

**XXXI CONGRESSO NACIONAL DO
CONPEDI BRASÍLIA - DF**

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

JOSÉ RENATO GAZIERO CELLA

LITON LANES PILAU SOBRINHO

Todos os direitos reservados e protegidos. Nenhuma parte destes anais poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

Diretoria - CONPEDI

Presidente - Profa. Dra. Samyra Haydée Dal Farra Naspolini - FMU - São Paulo

Diretor Executivo - Prof. Dr. Orides Mezzaroba - UFSC - Santa Catarina

Vice-presidente Norte - Prof. Dr. Jean Carlos Dias - Cesupa - Pará

Vice-presidente Centro-Oeste - Prof. Dr. José Querino Tavares Neto - UFG - Goiás

Vice-presidente Sul - Prof. Dr. Leonel Severo Rocha - Unisinos - Rio Grande do Sul

Vice-presidente Sudeste - Profa. Dra. Rosângela Lunardelli Cavallazzi - UFRJ/PUCRio - Rio de Janeiro

Vice-presidente Nordeste - Prof. Dr. Raymundo Juliano Feitosa - UNICAP - Pernambuco

Representante Discente: Prof. Dr. Abner da Silva Jaques - UPM/UNIGRAN - Mato Grosso do Sul

Conselho Fiscal:

Prof. Dr. José Filomeno de Moraes Filho - UFMA - Maranhão

Prof. Dr. Caio Augusto Souza Lara - SKEMA/ESDHC/UFMG - Minas Gerais

Prof. Dr. Valter Moura do Carmo - UFERSA - Rio Grande do Norte

Prof. Dr. Fernando Passos - UNIARA - São Paulo

Prof. Dr. Edinilson Donisete Machado - UNIVEM/UENP - São Paulo

Secretarias

Relações Institucionais:

Prof. Dra. Claudia Maria Barbosa - PUCPR - Paraná

Prof. Dr. Heron José de Santana Gordilho - UFBA - Bahia

Profa. Dra. Daniela Marques de Moraes - UNB - Distrito Federal

Comunicação:

Prof. Dr. Robison Tramontina - UNOESC - Santa Catarina

Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali - Rio Grande do Sul

Prof. Dr. Lucas Gonçalves da Silva - UFS - Sergipe

Relações Internacionais para o Continente Americano:

Prof. Dr. Jerônimo Siqueira Tybusch - UFSM - Rio Grande do Sul

Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA - Maranhão

Prof. Dr. Felipe Chiarello de Souza Pinto - UPM - São Paulo

Relações Internacionais para os demais Continentes:

Profa. Dra. Gina Vidal Marcilio Pompeu - UNIFOR - Ceará

Profa. Dra. Sandra Regina Martini - UNIRITTER / UFRGS - Rio Grande do Sul

Profa. Dra. Maria Claudia da Silva Antunes de Souza - UNIVALI - Santa Catarina

Eventos:

Prof. Dr. Yuri Nathan da Costa Lannes - FDF - São Paulo

Profa. Dra. Norma Sueli Padilha - UFSC - Santa Catarina

Prof. Dr. Juraci Mourão Lopes Filho - UNICHRISTUS - Ceará

Membro Nato - Presidência anterior Prof. Dr. Raymundo Juliano Feitosa - UNICAP - Pernambuco

D597

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: José Renato Gaziero Cella, Liton Lanes Pilau Sobrinho – Florianópolis: CONPEDI, 2024.

Inclui bibliografia

ISBN: 978-65-5274-061-8

Modo de acesso: www.conpedi.org.br em publicações

Tema: Saúde: UM OLHAR A PARTIR DA INOVAÇÃO E DAS NOVAS TECNOLOGIAS

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito. 3. Governança e novas tecnologias.
XXX Congresso Nacional do CONPEDI Fortaleza - Ceará (3: 2024 : Florianópolis, Brasil).

CDU: 34



XXXI CONGRESSO NACIONAL DO CONPEDI BRASÍLIA - DF

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

Apresentação

No XXXI Congresso Nacional do CONPEDI, realizado nos dias 27, 28 e 29 de novembro de 2024, o Grupo de Trabalho - GT “Direito, Governança e Novas Tecnologias I”, que teve lugar na tarde de 27 de novembro de 2024, destacou-se no evento não apenas pela qualidade dos trabalhos apresentados, mas pelos autores dos artigos, que são professores pesquisadores acompanhados de seus alunos pós-graduandos. Foram apresentados artigos objeto de um intenso debate presidido pelos coordenadores e acompanhado pela participação instigante do público presente no Centro Internacional de Convenções do Brasil - CICB, em Brasília/DF.

Esse fato demonstra a inquietude que os temas debatidos despertam na seara jurídica. Cientes desse fato, os programas de pós-graduação em direito empreendem um diálogo que suscita a interdisciplinaridade na pesquisa e se propõe a enfrentar os desafios que as novas tecnologias impõem ao direito. Para apresentar e discutir os trabalhos produzidos sob essa perspectiva.

Os artigos que ora são apresentados ao público têm a finalidade de fomentar a pesquisa e fortalecer o diálogo interdisciplinar em torno do tema “Direito, Governança e Novas Tecnologias”. Trazem consigo, ainda, a expectativa de contribuir para os avanços do estudo desse tema no âmbito da pós-graduação em direito, apresentando respostas para uma realidade que se mostra em constante transformação.

Os Coordenadores

Prof. Dr. José Renato Gaziero Cella

Prof. Dr. Liton Lanes Pilau Sobrinho

O DESAFIO DA OBTENÇÃO DE CONSENTIMENTO DE DADOS PESSOAIS NA ERA DIGITAL: A INFLUÊNCIA DOS PROCESSOS AUTOMATIZADOS DE INTELIGÊNCIA ARTIFICIAL E AS INCONSISTÊNCIAS NA APLICAÇÃO DA LGPD

THE CHALLENGE OF OBTAINING PERSONAL DATA CONSENT IN THE DIGITAL AGE: THE INFLUENCE OF AUTOMATED ARTIFICIAL INTELLIGENCE PROCESSES AND THE INCONSISTENCIES IN THE APPLICATION OF THE LGPD

Carlos Eduardo Marques Silva ¹

Rodrigo Alves De Freitas ²

Guilherme Theo Rodrigues da Rocha Sampaio ³

Resumo

Na atualidade, o operador jurídico enfrenta diversos desafios relacionados à nova dinâmica social, especialmente em uma sociedade centrada na coleta de dados, o que amplia significativamente a vulnerabilidade de grande parte da população, senão de todos os cidadãos. O Brasil possui um conjunto de normas específicas para proteger dados pessoais, e essas normas, juntamente com a proteção da intimidade e da vida privada, que são consideradas equivalentes à privacidade, são garantidas pela Constituição Federal como direitos fundamentais. No entanto, apesar de haver regulamentação e inclusão na Constituição, observa-se que existem muitas discussões quanto a efetividade da proteção desses direitos no cenário concreto. Nesse contexto, este trabalho tem como objetivo explorar a questão do consentimento do titular de dados, que é uma obrigação estabelecida pela LGPD para a coleta e o tratamento de dados pessoais, a fim de avaliar se o modo como esse consentimento é obtido hoje, especialmente quando se utilizam plataformas de tecnologia que lucram com a extração de dados pessoais, está alinhado com a finalidade prevista. Portanto, utilizando-se do método dedutivo, o estudo será realizado com amparo na pesquisa bibliográfica a partir da revisão de artigos, revistas e livros sobre o assunto, buscando-se debater o problema apresentado ao longo de três capítulos.

Palavras-chave: Privacidade, Lei geral de proteção de dados pessoais, Consentimento, Vulnerabilidade, Dados pessoais

¹ Advogado atuante na seara do Direito Regulatório. Discente no programa de Mestrado Profissional em Direito do IDP. Bacharel em Direito pela Universidade Federal de Goiás - UFG. Contato: marquescse@gmail.com.

² Advogado. Discente no programa de Mestrado Profissional em Direito do IDP. Pós-graduado em Direito Médico e Direito Processual Civil pelo IDD e em Direito Empresarial pela ESA – SP.

³ Diretor da Agência Nacional de Transportes Terrestres - ANTT. Mestre em Direito pelo IDP e Mestrando em Políticas Públicas pela ULisboa.

Abstract/Resumen/Résumé

Currently, the legal operator faces several challenges related to new social dynamics, especially in a society centered on data collection, which significantly increases the vulnerability of a large part of the population, except for all citizens. Brazil has a set of specific standards for the protection of personal data. These standards, together with the protection of intimacy and private life, which are considered equivalent to privacy, are guaranteed by the Federal Constitution as fundamental rights. However, despite there being standards and inclusion in the Constitution, it is observed that there are many discussions about the effectiveness of protecting these rights in the concrete scenario. In this context, this work aims to explore the issue of data subject consent, which is an obligation imposed by the LGPD for the collection and processing of personal data, in order to assess whether the way it is received today, especially when if they use technology platforms that profit from the use of personal data, they are intended for the intended purpose. Therefore, using the deductive method, the study will be carried out with the support of bibliographical research based on the review of articles, magazines and books on the subject, seeking to debate the problem presented over three chapters.

Keywords/Palabras-claves/Mots-clés: Privacy, General personal data protection law, Consent, Vulnerability, Personal data

1. INTRODUÇÃO

A proteção dos dados pessoais alcançou no Brasil o status de um direito fundamental do indivíduo, a partir da Emenda Constitucional nº 115, de 2022, que incluiu no artigo 5º, o inciso LXXIX, da Constituição Federal. Esse reconhecimento consolidou a importância de uma estrutura regulatória robusta, que busca assegurar o respeito à privacidade e à proteção dos dados pessoais em um ambiente cada vez mais digitalizado. O cenário atual, marcado pela crescente coleta e uso de dados pessoais, exige uma constante adaptação das normas e práticas, especialmente diante dos desafios impostos pelas tecnologias emergentes, como a inteligência artificial (IA) e os processos automatizados.

Embora a LGPD estabeleça que o consentimento do titular dos dados deve ser obtido de maneira expressa e inequívoca, os avanços tecnológicos, especialmente no uso de IA em processos automatizados de coleta de dados, apresentam novos desafios para garantir que esse consentimento seja verdadeiramente livre e informado. Esses processos podem obscurecer a compreensão do titular sobre como seus dados são utilizados, levantando a necessidade de investigar a adequação do consentimento obtido em relação ao que a lei exige.

O problema de pesquisa que norteia este estudo é: a forma como o consentimento é obtido atualmente garante uma proteção eficaz dos direitos dos titulares de dados pessoais na coleta e processamento de seus dados pessoais?

Dessa forma, torna-se essencial discutir a adequação dos mecanismos de obtenção de consentimento à luz dos princípios estabelecidos pela LGPD. A relevância deste estudo decorre da crescente digitalização da sociedade e do uso massivo de plataformas tecnológicas que lucram com a extração de dados pessoais. A insuficiência ou ineficácia desses mecanismos pode resultar em graves violações dos direitos fundamentais dos indivíduos e comprometer a segurança jurídica, o que enfraquece a confiança dos cidadãos nas plataformas digitais. Assim, a análise detalhada sobre esses aspectos justifica-se como necessária para aprimorar as proteções legais existentes.

O objetivo da pesquisa é investigar se os atuais processos automatizados de IA empregados na coleta e tratamento de dados pessoais estão cumprindo os princípios da LGPD, especialmente no que diz respeito à obtenção do consentimento do titular dos dados. A hipótese que orienta este estudo é que o consentimento obtido por meio de processos automatizados de IA, ainda que expresso, não se expressa como uma manifestação inequívoca da vontade do titular, sugerindo que a forma atual de obtenção do consentimento pode não estar de acordo com os princípios estabelecidos pela legislação.

Com base no método dedutivo e em uma revisão bibliográfica de artigos científicos, revistas e livros, o estudo está dividido em três capítulos. O primeiro capítulo analisa os imperativos da sociedade da vigilância e os desafios enfrentados pelos indivíduos em relação à sua privacidade. No segundo capítulo, é discutida a evolução normativa e a construção do direito fundamental à proteção de dados pessoais no Brasil. O terceiro capítulo foca na utilização da inteligência artificial no tratamento de dados pessoais, examinando se a forma atual de obtenção do consentimento garante a proteção eficaz dos direitos dos titulares de dados. A pergunta central deste estudo é: a forma como o consentimento é obtido atualmente garante a devida proteção dos direitos dos titulares de dados pessoais?

2. A MERCANTILIZAÇÃO DA VIDA NO CONTEXTO DIGITAL: IMPACTOS DO CAPITALISMO DE VIGILÂNCIA

Atualmente, grande parte da vida humana se desenrola em um ambiente virtual, controlado por gigantes da tecnologia que, constantemente, captam dados de seus usuários para transformá-los em informações valiosas, posteriormente comercializadas. De acordo com Mielli, Ormay e Bonone (2021, p. 64), essas plataformas digitais privadas se apropriam do fluxo e da dinâmica das interações sociais em seus sistemas para uso próprio.

Nick Srnicek (2017, p. 6) afirma que, nas primeiras décadas do século XXI, a sociedade entrou em uma nova fase do capitalismo, onde a exploração econômica dos dados é o alicerce da economia. Para Lévy (2020), empresas como Google, Amazon, Facebook, Apple e Microsoft alcançaram um poder sem precedentes, monopolizando a memória global e registrando praticamente tudo que ocorre na internet. Essas corporações não só se tornaram as mais ricas do mundo, superando até as do setor energético, como também dominam o mercado de dados, possuem as tecnologias mais avançadas e fornecem a infraestrutura necessária para a comunicação global. Isso lhes permite criar uma nova forma de poder econômico e político, desempenhando funções que antes eram exclusivas dos Estados-nação.

Nesse contexto, é crucial compreender por que os dados dos usuários são tão valiosos. Esse valor reside na capacidade das plataformas de conhecer detalhes específicos sobre seus consumidores/usuários, ao ponto de segmentar o que oferecem, alterando padrões de consumo e, inclusive, influenciando posicionamentos políticos.

Um exemplo significativo é a Cambridge Analytica (CA), que vendia "marketing eleitoral" com a promessa de modificar o comportamento dos eleitores. Conforme Oliveira (2020, p. 43), a estratégia inicial da Cambridge Analytica foi coletar informações sobre os

eleitores para traçar seus perfis psicográficos. Isso permitiu classificar os eleitores em grupos distintos e identificar aqueles mais suscetíveis à persuasão. A estratégia não se limitou a convencer pessoas a votarem em Trump, mas seguiu uma lógica de "nós versus eles", buscando persuadir indecisos a apoiar Trump, mobilizar seus apoiadores e desacreditar Hillary Clinton entre seus prováveis eleitores, desmotivando-os a votar.

A capacidade de processamento de dados por meio de inferências e deduções, potencializada pelas tecnologias de informação, tornou-se tão precisa que Michal Kosinski, David Stillwell e Thore Graepel (2013, p. 1) afirmam que, com registros digitais, a ciência de dados pode prever o comportamento individual. Além disso, Wu Youyou, Michal Kosinski e David Stillwell (2014, p. 2) concluíram que a análise computacional tem uma precisão em conhecer uma pessoa superior à de parentes próximos.

O rastreamento de usuários por meio de rastros digitais envolve a coleta de dados sobre suas atividades online, como sites visitados, produtos pesquisados e compras realizadas. Essas informações são obtidas por cookies e outros mecanismos, permitindo que empresas criem perfis comportamentais dos usuários e direcionem anúncios personalizados. A criação desses perfis utiliza os dados coletados para formar representações baseadas em padrões de comportamento, facilitando a publicidade mais alinhada às preferências dos usuários.

Marcos Dantas (2019, p. 132-158) discute como a evolução da internet favoreceu o surgimento de plataformas digitais que se assemelham a feiras, onde diversos produtos são comercializados, conectando produtores e consumidores, independentemente do tipo de atividade (seja um site de buscas, um aplicativo de música ou redes/mídias sociais). A presença de múltiplos vendedores em um único espaço gera competição e atrai ainda mais consumidores, ao passo que a presença de muitos consumidores facilita a troca de informações sobre preços, tornando o local atraente tanto para compradores quanto para vendedores. Assim, as plataformas que ocupam posições dominantes no mercado são aquelas que, em determinado momento, conseguem se mostrar mais atraentes. Esses ambientes se beneficiam do efeito de rede: quanto maior o número de usuários, maior o valor da plataforma, o que, por sua vez, atrai mais usuários, favorecendo a concentração e o monopólio, dominado por um pequeno grupo de corporações gigantescas.

As plataformas, portanto, permitem que fornecedores de serviços e produtos ofereçam diretamente ao consumidor final ou até mesmo convençam os indecisos de que precisam desses produtos. Entretanto, os consumidores muitas vezes desconhecem que são tratados como produtos comercializáveis pelas plataformas.

Um exemplo ilustrativo é apresentado por Zuboff (2015, p. 81-83), que aborda a discriminação de determinados usuários nas relações de consumo, resultante do monitoramento de informações, ou seja, o tratamento diferenciado de segmentos de consumidores.

Sarlet e Molinaro (2019) fornecem um exemplo relevante ao destacar que, mesmo em contratos existentes, empregadores e companhias de seguros de saúde têm um claro interesse na saúde de seus contratados. Monitorar o comportamento do paciente ou do empregado permite implementar políticas de incentivo para os saudáveis ou sanções para aqueles que mantêm estilos de vida considerados insalubres, o que pode gerar graves impactos na liberdade individual inerente ao desenvolvimento da pessoa humana.

Com a constatação de que dados pessoais podem ser extraídos e transformados em informações altamente lucrativas, surge o que Zuboff (2015, p. 77) denomina "capitalismo de vigilância". Ao explicar esse conceito, Zuboff (2015, p. 81) afirma que as plataformas são redes institucionais onipresentes que registram, modificam e mercantilizam diariamente as relações interpessoais, a comunicação, o pensamento e quaisquer outras informações inferíveis, com o objetivo de criar novas possibilidades de monetização e lucro.

A coleta e exploração de dados pessoais tornaram-se a espinha dorsal do modelo de negócios de muitas empresas de tecnologia. Através de plataformas digitais, redes sociais e aplicativos, grandes volumes de informações são capturados, processados e convertidos em ativos valiosos.

Esse fenômeno foi denominado "economia da atenção", na qual as plataformas desenvolvem layouts e escolhem conteúdo para manter os usuários ativos em seus aplicativos por mais tempo, coletando mais informações, aumentando o tempo de exposição aos produtos anunciados por empresas que pagaram por essa visibilidade e, conseqüentemente, ampliando seu lucro. Esse comportamento do mercado já era perceptível há mais de dois séculos, conforme observado por Davenport e Beck (2001), onde uma grande quantidade de informações é compartilhada diariamente em redes sociais como Twitter e Facebook. Essa abundância de informações, junto à rapidez com que são atualizadas nas timelines, cria uma verdadeira competição pela atenção dos potenciais consumidores, dentro da lógica da economia da atenção.

Nesse cenário, surgem novos padrões contratuais e dinâmicas de poder. A capacidade de monitorar indivíduos e suas atividades cria um ambiente em que a incerteza nas relações sociais é reduzida, mas às custas da liberdade pessoal. Dilemas éticos emergem quando empresas adquirem a capacidade de influenciar decisões individuais e coletivas, direcionando comportamentos e opiniões em prol de seus próprios interesses.

Em última análise, viver em uma sociedade de vigilância apresenta um complexo desafio entre conveniência e controle. À medida que as tecnologias de vigilância permeiam todos os aspectos da vida, torna-se essencial encontrar um equilíbrio entre os benefícios da conectividade digital e a preservação dos direitos fundamentais à privacidade, à autodeterminação e à liberdade. Refletir sobre os desafios e implicações dessa sociedade nos leva a reconsiderar nossa relação com a tecnologia, com as empresas e com as estruturas de poder que moldam o mundo moderno.

A forma como as grandes empresas de tecnologia coleta dados e informações pessoais reflete uma relação unilateral, sem diálogo ou consentimento genuíno, mesmo quando os usuários aceitam os "termos de uso" e as políticas das empresas. Isso ocorre porque, em primeiro lugar, os dados são coletados mesmo quando os usuários optam por não os compartilhar e, em segundo lugar, a decisão de não usar o serviço ou produto pode resultar em exclusão social, dada a importância fundamental da internet para uma vida digna.

Esse modelo de negócios foi viabilizado pela escolha da sociedade por um serviço de internet gratuito, financiado por publicidade, em vez de um serviço pago. Como resultado, as empresas de tecnologia passaram a extrair os dados dos usuários e vendê-los ao mercado publicitário para cobrir seus custos.

3. A PROTEÇÃO DE DADOS PESSOAIS DIANTE DO COMÉRCIO DE DADOS

O conceito de vigilância, por sua própria natureza, entra em conflito com a ideia de privacidade, levantando questões cruciais sobre os direitos fundamentais diante do avanço das tecnologias da informação. A forma como as gigantes da tecnologia (*Big Techs*) coletam dados e informações pessoais ilustra uma dinâmica unilateral e impositiva, muitas vezes desprovida de verdadeiro diálogo ou consentimento. Mesmo quando os usuários aceitam os "termos de uso" e as políticas das empresas, sua privacidade continua comprometida. Isto ocorre porque, primeiramente, as informações são coletadas independentemente das escolhas dos usuários sobre o compartilhamento de dados.

Em segundo lugar, o acesso à internet é hoje visto como um direito fundamental essencial para uma vida digna; portanto, a decisão de não utilizar determinados serviços ou produtos tecnológicos pode resultar em exclusão social. Assim, a privacidade, enquanto direito fundamental, é profundamente impactada por um sistema que privilegia a coleta e a análise de dados em detrimento da autonomia individual e da proteção das informações pessoais.

Críticas severas são direcionadas à maneira como os dados são coletados sem a devida

autorização dos seus donos. Um exemplo dessa prática é a atuação do Google, que realiza a coleta de imagens de residências para seus bancos de dados sem consultar previamente os proprietários das propriedades. Em vez de buscar consentimento, a empresa simplesmente apropria-se das informações que deseja.

Quando enfrenta oposição, o Google frequentemente opta por disputas legais ou aceita pagar multas que, para a empresa, são um custo insignificante em comparação com os benefícios obtidos. Esse comportamento é descrito como um “imperialismo de infraestrutura”, um conceito explorado por Zuboff (2015, p. 78), que ressalta a desproporcionalidade entre os custos legais enfrentados e os ganhos adquiridos através da coleta indiscriminada de dados.

Zuboff (2015, p. 78) observa que o Google frequentemente se refere aos dados brutos como "resíduos", uma terminologia que destaca a forma como as empresas de tecnologia desconsideram a dimensão pessoal e a riqueza intrínseca dessas informações. Ao tratar os dados pessoais como mera mercadoria, essas empresas reduzem a privacidade a uma transação comercial.

Neste contexto, as corporações de tecnologia operam através de quatro camadas distintas no mercado de dados. Primeiramente, há a coleta e armazenamento de informações; em seguida, ocorre o processamento e a mineração dos dados; a terceira camada envolve a análise e a formação de amostras; e, finalmente, a modulação. Essas camadas se inter-relacionam e se sobrepõem de acordo com a estrutura e estratégias das empresas envolvidas, conforme descrito por Silveira, Avelino e Souza (2016).

É evidente que o que Zuboff (2015, p. 76) identifica como o mercado tradicional, baseado na relação de troca direta entre fornecedor (empresa) e consumidor (indivíduo), está ficando obsoleto. Isso ocorre porque no mercado de dados, são os dados e informações pessoais que estão sendo comercializados, tornando o próprio indivíduo o produto dessa dinâmica. Ela também estabelece uma comparação entre o antigo modelo do fordismo, que valorizava o trabalhador-consumidor como a base da economia, uma vez que produzia e comprava produtos industriais, com o modelo atual, onde o uso crescente de *softwares* resulta em uma redução na demanda por empregos diretos e exclui a população como consumidora direta.

A transformação no modelo de negócios das empresas de tecnologia ocorreu devido à escolha da sociedade por serviços de internet gratuitos financiados por publicidade, em vez de opções pagas. Com essa decisão, as empresas passaram a utilizar a coleta de dados dos usuários como um meio de cobrir seus custos operacionais, convertendo essas informações em produtos valiosos para o mercado publicitário. A coleta e a venda de dados tornaram-se estratégias

centrais para a sustentabilidade financeira dessas empresas, substituindo a receita direta dos serviços pagos.

No caso do Google, os líderes da empresa demonstraram preocupação com o impacto potencial que a implementação de taxas sobre serviços poderia ter no crescimento da base de usuários. Em resposta, optaram por um modelo baseado em publicidade, que dependia fortemente da coleta de dados dos usuários. Essa abordagem permitiu a criação de análises e algoritmos proprietários que possibilitaram a segmentação e a venda de publicidade com um nível crescente de precisão e eficácia, utilizando um sistema de leilão sofisticado para maximizar o retorno sobre investimento (Zuboff, 2015, p. 79, tradução nossa).

Adicionalmente, à medida que os dados adquirem um valor considerável e têm uma natureza intrinsecamente privada, surge a oportunidade de debater a possibilidade de comercialização desses dados em troca de remuneração financeira. Essa questão se torna particularmente relevante quando se explora o conceito de autodeterminação da informação.

Nesse contexto, é crucial analisar o conceito de autodeterminação da informação e compará-lo com o direito à privacidade tradicional. Inicialmente definido por Warren e Brandeis (1890) como "o direito de ser deixado em paz", o direito à privacidade evoluiu para o conceito de autodeterminação da informação pessoal. Este termo, introduzido por Alan Westin (1967) e posteriormente ampliado por Danilo Doneda, refere-se ao direito dos indivíduos de controlar como e quando seus dados pessoais são usados. Na década de 1970, essa ideia já estava presente na doutrina norte-americana, mas ganhou nova dimensão ao ser reconhecida como um direito fundamental, alinhado ao direito geral de personalidade, oferecendo aos indivíduos maior controle sobre suas informações (Doneda, 2021, p. 173).

No entanto, a prática da autodeterminação informativa enfrenta desafios significativos na sociedade da vigilância. Apesar de ser um direito fundamental que garante o controle sobre o acesso, uso e divulgação das informações pessoais, a realidade atual muitas vezes compromete esse controle em benefício dos interesses econômicos das empresas que exploram dados. A concentração de poder nas mãos de grandes corporações de tecnologia frequentemente resulta na minoração da privacidade individual, à medida que a coleta e o uso de dados pessoais se tornam instrumentos para maximizar lucros, em detrimento do direito à autodeterminação da informação.

Portanto, trata-se da capacidade de definir os limites nos quais seus pensamentos, emoções e informações serão compartilhados e, se optarem por compartilhar, quais são os parâmetros do que será divulgado, bem como a capacidade de revogar essa autorização a

qualquer momento. Nesse contexto, observa-se uma interligação com outras questões jurídicas e sociais, como a autodeterminação individual, o direito à personalidade e a própria liberdade.

Em relação à privacidade, a capacidade de processamento de dados por meio de inferências e deduções, obtida pelas tecnologias de informação, tornou-se tão precisa que Michal Kosinski, David Stillwell e Thore Graepel (2013, p. 1) afirmaram que a partir de registros digitais, era possível que a ciência de dados previsse o comportamento de indivíduos. Além disso, Wu Youyou, Michal Kosinski e David Stillwell (2014, p. 2) concluíram que a precisão da análise computacional em conhecer uma pessoa é até superior à de parentes próximos.

É evidente que o avanço da ciência da informação e seu impacto no mercado têm impulsionado o desenvolvimento de ferramentas de aprendizado de máquina, como o *Deep Learning*, a partir do processamento de dados. Esse progresso tem levado a melhorias notáveis no campo de conhecimento inicialmente conceituado por John McCarthy (1955, p. 251-256) como "inteligência artificial" e, portanto, exige uma exploração mais aprofundada em sua essência.

4. O USO DA INTELIGÊNCIA ARTIFICIAL NA DINÂMICA DE COLETA E PROCESSAMENTO DE DADOS PESSOAIS E A QUESTÃO DO CONSENTIMENTO

O avanço da inteligência artificial tem promovido uma transformação significativa na forma como os dados pessoais são coletados e gerenciados. Atualmente, essa tecnologia é amplamente empregada na análise e processamento de informações pessoais, com o objetivo de prever e influenciar comportamentos por meio da chamada "definição de perfil" (Lima, Oliveira, Ruiz, 2021). Esse processo envolve a criação de perfis detalhados com base em diversos dados, como hábitos de navegação, históricos de pesquisa, visualizações de páginas, interações em redes sociais e informações sobre compras recentes. Através dessa prática, as empresas de tecnologia conseguem direcionar produtos e serviços de forma personalizada, maximizando o impacto de suas estratégias publicitárias.

Apesar da necessidade de obter consentimento para a coleta e o uso de dados, a forma como esse consentimento é obtido frequentemente não cumpre adequadamente os requisitos legais estabelecidos. De acordo com o artigo 5º, XII da Lei Geral de Proteção de Dados (LGPD), o consentimento deve ser livre, informado e inequívoco, permitindo que o titular tenha uma escolha consciente sobre o tratamento de seus dados pessoais. No entanto, na prática, os usuários muitas vezes aceitam os termos de uso e políticas de privacidade sem uma

compreensão verdadeira das implicações. Muitas vezes, clicam em botões de “autorizar cookies” sem ler ou entender os detalhes das permissões concedidas.

Essa situação é exacerbada pelo design dos sites e aplicativos, que frequentemente facilitam a aceitação dos termos sem oferecer alternativas claras ou opções para uma escolha mais informada. A estrutura das interfaces digitais muitas vezes pressiona os usuários a concordarem com os termos para acessar serviços essenciais, como e-mail ou redes sociais, tornando quase impossível a recusa sem sofrer uma exclusão das interações sociais e profissionais no ambiente digital. Assim, o consentimento é obtido de forma que não reflete uma decisão verdadeiramente informada e consciente.

Essa discrepância entre o ideal legal e a prática real levanta questões sérias sobre a validade do consentimento concedido pelos usuários. Em um cenário onde a recusa pode resultar na impossibilidade de acessar serviços essenciais, o conceito de consentimento livre e informado se torna questionável. A necessidade de reconsiderar e reformular a abordagem de coleta de dados e o processo de obtenção de consentimento é evidente, de modo a garantir que os direitos dos titulares de dados sejam efetivamente protegidos e respeitados.

A problemática se agrava quando, frequentemente, o usuário não possui a oportunidade ou a capacidade de compreender o que está consentindo ao aceitar os "termos de uso" de plataformas digitais. Isso não ocorre apenas devido à necessidade de entendimento técnico desses documentos, mas, sobretudo, devido ao custo de tempo envolvido em analisar cada termo de uso de dezenas de aplicativos e plataformas utilizados atualmente, o qual é enorme. Em uma pesquisa conduzida pela Universidade Carnegie Mellon, com base em usuários dos Estados Unidos, foi constatado que se todos lessem anualmente os termos de uso de cada site que visitam, a população dos Estados Unidos gastaria aproximadamente 54 bilhões de horas lendo essas políticas de privacidade. Em outras palavras, cada pessoa precisaria dedicar cerca de 244 horas por ano para ler esses termos, o que equivale a aproximadamente 40 minutos por dia (McDonald; Cranor, 2008, p. 563).

No contexto atual, é essencial reconhecer que os indivíduos frequentemente autorizam as empresas a processar seus dados pessoais sem compreender plenamente as consequências dessa autorização. Isso revela uma vulnerabilidade informacional significativa, especialmente para os consumidores de bens e serviços no mercado digital. A dinâmica dos processos de consentimento muitas vezes prejudica a capacidade dos usuários de exercer controle adequado sobre as informações que fornecem. A complexidade e a falta de transparência nos termos de consentimento tornam difícil para os indivíduos entenderem a extensão e a finalidade do uso de seus dados pessoais.

A Lei Geral de Proteção de Dados Pessoais (LGPD) aborda essa questão ao exigir que o consentimento do titular dos dados seja obtido de forma clara e inequívoca. Conforme estipulado no artigo 7º, inciso I, da LGPD, o consentimento é uma condição essencial para qualquer processamento de dados pessoais. Adicionalmente, o artigo 8º da mesma legislação estabelece que essa autorização deve ser "expressa", podendo ser formalizada por escrito ou por outros meios que evidenciem claramente a vontade do titular. O parágrafo 3º desse artigo ainda reforça que o tratamento de dados pessoais que se baseie em consentimento obtido de forma forçada ou viciada é proibido.

A legislação, portanto, visa proteger os titulares de dados contra a violação de seu consentimento, considerando-o um elemento crucial para a legitimidade do processamento de dados. A LGPD pretende assegurar que qualquer prática que infrinja essas disposições seja considerada abusiva e sujeita a sanções conforme previsto na legislação vigente. A implementação rigorosa dessas normas é fundamental para garantir que os direitos dos indivíduos sejam respeitados e que a coleta e o uso de dados pessoais ocorram de maneira transparente e justa.

É importante refletir sobre os limites do consentimento no contexto atual, uma vez que frequentemente, a recusa em aceitar as políticas de privacidade ou a coleta de dados pessoais resulta na impossibilidade de acessar o produto ou serviço desejado. Nesse cenário, a recusa do usuário se transforma em uma barreira coercitiva, forçando-o a aceitar os termos impostos pelos controladores de dados para obter acesso. Esse dilema revela uma questão fundamental sobre a real eficácia do consentimento como expressão da autonomia do usuário.

A função do consentimento, conforme abordado na literatura, é assegurar que o indivíduo tenha o controle sobre suas informações pessoais e possa decidir livremente sobre seu processamento. Mendes (2014, p. 60) destaca que o consentimento é o mecanismo jurídico que permite ao cidadão exercer seu poder de autodeterminação informativa, garantindo sua autonomia privada. No entanto, o consentimento muitas vezes se torna uma formalidade em vez de uma verdadeira escolha, como mencionado por Mendes (2014, p. 65). O principal desafio surge quando um usuário que não concorda com os termos de um serviço digital enfrenta a exclusão do mercado de consumo, evidenciando a limitação do consentimento como ferramenta para garantir uma escolha genuína.

Esse problema revela que, apesar das intenções legais de proteger a autonomia do usuário, a prática muitas vezes não reflete essa proteção. A necessidade de aceitar os termos para acessar serviços essenciais pode transformar o consentimento em uma formalidade superficial, comprometendo sua eficácia e a verdadeira autonomia do indivíduo. Portanto, é

crucial reavaliar como o consentimento é obtido e aplicado para assegurar que os direitos dos usuários sejam efetivamente respeitados e que sua escolha seja realmente livre e informada.

No contexto da proteção de dados pessoais, Rodotà (2008) destaca a importância de uma análise detalhada das condições em que o consentimento é concedido. É essencial verificar se o consentimento resulta de um entendimento claro e se sua expressão pode ser considerada genuinamente livre. A proteção dos consumidores é especialmente crítica, considerando a falta frequente de informações claras que expõe os consumidores a uma vulnerabilidade significativa. Em resposta a essa situação, as legislações de proteção ao consumidor oferecem uma proteção adicional, reconhecendo a vulnerabilidade inerente à posição do consumidor e introduzindo o conceito de "contratante vulnerável". Este conceito é caracterizado pela falta de liberdade real na determinação de sua vontade (Rodotà, 2008, p. 138).

Rodotà (2008, p. 138) argumenta que a autenticidade do consentimento pode ser comprometida quando a recusa em aceitar a coleta e o uso de dados resulta em consequências severas, como a impossibilidade de acessar um bem ou serviço essencial. Ele ilustra esse ponto ao comparar o sistema de consentimento nos Estados Unidos, onde o consentimento para a coleta de informações sobre a saúde é muitas vezes uma condição para obter cobertura médica. Nesse contexto, a ausência de uma garantia de direito à saúde fundamental e a prevalência de um sistema privatizado de seguros criam uma situação em que a privacidade do paciente pode ser sacrificada em favor de requisitos das seguradoras. Isso demonstra como, mesmo quando o consentimento informado é formalmente obtido, ele pode ser efetivamente anulado ou se tornar uma questão de privilégio para aqueles que podem pagar diretamente pelas despesas médicas.

Portanto, para que o consentimento seja considerado legítimo, ele deve ser obtido de forma que a recusa não acarrete consequências desproporcionais para o usuário, como a exclusão de um serviço essencial. Quando o consentimento é uma condição indispensável para a utilização contínua de um serviço, funcionando como uma forma de moeda de troca, a sua autenticidade e eficácia são comprometidas. A legítima obtenção de consentimento exige que os usuários possam optar por não fornecer seus dados sem enfrentar barreiras injustas ou exclusões que afetam sua capacidade de acesso a serviços fundamentais.

Uma inovação significativa trazida pela legislação, e amplamente respaldada pela literatura, é o direito de revogação do consentimento previamente concedido. Este direito se configura como uma proteção essencial que permite aos titulares de dados exercerem controle sobre suas informações pessoais. A revogação do consentimento pode ser vista como uma extensão natural dos direitos da personalidade, que enfatiza a autonomia do indivíduo em relação ao tratamento de seus dados.

A teoria jurídica sugere que a possibilidade de revogação do consentimento, sem a necessidade de justificativas, é particularmente adequada, dado que a proteção de dados é considerada um direito da personalidade. Diferente de obrigações contratuais, onde o descumprimento pode ter implicações legais, o direito à proteção de dados se baseia na autonomia individual e, portanto, deve incluir a opção de revogação como um aspecto intrínseco. Mendes (2014, p. 64 e 65) argumenta que a dificuldade enfrentada pelos indivíduos em avaliar as implicações de seu consentimento no início do tratamento de dados reforça a necessidade de uma revogação livre e sem complicações.

De acordo com o artigo 8º, parágrafo 5º da Lei Geral de Proteção de Dados (LGPD), o titular de dados possui o direito de retirar seu consentimento a qualquer momento, por meio de um processo simples e sem custos. Essa disposição ressalta a autonomia do titular, permitindo-lhe solicitar a exclusão de seus dados de qualquer base de armazenamento sempre que se sentir desconfortável com o tratamento desses dados ou decidir não permitir mais seu uso. Esse direito de revogação é fundamental para garantir que os titulares mantenham o controle sobre suas informações pessoais e possam proteger sua privacidade de maneira eficaz.

Atualmente, os dados pessoais desempenham um papel crucial na economia da informação, conforme destacado por Bioni (2021, p. 6). A coleta e análise de informações sobre o comportamento, preferências e atividades recentes de um indivíduo permitem a personalização de ofertas de produtos e serviços de maneira eficiente. Este processo, conhecido como publicidade direcionada, é eficaz porque apresenta aos consumidores produtos que estão alinhados com seus interesses específicos, aumentando a probabilidade de aquisição desses produtos (Bioni, 2021, p. 15).

A publicidade direcionada é uma técnica que busca adaptar a comunicação publicitária com base em dados específicos do usuário, para maximizar a probabilidade de sucesso na indução ao consumo. Segundo Bioni (2021, p. 15), essa prática pode ser subdividida em diferentes tipos, como a publicidade contextual, segmentada e comportamental. Essas abordagens visam personalizar a publicidade com base em fatores que influenciam o comportamento do consumidor, aumentando a eficácia da mensagem.

Com o avanço da inteligência artificial, a coleta e análise de dados pessoais tornaram-se ainda mais sofisticadas. A tecnologia atual permite que a inteligência artificial avalie o estado emocional de um usuário através da análise de emojis em conversas, do contexto das interações e das preferências de conteúdo, como músicas e entretenimento. Esses dados são valiosos para os profissionais de marketing, pois possibilitam a implementação de estratégias de publicidade

comportamental, que se baseiam em uma vigilância contínua e detalhada dos usuários (Bioni, 2021, p. 22).

O avanço tecnológico e a integração da inteligência artificial na vida cotidiana transformaram a dependência de dispositivos tecnológicos e plataformas digitais em uma realidade consolidada. Embora essas tecnologias prometam simplificar tarefas complexas, como a organização de agendas, elas também levantam questões sobre a privacidade e o compartilhamento de dados pessoais. A coleta de informações sobre o histórico de pesquisas, os locais frequentados, o conteúdo acessado e os horários de atividade em redes sociais, conhecida como "big data", é utilizada para influenciar o comportamento dos indivíduos, evidenciando os desafios associados à privacidade na era digital.

Na sociedade atual, a atenção dos usuários emergiu como um recurso de imenso valor, conforme ressaltado por Souza, Avelino e Da Silveira (2018, p. 25). O tempo que os indivíduos passam engajados nas redes sociais se tornou um dos principais indicadores para medir seu envolvimento digital. Esse fator é de grande interesse para empresas que utilizam o marketing online para promover seus produtos. Nos bastidores, os desenvolvedores de software trabalham incessantemente para maximizar o tempo que os usuários permanecem conectados e ativos no ambiente digital.

Como resultado, desde as notificações de novas mensagens que aparecem nas telas de bloqueio dos dispositivos até os alertas que informam sobre novas postagens nas redes sociais, todos esses mecanismos são projetados com o objetivo de incentivar o uso contínuo e a permanência dos indivíduos no mundo virtual. De acordo com a literatura, a vasta quantidade de dados pessoais coletados e processados por meio da inteligência artificial e do Big Data oferece aos profissionais de marketing e desenvolvedores uma quantidade sem precedentes de oportunidades para criar e explorar novos mercados, ampliando assim os lucros de suas empresas (Souza, Avelino & Da Silveira, 2018, p. 26).

A influência das plataformas digitais na formação de opiniões é inegável na dinâmica social contemporânea. A variedade de sites e redes sociais desempenha um papel crucial na maneira como as pessoas percebem e interagem com o mundo. Esse impacto é resultado da integração do "mundo virtual" com a realidade física, criando um paralelo que molda e amplia a experiência e a percepção dos indivíduos na sociedade atual.

No cenário atual, onde as interações digitais frequentemente envolvem os mesmos indivíduos do mundo físico, a capacidade de exercer controle sobre o comportamento do usuário se torna mais viável, especialmente quando esse controle está nas mãos do próprio usuário de forma voluntária. Essa dinâmica oferece uma oportunidade significativa para

direcionar o comportamento dos consumidores com o intuito de otimizar o sucesso das transações comerciais. Nesse sentido, o marketing se estabelece como uma ferramenta poderosa que pode não apenas influenciar, mas também moldar o comportamento do consumidor.

Como argumenta Lazzaroto (2006, p. 103), o marketing tem a capacidade de transformar a sensibilidade do consumidor e incentivá-lo a realizar compras. A publicidade, ao criar um fluxo incessante de imagens e sons, desenvolve uma nova sensibilidade nos espectadores, apresentando-lhes um mundo ideal que, embora muitas vezes seja fictício, é capaz de gerar um desejo de pertencimento a esses mundos imaginários. Esse processo é descrito por Lazzaroto (2006, p. 1780) como uma forma de subjetivação que fomenta desejos e frustrações, influenciando a percepção do consumidor e contribuindo para uma forma de controle que se alinha com a expropriação capitalista contemporânea.

A combinação desses mecanismos de controle revela as características de uma "sociedade de controle", que exerce uma influência contínua sobre os desejos mais íntimos das pessoas, moldando e direcionando seu comportamento de maneira constante. Nesse cenário, torna-se evidente que o conceito de consentimento efetivo muitas vezes se desvia da realidade, pois a influência e o controle exercidos sobre o usuário podem comprometer a autenticidade do consentimento dado.

Com base nisso, pode-se dizer que o avanço das tecnologias digitais e o uso extensivo de dados pessoais transformaram profundamente o marketing e a interação com o consumidor. A capacidade das empresas de direcionar e moldar o comportamento dos usuários, utilizando técnicas sofisticadas de coleta e análise de dados, levanta questões significativas sobre o verdadeiro caráter do consentimento e da privacidade. Embora a legislação, como a Lei Geral de Proteção de Dados Pessoais, busque garantir direitos como a revogação do consentimento, a prática revela uma realidade em que a autonomia do usuário é frequentemente comprometida. A crescente integração da inteligência artificial e a dependência das plataformas digitais para atividades cotidianas enfatizam a necessidade urgente de reforçar a proteção dos dados pessoais e assegurar que o consentimento seja genuinamente informado e livre de coerções implícitas.

5. CONSIDERAÇÕES FINAIS

Diante do exposto, a interseção entre os avanços tecnológicos, a inteligência artificial e a preservação da privacidade individual revelam uma complexidade significativa no contexto da sociedade da vigilância. O ambiente digital contemporâneo, sustentado pela coleta massiva e processamento de dados pessoais, tem transformado a economia em uma esfera focada na

personalização e influência do comportamento do consumidor. Empresas de tecnologia desempenham um papel central nesse cenário, muitas vezes explorando informações sensíveis dos usuários sem garantir um consentimento verdadeiramente informado e livre.

A privacidade, um direito fundamental que busca assegurar a autodeterminação sobre as informações pessoais, enfrenta sérias ameaças nesta era digital. A disparidade de poder entre usuários e plataformas, onde o consentimento é frequentemente obtido de maneira questionável, compromete a essência da escolha e controle individual sobre seus dados. Este problema é agravado pela crescente dependência da sociedade em relação à tecnologia e pela integração da inteligência artificial nas atividades cotidianas.

O consentimento, que deveria fundamentar a coleta e o processamento legítimos de dados, frequentemente se reduz a uma formalidade sem substância, limitando a capacidade dos usuários de exercerem sua autodeterminação informativa. A exigência de aceitar termos de uso para acessar serviços essenciais e a complexidade das políticas de privacidade criam um ambiente onde a liberdade de escolha verdadeira é frequentemente comprometida.

Para garantir um equilíbrio entre os benefícios da inteligência artificial e a proteção da privacidade, é necessário adotar uma abordagem multidisciplinar. Isso envolve não apenas aspectos legais, como os estabelecidos pela Lei Geral de Proteção de Dados Pessoais (LGPD), que inclui o direito de revogar o consentimento, mas também considerações éticas e tecnológicas, além de promover a conscientização pública. O diálogo contínuo entre legisladores, reguladores, empresas e a sociedade é crucial para desenvolver soluções que protejam os direitos individuais sem comprometer a inovação tecnológica.

Portanto, a questão da privacidade na sociedade da vigilância vai além de considerações legais e tecnológicas, representando uma reflexão sobre os valores fundamentais que moldam nossa interação com a tecnologia e com os outros. À medida que navegamos por este ambiente em constante evolução, é essencial avaliar as implicações éticas e sociais das nossas ações para assegurar um futuro digital em que a autodeterminação informativa seja efetivamente respeitada e protegida.

6. REFERÊNCIAS

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos.

Constituição da República Federativa do Brasil de 1988. Brasília, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 17 ago. 2023.

_____. Presidência da República. Secretaria-Geral. Subchefia para Assuntos Jurídicos. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais – LGPD (Redação dada pela Lei nº 13.853, de 2019). Brasília, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 17 ago. 2023.

BELTRAMINI, Franciano; GUNTHER, Luiz Eduardo. O “Novo Petróleo” da Sociedade Contemporânea. **Relações Internacionais no Mundo Atual**, [s. l.], v. 1, n. 34, p. 258-278, mar. 2021. Disponível em: <http://revista.unicuritiba.edu.br/index.php/RIMA/article/view/5736/371373716>. Acesso em: 13 out. 2022.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 2. ed. Rio de Janeiro: Forense, 2021.

DONEDA, Danilo Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados. Prefácio: Gustavo Tepedino. Apresentação: Bruno Gencarelli. 3. ed. São Paulo: Revista dos Tribunais, 2021. p. 173.

DANTAS, M. **The financial logic of internet platforms: the turnover time of money at the limit of zero**. TripleC, v. 17, n. 1, p. 132-158, 2019.

DAVENPORT, Thomas H.; BECK, John C. **Economia da atenção**. 1. ed. Rio de Janeiro: Elsevier, 2001.

MCCARTHY, J. Proposal for the Dartmouth Summer Research Project on Artificial Intelligence. Dartmouth College. p. 251-256, 1955.

KOSINSKI, Michal; STILLWELL, David; GRAEPEL, Thore. **Private traits and attributes are predictable from digital records of human behavior**. Centro de Psicologia da Universidade de Cambridge. Reino Unido, 2013.

LÉVY, Pierre. **‘Gigantes da web são novo Estado’**. Entrevista concedida a Daniela Fernandes. Paris: Valor Econômico, 23 out. 2020. Disponível em: Acesso em: 19 ago. 2024.

LIMA, Cíntia Rosa Pereira de e OLIVEIRA, Cristina Godoy Bernardo de e RUIZ, Evandro Eduardo Seron. **Inteligência artificial e proteção de dados pessoais: onde essas áreas se**

encontram? 2021, Anais.. Ribeirão Preto: Instituto de Estudos Avançados - IEA-RP/USP, 2021. Disponível em: <https://www.youtube.com/watch?v=YmyGfS3Pvmg&t=714s>. Acesso em: 17 ago. 2023.

MENDES, Laura Schertel Ferreira. **Privacidade, proteção de dados e defesa do consumidor**. Linhas gerais de um novo direito fundamental. Ed. Saraiva: São Paulo, 2014.

MIELLI, Renata; ORMAY, Larissa; BONONE, Luana Meneguelli. **A democracia liberal pode sobreviver à corrosão do debate público criada pelo monopólio das big techs?**. 2021.

OLIVEIRA, João António França de. **Rússia, Cambridge Analytica e as eleições presidenciais norte-americanas de 2016: O ciberespaço como o mais recente domínio da conflitualidade política**. Universidade Católica Portuguesa, p. 43, 2020.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD)**. São Paulo: Saraiva Educação, 2018. *E-book*.

PROVOST, Foster; FAWCETT, Tom. Data science and its relationship to big data and data-driven decision making. **Big Data**, [s.l.], v. 1, n. 1, p. 51-59, 2013. Disponível em: <https://www.liebertpub.com/doi/10.1089/big.2013.1508>.

RODOTÀ, Stefano. **A vida na sociedade da vigilância: A privacidade hoje**. Org. Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SARLET, Gabrielle Bezerra Sales; MOLINARO, Carlos Alberto. **Questões tecnológicas, éticas e normativas da proteção de dados pessoais na área da saúde em um contexto de Big Data**. Direitos Fundamentais & Justiça, Belo Horizonte, a. 13, n. 41, p. 190, jul./dez. 2019.

SOUZA, Joyce; AVELINO, Rodolfo; DA SILVEIRA, Sérgio Amadeu. **A Sociedade de Controle: Manipulação e modulação nas redes sociais**. Hedra: São Paulo, 2018.

SILVEIRA, Sergio Amadeu da; AVELINO, Rodolfo; SOUZA, Joyce. **A privacidade e o mercado de dados pessoais**. Liinc em Revista, Rio de Janeiro, v.12, n.2, p. 217-230, nov. 2016.

SRNICEK, Nick. **Plataform capitalism**. Cambridge: Polity Press, 2018.

WARREN, Samuel Dennis; BRANDEIS, Louis. **The right to privacy**. Harvard Law Review, [s.l.], v. 4, n. 5, dez. 1890.

WEBINAR: #Inteligência artificial e #proteção de #dados pessoais: onde essas áreas se encontram?. [S. l.: s. n], 2021. 1 vídeo (1 h 34 min 31 seg). Publicado pelo canal Instituto de Estudos Avançados IEA-RP/USP. Disponível em:
<https://www.youtube.com/watch?v=YmyGfS3Pvmg&t=714s>. Acesso em: 17 ago. 2023.

WESTIN, Alan. Privacy and freedom. New York: Atheneum, 1970, p. 70..

YOUYOU, Wu; KOSINSKI, Michal; STILLWELL, David. **Computer-based personality judgments are more accurate than those made by humans**. Departamento de Psicologia da Universidade de Cambridge; Departamento de Ciência da Informação da Universidade de Stanford. Reino Unido, 2014.

ZUBOFF, S. **Big other: Surveillance Capitalism and the Prospects of an Information Civilization**. Journal of Information Technology, v. 30, n. 1, p. 75–89, 2015. Disponível em:
<https://doi.org/10.1057/jit.2015.5>.