observar que grandes empresas brasileiras estão se antecipando e elaborando relatórios de impacto, especialmente aquelas que operam globalmente, em especial as localizadas na UE. Essas empresas costumam implementar práticas adequadas de maneira similar ao que aconteceu com a adaptação ao GDPR.

A definição de normas sobre o uso de IA na UE é um avanço significativo para a tecnologia. No Brasil, a discussão recente resultou em um projeto que, embora não perfeito, adota boas práticas de controle, com critérios de transparência. O texto atual garante direitos às pessoas afetadas, como a informação sobre interações com IA e a proteção de dados, além de proibir o uso de imagens faciais da internet ou de circuito de câmeras de segurança para criação de bancos de dados de reconhecimento facial³⁸. O AI Act prevê sanções severas por descumprimento, podendo chegar a 35 milhões de euros ou 7% do faturamento global. Por outro lado, no Brasil, a responsabilidade civil dos provedores de IA varia entre objetiva e subjetiva.

9. Considerações Finais

Portanto, a inteligência artificial é uma tecnologia em constante evolução e possui o poder de transformar diversos setores da sociedade. Contudo, à medida que seu avanço pode proporcionar melhorias sociais, seu uso pode acarretar riscos significativos à privacidade, especialmente no que se refere ao tratamento inadequado de dados pessoais. A LGPD e o GDPR são marcos regulatórios que visam assegurar os direitos fundamentais dos cidadãos sobre seus dados e estabelecer diretrizes seguras para seu tratamento.

Tanto a LGPD quanto o GDPR são regulações que surgiram devido os entraves sociais gerados pela chegada da internet e o avanço tecnológico, ambas definem princípios e diretrizes que orientam o manejo de dados pessoais, incluindo a proteção da privacidade, a autodeterminação informativa e a liberdade de expressão. Essas regulamentações também delineiam normas específicas para o tratamento de dados automatizados e para a tomada de decisões por meio de processos automatizados.

³⁸ TEC MUNDO. União Europeia aprova conjunto de leis para regulação de IA; veja detalhes. TecMundo, 2023. Disponível em: <https://www.tecmundo.com.br/mercado/280906-uniao-europeia-aprova-conjunto-leis-regulacao-ia-veja-detalhes.htm>. Acesso em: 06 nov. 2024.

Contudo, conforme discutido, a IA pode perpetuar preconceitos, como a elaboração de perfis de risco baseados em estereótipos de gênero, além de potencialmente manipular a vontade e os valores éticos e morais dos indivíduos. Nesse sentido, a regulamentação da IA no Brasil, como extensão da LGPD e na UE, como avanço do GDPR, apresenta um desafio complexo, uma vez que é fundamental equilibrar a proteção dos direitos dos cidadãos com a necessidade de fomentar a inovação e o avanço tecnológico, como a criação de aparelhos para o tratamento de doenças neurológicas, por exemplo. Nesse contexto, a proposta de criação de neurodireitos visa salvaguardar a integridade mental e a privacidade das pessoas frente às implicações da IA.

Em síntese, a regulamentação da IA é um assunto intrincado que demanda uma abordagem cuidadosa e equilibrada. É imperativo estabelecer princípios e diretrizes claros para o tratamento de dados pessoais e a tomada de decisões automatizadas, além de implementar mecanismos de proteção que garantam o respeito e a segurança dos indivíduos em relação à tecnologia.

10. Referências

BARBIERI. Governança de Dados. UFLA, Lavras, 2022. Disponível em: <<https://kb.ufla.br/books/termos-e-definicoes-governanca-de-dados/page/governanca-de-dados>>. Acesso em 31 de out. de 2024.

BITTENCOURT, G. Inteligência artificial: ferramentas e teorias. 2. ed. Florianópolis: Editora da UFSC, 2001, p. 16.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.html>. Acesso em: 18 out. de 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais. Brasília, DF: Planalto, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.html>. Acesso em 18 out. de 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e dá outras providências. Art. 5º, V e VI. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2018/L13709.htm>. Acesso em: 02 nov. 2024.

COMISSÃO Nacional de Proteção de Dados. 10 medidas para preparar a aplicação do Regulamento Europeu de Proteção de Dados. [S.l.], 28.01.2017. Disponível em: <https://www.cnpd.pt/bin/rgpd/10_Medidas_para_preparar_RGPD_CNPD.pdf>. Acesso em: 19 out. de 2024.

CONJUR. A proteção ao neurodireito e a integridade mental na Constituição do RS. Disponível em: <<https://www.conjur.com.br/2024-jan-05/protecao-ao-neurodireito-a-integridade-mental-na-constituicao-do-rs/>>. Acesso em: 01 nov. 2024.

CONJUR. Garantias de consumo: CPF em farmácias e a obtenção de descontos fictícios. Disponível em: <<https://www.conjur.com.br/2023-out-11/garantias-consumo-cpf-farmacias-obtencao-descontos-ficticios/>>. Acesso em: 01 nov. 2024.

DEMARTINI, Felipe. Campanha de Trump usou dados de 50 milhões de usuários do Facebook. Canaltech, 19 de Março de 2018. Disponível em: <<https://canaltech.com.br/redes-sociais/campanha-de-trump-usou-dados-de-50-milhoes-de-usuarios-do-fac...>>. Acesso: 23/10/24.

DICIO. PRIVACIDADE. Porto: 7Graus, 2024.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006, p. 162.

Disrupção tecnológica ocorre quando uma tecnologia altera as regras do jogo de um mercado, a vida das pessoas ou uma sociedade inteira. Iberdrola. Disponível em: <<https://www.iberdrola.com/inovacao/disrupcao-tecnologica#:~:text=O%20que%20significa%20a%20disrup%C3%A7%C3%A3o,pessoas%20ou%20uma%20sociedade%20inteira>>. Acesso em: 31 de out. de 2024.

EDPB/WP29. Guidelines on Automated individual decision-making and profiling for the purposes of Regulation 2016/679 (WP251rev.01), Brussels: EU, 2018, p. 19.

EMPRESAS utilizam Big Data para obtenção de informações sobre negócios e ter impacto positivo no mercado. Terra, São Paulo, 6 de julho de 2024. Disponível em: <https://www.terra.com.br/noticias/empresas-utilizam-big-data-para-obtencao-de-informacoes-sobre-negocios-e-ter-impacto-positivo-no-mercado,d07f7431108cfdb4789f76fe4fb3bb82e21j1qy9.html?utm_source=clipboard>. Acesso em: 31 de out. de 2024.

EMENDA CONSTITUCIONAL Nº 115, DE 2022. Disponível em: <<https://www2.camara.leg.br/legin/fed/emecon/2022/emendaconstitucional-115-10-fevereiro-2022-792285-norma-pl.html>>. Acesso em: 31 de out. de 2024.

EUROPA. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. General Data Protection Regulation (GDPR). Art. 26. Disponível em: <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>>. Acesso em: 02 nov. 2024.

FERRAZ JR., Tércio Sampaio. Sigilo de dados: O direito à privacidade e os limites à função fiscalizadora do Estado. Revista da FD-USP, v. 88, 1993, p. 439.

FERRAZ JR., Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado, p. 440.

FICHAS temáticas. Parlamento europeu, Europa, maio de 2024. Disponível em: <<https://www.europarl.europa.eu/factsheets/pt/sheet/157/protecao-dos-dados-pessoais>>. Acesso em: 31 de out. de 2024.

GAZETA DO POVO. Algoritmo racista: sistema exclui pessoas de pele escura de concurso de beleza. Disponível em: <<https://www.gazetadopovo.com.br/economia/inteligencia-artificial/algoritmo-racista-sistema-exclui-pessoas-de-pele-escura-de-concurso-de-beleza-ao64d50xmcfelmh468x9cvxrh/>>. Acesso em: 01 nov. 2024.

GOVERNO DO BRASIL. Conheça os 10 princípios da Lei Geral de Proteção de Dados Pessoais. Disponível em: <<https://www.gov.br/lncc/pt-br/centrais-de-conteudo/campanhas-de-conscientizacao/campanha-lgpd/conheca-os-10-principios-da-lei-geral-de-protecao-de-dados-pessoais>>. Acesso em: 01 nov. 2024.

LEMOALLE, Edouard; CARBONI, Guilherme. Lei Europeia de Proteção de Dados Pessoais (GDPR) e seus efeitos no Brasil.

O que é privacy by design e privacy by default? 10.2024. Disponível em: <<https://www.terraap.df.gov.br/index.php/listagem-faq/78-lgpd-lei-geral-de-protecao-de-dados-pessoais/196-53-o-que-e-privacy-by-design-e-privacy-by-default>>. Acesso em: 19 out. de 2024.

PRIVACIDADE. In: DICIO, Dicionário Online de Português. Porto: 7Graus, 2024.

ROSENBERG, Matthew. How Trump consultants exploited the Facebook data of millions. The New York Times, March 17, 2018. Disponível em: <<https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>>. Acesso disponível em 28 de out. de 2024.

RIBEIRO, Ana. Discriminação em algoritmos de inteligência artificial: uma análise acerca da LGPD como instrumento normativo mitigador de vieses discriminatórios. 2023.

SILVA, Rafael Meira; OLIVEIRA, Cristina Godoy Bernardo de. Inteligência Artificial e proteção de dados: definição de perfil e desafios. Migalhas de Proteção de Dados, 22 jan. 2021. Disponível aqui. Acesso em 30 de outubro de 2024.

TEC MUNDO. União Europeia aprova conjunto de leis para regulação de IA; veja detalhes. TecMundo, 2023. Disponível em: <https://www.tecmundo.com.br/mercado/280906-uniao-europeia-aprova-conjunto-leis-regulacao-ia-veja-detalhes.htm>. Acesso em: 06 nov. 2024.

UOL NOTÍCIAS. Remédio para engravidar pode direcionar até propaganda de carro. Disponível em: <<https://noticias.uol.com.br/saude/ultimas-noticias/redacao/2023/09/01/remedio-para-engravidar-pode-direcionar-ate-propaganda-de-carro.htm>>. Acesso em: 01 nov. 2024.

YUSTE, R., GOERING, S., ARCAS, B. et al. Four ethical priorities for neurotechnologies and AI. Nature 551, 159–163 (2017). Disponível em: <https://doi.org/10.1038/551159a>. Acesso em: 20 fev. 2022.