XXXII CONGRESSO NACIONAL DO CONPEDI SÃO PAULO - SP

DIREITOS HUMANOS E EFETIVIDADE: FUNDAMENTAÇÃO E PROCESSOS PARTICIPATIVOS

JOANA STELZER

ABNER DA SILVA JAQUES

FLÁVIO DE LEÃO BASTOS PEREIRA

D597

Direitos humanos e efetividade: fundamentação e processos participativos[Recurso eletrônico on-line] organização CONPEDI
Coordenadores: Joana Stelzer, Abner da Silva Jaques, Flávio de Leão Bastos Pereira – Florianópolis: CONPEDI, 2025.

Inclui bibliografia
ISBN: 978-65-5274-299-5
Modo de acesso: www.conpedi.org.br em publicações
Tema: Os Caminhos Da Internacionalização E O Futuro Do Direito

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direitos humanos e efetividade. 3. Fundamentação e processos participativos. XXXII Congresso Nacional do CONPEDI São Paulo - SP (4: 2025: Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

XXXII CONGRESSO NACIONAL DO CONPEDI SÃO PAULO - SP

DIREITOS HUMANOS E EFETIVIDADE: FUNDAMENTAÇÃO E PROCESSOS PARTICIPATIVOS

Apresentação

Estimados Leitores,

É com alegria que apresentamos os Anais do Grupo de Trabalho (GT) DIREITOS HUMANOS E EFETIVIDADE: FUNDAMENTAÇÃO E PROCESSOS PARTICIPATIVOS I. Esta publicação consolida a produção científica apresentada durante o XXXII Congresso Nacional do Conpedi, que ocorreu na Universidade Presbiteriana Mackenzie, em São Paulo, de 26 a 28 de novembro de 2025.

Consolidado ao longo do tempo, o Congresso não se limita à mera apresentação de pesquisas; mas, catalisa debates sobre o futuro do Direito e sua responsabilidade social, reunindo a vanguarda da pesquisa jurídica – doutores, mestres, pesquisadores e estudantes – de todas as regiões do país. A escolha de um tema central e a organização de Grupos de Trabalho (GTs) garantem que a discussão seja ao mesmo tempo ampla e profundamente especializada, promovendo interação entre diferentes linhas de pesquisa e consolidando a comunidade acadêmica brasileira de Direito.

Entre os diversos eixos temáticos propostos, o GT DIREITOS HUMANOS E EFETIVIDADE: FUNDAMENTAÇÃO E PROCESSOS PARTICIPATIVOS I se destacou pela sua relevância intrínseca e pela urgência dos desafios sociais contemporâneos. O GT, em síntese, acolhe trabalhos que investigam tanto os êxitos na concretização dos Direitos Humanos quanto as causas da ineficácia, sejam elas estruturais, institucionais ou culturais, e propõe caminhos para a superação de tais barreiras, como a reinterpretação de dispositivos legais, a proposição de novas políticas públicas e a fiscalização de práticas estatais e privadas. Busca-se transformar os Direitos Humanos de meros enunciados programáticos em instrumentos reais de transformação social.

Em tal contexto, há um forte estímulo à crítica dogmática, na qual os participantes analisam se os modelos teóricos atuais são suficientes para abarcar novos desafios, como as crises climáticas, as novas tecnologias ou as crescentes desigualdades globais. Este componente teórico-crítico é vital para garantir que a busca pela efetividade não seja apenas instrumental, mas embasada em entendimento sólido e progressista da dignidade da pessoa humana no século XXI.

No que tange aos "Processos Participativos", almeja-se uma compreensão contemporânea de que a efetividade dos Direitos Humanos não pode ser alcançada apenas por meio de uma intervenção vertical (Estado para o cidadão). Pelo contrário, ela é intrinsecamente ligada à democratização e à horizontalização do poder. O GT explora o papel da sociedade civil, das organizações não governamentais, dos movimentos sociais e das comunidades vulneráveis na formulação, implementação e fiscalização das políticas de Direitos Humanos. Pesquisas neste eixo analisam a eficácia de instrumentos como audiências públicas, conselhos gestores, iniciativas populares e litigância estratégica como meios pelos quais os cidadãos podem exercer seu direito à participação e, assim, garantir que as ações de efetivação dos direitos sejam responsivas às suas necessidades reais e específicas. A participação é vista, portanto, não apenas como um direito, mas como o principal vetor para a realização plena de todos os outros direitos.

Dessa forma, o encerramento das atividades do Grupo de Trabalho Direitos Humanos e Efetividade: Fundamentação e Processos Participativos I, no âmbito do Congresso Nacional do CONPEDI, não apenas cumpriu sua missão de promover a ciência jurídica, mas também ofereceu perspectiva clara e imperativa: a garantia da efetividade dos Direitos Humanos transcende a esfera estatal e normativa, ancorando-se na responsabilidade individual. As pesquisas apresentadas sublinharam que a construção de uma sociedade genuinamente humanitária e justa exige que cada indivíduo assuma uma postura proativa, ética e consciente em suas ações, reconhecendo-se como peça-chave para o futuro e para a plena realização dos direitos de todos, reafirmando o papel central do CONPEDI na articulação e disseminação desse conhecimento.

Desejamos Excelente Leitura!

Profa. Dra. Joana Stelzer

Prof. Dr. Abner da Silva Jaques

Prof. Dr. Flávio de Leão Bastos Pereira

PRIVACIDADE, BIOMETRIA E CAPITALISMO DE VIGILÂNCIA: DESAFIOS DA LGPD NA SOCIEDADE DE CONTROLE

PRIVACY, BIOMETRICS AND SURVEILLANCE CAPITALISM: CHALLENGES OF BRAZIL'S GENERAL DATA PROTECTION LAW (LGPD) IN THE CONTROL SOCIETY

Frank Sérgio Pereira
Marcelo Toffano
Catarina Araujo Quaresemin

Resumo

O presente artigo analisa os impactos do uso de tecnologias biométricas e de vigilância no setor privado, considerando os limites jurídicos e éticos estabelecidos pela Lei Geral de Proteção de Dados (LGPD) e pelo Marco Civil da Internet. A pesquisa parte da compreensão da privacidade como direito fundamental implícito e condição indispensável para o exercício pleno da autonomia individual, resgatando contribuições teóricas de John Stuart Mill, Hannah Arendt, Michel Foucault e Shoshana Zuboff. A análise destaca a tensão existente entre a inovação tecnológica e a proteção de direitos fundamentais, sobretudo em ambientes privados como condomínios residenciais, empresas e relações laborais. Evidencia-se que, embora a biometria e o reconhecimento facial ofereçam eficiência e segurança, sua utilização levanta riscos concretos de discriminação algorítmica, violação da dignidade humana e restrição da liberdade individual. Conclui-se que o tratamento responsável dos dados biométricos deve observar rigorosamente os princípios da LGPD, assegurando proporcionalidade, transparência, minimização de dados e alternativas menos invasivas. Dessa forma, pretende-se contribuir para o debate acadêmico sobre os desafios impostos pela sociedade de vigilância e pela lógica do capitalismo de dados, ressaltando a importância de práticas que conciliem inovação tecnológica e respeito aos direitos fundamentais.

Palavras-chave: Privacidade, Biometria, Lgpd, Capitalismo de vigilância, Sociedade de controle

Abstract/Resumen/Résumé

This article analyzes the impacts of biometric and surveillance technologies in the private sector, considering the ethical and legal limits established by Brazil's General Data Protection Law (LGPD) and the Marco Civil da Internet. The research is grounded on the understanding of privacy as an implicit fundamental right and a necessary condition for the exercise of individual autonomy, drawing on the theoretical contributions of John Stuart Mill, Hannah Arendt, Michel Foucault, and Shoshana Zuboff. The study highlights the tension between technological innovation and the protection of fundamental rights, especially in private contexts such as residential condominiums, companies, and labor relations. Although biometrics and facial recognition may provide efficiency and security, their use raises

concrete risks of algorithmic discrimination, violations of human dignity, and restrictions on individual freedom. The article concludes that the responsible use of biometric data must strictly comply with LGPD principles, ensuring proportionality, transparency, data minimization, and less invasive alternatives. In this way, the work seeks to contribute to the academic debate on the challenges posed by surveillance society and the logic of surveillance capitalism, emphasizing the importance of reconciling technological innovation with respect for fundamental rights.

Keywords/Palabras-claves/Mots-clés: Privacy, Biometrics, Lgpd, Surveillance capitalism, Control society

INTRODUÇÃO

O avanço das tecnologias digitais e a consolidação da sociedade em rede provocaram mudanças profundas na forma como os dados pessoais são coletados, tratados e compartilhados. Nesse cenário, a biometria e os sistemas de reconhecimento facial emergem como instrumentos amplamente utilizados por empresas e instituições, seja para fins de segurança, controle de acesso ou gestão de informações. Embora ofereçam ganhos de eficiência e praticidade, tais ferramentas também suscitam preocupações jurídicas e éticas relacionadas à privacidade, à dignidade humana e aos riscos de discriminação algorítmica.

No Brasil, a promulgação da Lei nº 13.709/2018 — Lei Geral de Proteção de Dados Pessoais (LGPD) — e a atuação da Autoridade Nacional de Proteção de Dados (ANPD) estabeleceram um marco regulatório fundamental para a proteção dos titulares diante dos novos desafios tecnológicos. Entretanto, a aplicação dessas normas ainda se encontra em fase de amadurecimento, especialmente em contextos específicos como o ambiente condominial e as relações laborais.

A análise do tema não pode ser dissociada das reflexões filosóficas e sociológicas sobre poder e controle. Desde os escritos de John Stuart Mill, passando pelas concepções de Hannah Arendt e Michel Foucault, até as formulações recentes de Shoshana Zuboff acerca do capitalismo de vigilância, percebe-se que a privacidade se apresenta não apenas como um aspecto individual, mas como condição indispensável ao exercício da cidadania e da democracia.

Diante desse panorama, o presente artigo busca examinar a biometria e outras tecnologias de monitoramento à luz dos direitos fundamentais e da LGPD, com especial atenção aos desafios surgidos no setor privado. O estudo pretende identificar os limites jurídicos e éticos do uso dessas ferramentas, explorando tanto a doutrina quanto a jurisprudência recente, de modo a contribuir para o debate acadêmico e para a consolidação de práticas que compatibilizem inovação tecnológica com a preservação da dignidade humana.

1 O CONCEITO DE PRIVACIDADE COMO DIREITO FUNDAMENTAL IMPLÍCITO E COMO CONDIÇÃO PARA O EXERCÍCIO PLENO DA AUTONOMIA INDIVIDUAL

A noção de privacidade, historicamente construída e em constante transformação, consolidou-se como um dos direitos fundamentais mais relevantes na contemporaneidade. Na era digital, marcada pela coleta massiva de dados, a privacidade transcende a mera proteção da intimidade para configurar-se como condição necessária ao pleno exercício da autonomia

individual. Nesse contexto, autores como John Stuart Mill e Hannah Arendt oferecem aportes teóricos essenciais: o primeiro ao delimitar os limites da ação do Estado sobre a vida privada, e a segunda ao valorizar o espaço privado como esfera da liberdade.

1.1 A Evolução do Conceito de Privacidade

O direito à privacidade não surge como um constructo estático, mas como fruto de mudanças sociais e tecnológicas. Seu conteúdo acompanha a própria transformação da sociedade, que, com o avanço das tecnologias de informação, viu ampliar-se o espectro de riscos e violações possíveis. De acordo com Ferreira, Pinheiro e Marques (2021, p. 152), "a proteção de dados pessoais é considerada em diversos ordenamentos jurídicos como um instrumento essencial para a proteção da pessoa humana e como um direito fundamental". A privacidade, nesse sentido, consolida-se como valor indispensável à preservação da dignidade, em especial diante da coleta massiva de dados sensíveis. Essa perspectiva é reforçada por Bastos, Pantoja e Santos (2021), que observam:

> As novas tecnologias não só agridem a privacidade dos indivíduos que têm seus dados coletados por grandes empresas do segmento tecnológico, mas também geram uma grande insegurança no meio digital, uma vez que os usuários muitas vezes não são informados sobre como isso será feito ou quais informações serão utilizadas, nem por quanto tempo as informações serão mantidas nos bancos cadastrais.

Essa constatação evidencia que a privacidade deve ser compreendida em sua dimensão dinâmica: um direito que se atualiza conforme os meios de vigilância e controle evoluem. De uma concepção inicial ligada à inviolabilidade do lar e da correspondência, a privacidade passou a abranger o controle sobre dados digitais, biométricos e até mesmo padrões comportamentais.

Além disso, a noção contemporânea de privacidade está diretamente associada à autonomia individual. Isso porque, sem controle sobre os próprios dados, o sujeito se torna vulnerável a práticas de manipulação de comportamento e de restrição de escolhas. Assim, a proteção jurídica da privacidade não apenas resguarda a intimidade, mas também possibilita o pleno exercício da liberdade de decisão no espaço público e privado.

Portanto, a evolução histórica do conceito de privacidade revela que ele não é apenas um direito defensivo contra interferências externas, mas também um pressuposto da autonomia. No cenário atual, marcado pelo capitalismo de dados e pela vigilância digital, proteger a

privacidade significa, ao mesmo tempo, resguardar a dignidade humana e garantir condições reais para o exercício da cidadania e da autodeterminação.

1.2 Os Limites da Ação Estatal e a Autonomia Individual

O pensamento do filósofo britânico John Stuart Mill acerca da liberdade individual é fundamental para compreender a privacidade como condição de autonomia. Em sua clássica obra *On Liberty*, Mill estabelece uma concepção liberal da relação entre o indivíduo e o Estado, sustentando que o poder político só pode ser legitimamente exercido quando busca evitar danos a terceiros. Nesse sentido, o autor afirma que "o único fim pelo qual a humanidade está autorizada, individual ou coletivamente, a interferir na liberdade de ação de qualquer um de seus membros é a autoproteção" (Mill, 1859, p. 14).

Essa formulação, conhecida como princípio do dano (*harm principle*), delimita de maneira clara a fronteira entre a vida privada e o espaço da intervenção estatal. A privacidade, portanto, não pode ser vista apenas como um direito negativo, mas como um requisito para que o indivíduo desenvolva livremente sua personalidade, longe de ingerências desnecessárias ou arbitrárias. Como observa Bobbio (1992, p. 43), "a liberdade individual só se efetiva quando o poder é contido por limites jurídicos claros que resguardam a esfera privada do cidadão".

Ao aplicar esse raciocínio ao contexto contemporâneo, pode-se afirmar que a privacidade é um instrumento de defesa contra a hipertrofia do poder estatal. A vigilância generalizada, ainda que justificada pela segurança pública, pode extrapolar os limites fixados por Mill, ao submeter os indivíduos a uma constante supervisão que restringe sua capacidade de autodeterminação. Ferreira, Pinheiro e Marques (2021, p. 156) lembram que

> O direito à privacidade só alcança sua efetividade plena quando entendido como um limite imposto tanto ao Estado quanto ao mercado, ambos capazes de restringir a liberdade de escolha dos indivíduos.

Assim, reconhecer a privacidade como condição para a autonomia implica admitir que sem o resguardo de um espaço próprio, livre de pressões externas, não há como falar em liberdade autêntica. A ingerência desproporcional do Estado, mesmo quando voltada a finalidades legítimas, pode acarretar um efeito paralisante sobre a vida social, pois reduz a esfera de escolha e gera conformismo. Nesse sentido, Mill antecipa a crítica que hoje se dirige às tecnologias de vigilância, quando o monitoramento contínuo tende a produzir autocensura e obediência cega.

Em suma, a concepção milliana dos limites da ação estatal oferece uma base sólida para a compreensão da privacidade como direito fundamental implícito. Mais do que um simples atributo da intimidade, a privacidade deve ser entendida como condição necessária ao florescimento da autonomia individual, na medida em que estabelece a barreira mínima de proteção contra abusos do poder político e econômico.

1.3 O Espaço Privado como Esfera da Liberdade

Para se entender de forma ampla acerca do assunto, torna-se crucial fazer um estudo sobre as proposições da filósofa alemã, Hannah Arendt. Em sua análise clássica sobre "A Condição Humana", distingue as esferas da vida pública e da vida privada como dimensões fundamentais da existência humana. Para a autora, a esfera pública é o espaço da ação e do discurso, no qual os indivíduos participam do mundo comum e se inserem na política. Já a esfera privada é concebida como o local do recolhimento, da intimidade e da preservação da individualidade. Nesse sentido, Arendt (2018, p. 74) observa que "a privacidade foi considerada o refúgio onde o indivíduo podia escapar da esfera pública e desenvolver sua individualidade em segurança".

Essa concepção demonstra que a privacidade não é apenas ausência de exposição, mas um pressuposto para a liberdade autêntica, pois garante ao sujeito um espaço de proteção contra as exigências e pressões externas. Como explica Duarte (2020, p. 51), "o espaço privado é essencial para que a pessoa possa cultivar sua singularidade sem a constante necessidade de se justificar perante os demais, constituindo-se, assim, em elemento imprescindível para a dignidade humana".

A leitura dos pensamentos de Arendt revela ainda que o esvaziamento do espaço privado ameaça a própria possibilidade de ação no espaço público. Se o indivíduo não dispõe de um refúgio para elaborar suas convicções, refletir criticamente e construir sua identidade, sua presença no espaço comum tende a ser marcada pela conformidade e pela ausência de autenticidade. Em outras palavras, o espaço privado é o terreno fértil da liberdade interior, sem o qual a liberdade política se torna frágil e superficial.

> A esfera privada da vida, necessária à sobrevivência do indivíduo e da espécie, foi considerada como uma esfera de privação. Ser privado da realidade que advém do estar entre os homens, ser privado da relação com os outros, significa estar privado de uma vida plena e autenticamente humana. Entretanto, foi nesse espaço de privacidade que o homem pôde preservar a sua individualidade, manter sua autonomia diante da coletividade e desenvolver

> aquelas qualidades que não se submetem ao julgamento público, mas que são igualmente essenciais à dignidade humana. (Arendt, 2018, p. 74-75).

No contexto contemporâneo, essa análise é especialmente relevante diante da lógica da sociedade da vigilância. A exposição contínua promovida por plataformas digitais, a coleta massiva de dados pessoais e a vigilância estatal ampliada corroem o espaço privado e reduzem as condições de exercício da liberdade individual. Ao transformar a vida íntima em objeto de monitoramento e mercantilização, abre-se espaço para a colonização do indivíduo pela lógica do consumo e do controle social, fenômeno já identificado por Zuboff (2019) como "capitalismo de vigilância".

A valorização do espaço privado por Arendt reforça que a privacidade é uma condição de liberdade. Ela não se reduz a uma escolha individual, mas constitui uma estrutura necessária para que os sujeitos mantenham sua autonomia, resguardem sua dignidade e possam participar do espaço público de forma consciente e crítica.

1.4 O direito à privacidade em risco na sociedade da vigilância

O filósofo francês, Michel Foucualt, realiza uma análise importantíssima sobre poder disciplinar em sua obra "Vigiar e Punir" e encontra no panoptismo uma das metáforas mais potentes para compreender os mecanismos de controle social. Inspirado no modelo arquitetônico de Jeremy Bentham, o panóptico é um espaço no qual um único vigilante pode observar a todos sem ser visto, instaurando uma lógica de autocontrole e vigilância internalizada. Foucault (1983, p. 177) descreve:

> Basta então colocar um vigia na torre central, e em cada cela trancar um louco, um doente, um condenado, um operário ou um escolar. Pelo efeito da contraluz, pode-se perceber da torre, recortando-se exatamente sobre a claridade, as pequenas silhuetas cativas nas celas da periferia.

Tal mecanismo não se resume a uma técnica prisional, mas revela um paradigma de poder moderno, baseado na disciplina e na produção de subjetividades dóceis e úteis à ordem social. Conforme Anamelechi (2025), o panoptismo "transcende sua origem arquitetônica para se tornar uma poderosa metáfora das formas modernas e capilares de exercício do poder".

Ao deslocar o foco do suplício corporal para a vigilância difusa, Foucault (1983) identifica o nascimento de uma sociedade disciplinar, na qual quartéis, escolas, hospitais e fábricas compartilham a lógica panóptica: observar, registrar, classificar e corrigir condutas.

Como observa Brandão (2023, p. 5), “as disciplinas funcionam cada vez mais como técnicas que fabricam indivíduos úteis”, internalizando o controle e tornando cada sujeito vigia de si mesmo

O efeito mais profundo do panoptismo não é a coerção física, mas a normalização do comportamento por meio da possibilidade constante de estar sob olhar. Daí decorre a noção de autovigilância: o indivíduo adapta suas práticas e pensamentos como se estivesse permanentemente sendo observado.

1.4.1 O panoptismo digital

Na contemporaneidade, essa lógica de poder assume novas feições. As tecnologias digitais ampliam exponencialmente o alcance da vigilância. Como sintetiza Queiroga (2022), “as redes sociais oferecem diversos instrumentos que estimulam, controlam e traçam perfis de seus usuários”, convertendo a vida digital em fonte permanente de dados e monitoramento

Essa vigilância é voluntária e participativa: os próprios usuários entregam dados, opiniões e hábitos de consumo, legitimando o poder das plataformas. Diferente do panóptico prisional, o panoptismo digital atua por meio de algoritmos invisíveis, que classificam e preveem comportamentos, produzindo novas formas de sujeição. Segundo Araújo, Silva e Silva Junior (2021, p. 111), vivemos a transição “do panóptico da sociedade disciplinar aos dispositivos tecnopolíticos da sociedade de controle”.

Em contextos urbanos, o videomonitoramento massivo atualiza essa lógica. Assim, o panoptismo digital não apenas vigia, mas cria categorias de sujeitos a serem controlados ou marginalizados.

A filósofa e psicóloga social norte-americana Shoshana Zuboff cunhou a expressão capitalismo de vigilância para descrever uma nova fase do sistema capitalista, marcada pela apropriação da experiência humana como matéria-prima gratuita para a extração, análise e comercialização de dados. Como sintetiza: “O capitalismo de vigilância reivindica de maneira unilateral a experiência humana como matéria-prima gratuita para a tradução em dados comportamentais” (Zuboff, 2021, p. 22).

O ponto central da crítica de Zuboff é que o capitalismo de vigilância opera por meio da expropriação da experiência humana, transformando cada interação cotidiana — buscas na internet, uso de redes sociais, compras online, localização via GPS — em informações tratadas como ativos comportamentais. Segundo Koerner (2021), “as Big Techs usam tecnologias da

informação e comunicação para expropriar a experiência humana, que se torna matéria-prima processada e mercantilizada como dados comportamentais".

Esse processo não apenas invade a esfera da privacidade, mas cria condições para a modificação do comportamento dos indivíduos, gerando previsibilidade e controle. A manipulação é sutil e ocorre por meio de algoritmos que induzem escolhas de consumo, moldam preferências políticas e influenciam decisões sociais.

Diante do exposto, verifica-se que a privacidade, concebida como direito fundamental implícito, enfrenta graves desafios na sociedade contemporânea marcada pela vigilância difusa e pelo capitalismo de dados. De Mill a Arendt, passando por Foucault e Zuboff, fica evidente que a privacidade não se reduz à esfera íntima, mas constitui condição indispensável para a autonomia individual e para a própria democracia. O panoptismo digital e o capitalismo de vigilância demonstram que a liberdade não pode ser garantida apenas por normas jurídicas formais, mas exige a construção de barreiras éticas, políticas e sociais contra a expropriação da experiência humana e a mercantilização da vida. Assim, proteger a privacidade hoje significa preservar a dignidade, a cidadania e a possibilidade de um futuro em que o indivíduo não seja reduzido a mero objeto de observação e controle.

2. UTILIZAÇÃO DAS FERRAMENTAS DIGITAIS

2.1. Regulamentação e controle de dados

A segurança privada vem sendo alvo de constantes debates devido ao avanço tecnológico e a crescente utilização de ferramentas digitais como câmeras de reconhecimento facial, sistemas de monitoramento e bancos de dados de acesso, em consequência, trouxe novos desafios para a proteção da privacidade e dos direitos fundamentais dos indivíduos. Nesse cenário, torna-se primordial compreender as normas Jurídicas brasileiras aplicáveis, especialmente o Marco Civil da Internet (Lei nº 12.965/2014) e a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018).

Enquanto o Marco Civil estabelece princípios gerais de uso da internet, como a proteção à intimidade, a privacidade e aos dados pessoais, a LGPD detalha os mecanismos e limites para o tratamento dessas informações, com especial atenção aos dados sensíveis, como os biométricos. A análise conjunta dessas normas é fundamental para compreender os limites legais da coleta e do uso de dados no setor de segurança privada, bem como para garantir um equilíbrio entre a eficiência dos serviços prestados e a proteção dos direitos dos usuários.

Acerca do Marco Civil da Internet (Lei nº 12.965/2014), pode-se dizer que ele surge como um marco normativo ao estabelecer os princípios que orientam o uso da rede no Brasil e são pilares regulatórios indispensáveis diante desta crescente digitalização de serviços e do monitoramento no âmbito da segurança privada.

Entre eles, destacam-se os princípios tratados no Art.3˚

> II - proteção da privacidade;
> III - proteção dos dados pessoais, na forma da lei;
> VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei; (Brasil, 2014).

Além disso, o diploma legal assegura aos usuários da internet o direito ao consentimento livre, expresso e informado para a coleta, utilização, armazenamento e tratamento de seus dados (art. 7º). Essa previsão é particularmente relevante para o setor da segurança privada, que frequentemente depende da captação de informações pessoais e, em muitos casos, de dados biométricos.

Concomitantemente, o Marco Civil impõe responsabilidades aos provedores de serviços quanto à segurança das informações e ao uso restrito dos dados coletados, limitando sua utilização apenas para as finalidades previamente autorizadas pelo titular. Assim, cria-se uma estrutura normativa que busca equilibrar o uso da tecnologia com a tutela dos direitos fundamentais.

Deste modo, a Lei 12.965, de 23 de abril 2014, foi a primeira legislação a regulamentar o uso da internet no Brasil, focada em estabelecer princípios, garantias, direitos e deveres para usuários da rede. Já a LGPD, é mais abrangente, e trata especificamente do tratamento de dados pessoais, com objetivo de proteger os direitos fundamentais de liberdade e privacidade dos cidadãos, garantindo que suas informações sejam devidamente utilizadas (Cardoso, 2024).

2.2. Tratamento de dados dos usuários

Os princípios estabelecidos pela LGPD trazem novas diretrizes e limitações sobre como os dados pessoais poderão ser tratados, de forma não exaustiva, tais princípios estabelecem um dever de transparência sobre como os dados pessoais são tratados dentro das respectivas organizações, os dados devem ser mantidos em segurança, e a organização que trata dos respectivos dados pessoais deve demonstrar o cumprimento dos requisitos previstos na lei (Thomaz, 2020).

A mesma Lei dispõe que as informações pessoais de indivíduos devem ser tratadas de acordo com parâmetros legais por empresas, sejam elas privadas ou públicas, independentemente da localização da sede ou do banco de dados. Assim, qualquer segmento empresarial que trabalhe com dados de clientes precisa se adequar à norma.

A lei define em seu art. 5º quais são os dados pessoais, dividindo-os em dois tipos: Dados pessoais sensíveis, que trata 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 e Dados pessoais, que tem relação com informações de pessoa natural identificada ou identificável (BRASIL, 2018).

O entusiasmo pelas novas práticas de vigilância não é consensual e há cada vez mais frestas sendo exploradas por aqueles que visam barrar ou regular formas de controle e monitoramento que se traduzem em práticas seletivas de segurança (Jefferson, 2020). A partir deste cenário, é imprescindível abordar o contexto da segurança privada e a utilização destes dados. À exemplo de locais com entrada controlada, que se utilizam de câmeras de segurança e dados biométricos para cadastro. Para o funcionamento e eficácia desse tipo de tecnologia, bases de dados vastas (*big data*) são essenciais para os sistemas de inteligência artificial e, frequentemente, os usuários não tem conhecimento do que será feito com estes dados.

2.3. Biometria e privacidade

Como forma de monitoramento, a biometria é a análise, realizada por meios matemáticos e estatísticos, das características físicas ou comportamentais de um indivíduo. Ela abrange o uso de uma variedade de técnicas e tecnologias para reconhecer uma pessoa por meio de suas características fisiológicas ou comportamentais (Cebrian, 2024). A biometria refere-se à detectar faces em imagens e vídeos, comparando o *template* de uma pessoa com as demais inseridas no sistema, por esta questão a base de dados vasta é fundamental.

Cumulativamente, em seu artigo 5º da LGPD, o dado biométrico é tido como 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 vinculados a uma pessoa natural (Brasil, 2018).

Um problema em potencial na utilização de identificação biométrica, é o risco de que erros causem constrangimentos às pessoas. Em situações envolvendo reconhecimento facial, após a detecção da face e análise do sistema, pode ocorrer um resultado equivocado que leve à identificação incorreta de alguém no pleno exercício de seus direitos civis e políticos, associando-o, por exemplo, a indivíduos sujeitos a medidas judiciais restritivas (EPRS, 2021a, p. 7). Ademais, fatores culturais, sociais e normativos presentes no processo de tratamento desses dados podem influenciar os algoritmos e modelos de aprendizado, ocasionando possíveis discriminações de natureza racial, social, étnica, econômica, entre outras.

Além de possíveis erros de identificação, existe o uso secundário de dados pessoais, referente ao processamento dessas informações para atingir objetivos diferentes daqueles que motivaram o tratamento inicial. Esse processamento posterior somente pode ocorrer quando houver compatibilidade entre a nova finalidade e a finalidade original, em conformidade com os princípios de finalidade e adequação previstos no art. 6º da LGPD, caso haja intenção de utilizar os dados para objetivos diversos daqueles que justificaram o tratamento inicial, é imprescindível avaliar se tal uso está em conformidade com a LGPD.

A análise do Marco Civil da Internet e da Lei Geral de Proteção de Dados Pessoais demonstra que o setor de segurança privada enfrenta desafios significativos diante da digitalização e de tecnologias avançadas, como reconhecimento facial e biometria. Essas ferramentas, embora aumentem a eficiência dos serviços, exigem rigoroso cumprimento das normas jurídicas para assegurar a proteção da privacidade e dos direitos dos indivíduos.

A fiscalização do cumprimento de tais normas é feita pela ANPD (Autoridade Nacional de Proteção de Dados), a qual estimula a adoção de comportamentos em conformidade com a LGPD. Fiscalizando todos os agentes de tratamento, desde que: A operação de tratamento esteja sendo realizada no território nacional; O tratamento tenha por objetivo a oferta de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou os dados pessoais tenham sido coletados no Brasil (ANPD, 2025).

É imprescindível que as empresas de segurança privada adotem práticas de governança de dados, garantindo transparência no tratamento das informações e implementando medidas técnicas e administrativas adequadas para prevenir violações. Assim, a conformidade normativa não apenas preserva os direitos dos cidadãos, mas também fortalece a credibilidade do setor, promovendo um equilíbrio entre inovação tecnológica e responsabilidade jurídica.

3 USO DE CÂMERAS E BIOMETRIA NO SETOR PRIVADO À LUZ DA LGPD

3.1 Aplicações em condomínios e empresas

O uso de tecnologias biométricas, sobretudo câmeras com reconhecimento facial, tem se disseminado no setor privado como promessa de maior segurança e praticidade. Em condomínios residenciais e comerciais, sistemas de controle de acesso substituem chaves e cartões por câmeras capazes de identificar moradores e visitantes. Nas empresas, a biometria é aplicada ao registro de ponto e à limitação de acesso a áreas restritas.

O setor privado tem intensificado o uso de tecnologias de identificação e biometria, como câmeras e sistemas de reconhecimento facial, para aprimorar a segurança, a eficiência e a gestão de fluxo. Essa expansão tecnológica está inserida no contexto da chamada "sociedade de controle" e do "capitalismo de vigilância" (OLIVEIRA e SILVA, 2024; MEIRELES, 2023), onde as experiências privadas dos indivíduos se tornam insumos valiosos para gerar lucro e vantagem mercadológica (Zuboff, 2019).

Contudo, o crescimento desse tipo de monitoramento provoca questionamentos éticos e jurídicos. Em muitos condomínios, os moradores não têm alternativa: para ingressar no edifício precisam fornecer sua biometria, o que transforma um dado sensível em requisito obrigatório de convivência. Segundo o IDEC (2023), essa prática é desproporcional, porque restringe direitos de escolha e impõe riscos que poderiam ser evitados com meios menos invasivos.

No contexto dos condomínios residenciais e comerciais, por exemplo, o uso de biometria para controle de acesso deve ser precedido de uma Análise de Risco e Proporcionalidade que demonstre que os objetivos de segurança não poderiam ser alcançados por métodos menos invasivos, como cartões ou QR codes. Conforme indicam Oliveira e Silva (2024), a exigência de dados biométricos em ambientes de convivência, sem alternativas razoáveis, pode configurar restrição desproporcional aos direitos fundamentais. Nesse mesmo sentido, o IDEC e o InternetLab (2020) ressaltam que, se não demonstrada a absoluta necessidade, a imposição da biometria representa limitação indevida aos direitos dos titulares.

A crítica também é filosófica. Michel Foucault (1983), ao tratar do panoptismo, descreveu a vigilância como mecanismo de disciplinamento social. Nos condomínios equipados com reconhecimento facial, o indivíduo se percebe constantemente observado, internalizando comportamentos moldados pela presença de câmeras. Shoshana Zuboff (2019), por sua vez, lembra que a coleta de dados em larga escala se insere na lógica do “capitalismo de vigilância”, em que a vida privada é transformada em matéria-prima para exploração econômica.

O CESeC (2023) acrescenta que o monitoramento biométrico não é neutro: ele pode ampliar desigualdades, uma vez que os sistemas de reconhecimento facial são mais propensos a falhas quando se trata de mulheres, pessoas negras e pessoas trans. Esse dado torna ainda mais preocupante a imposição desses sistemas em espaços privados, em que não há liberdade real para recusar o tratamento de dados.

3.2 Boas práticas e compliance com a LGPD

A Lei Geral de Proteção de Dados (Lei nº 13.709/2018) classifica dados biométricos como sensíveis (art. 5º, II), exigindo maior cautela em seu tratamento.

O marco legal brasileiro classifica os dados biométricos – como as características faciais e digitais capturadas por câmeras e leitores – como dados pessoais sensíveis (art. 5º, II, LGPD), em razão do seu elevado potencial de gerar riscos, como fraudes, estigmas e discriminação para o titular (ALMEIDA e SOARES, 2022). Em função dessa classificação, o tratamento desses dados exige uma base legal mais robusta e o cumprimento estrito dos princípios da Lei.
Para legitimar o uso, condomínios e empresas precisam se apoiar em bases legais específicas, como o consentimento explícito do titular (art. 7º, I) ou o legítimo interesse do controlador, desde que demonstrada a compatibilidade com os direitos fundamentais do titular e elaborados relatórios de impacto (art. 38).

Do ponto de vista da governança, a LGPD exige o cumprimento de princípios como finalidade, adequação, necessidade e minimização de dados (art. 6º). Isso significa que não é legítimo coletar mais dados do que o estritamente necessário, nem manter registros biométricos por prazo superior ao indispensável. Além disso, o art. 46 impõe o dever de adoção de medidas de segurança técnicas e administrativas para proteger tais dados contra acessos não autorizados.

Casos práticos mostram como o descumprimento dessas obrigações gera controvérsia. Academias e clubes, por exemplo, foram criticados por exigir a biometria como condição de acesso sem disponibilizar alternativa, prática que o IDEC classificou como abusiva (IDEC; InternetLab, 2023, p. 16-23). Da mesma forma, a Defensoria Pública de São Paulo recebeu reclamações de moradores de condomínios obrigados a fornecer seus dados faciais sem opção equivalente, situação que evidencia violação ao princípio do consentimento (CESeC; DPU, 2023, p. 2-4).

Além disso, a literatura especializada alerta para o risco de viés algorítmico. Bianca Kremer (2023) destaca que os erros em sistemas de reconhecimento facial não são exceções, mas sim “reproduções automatizadas de discriminações sociais preexistentes”. Esse ponto

conecta o debate jurídico ao campo dos direitos humanos, pois demonstra que a coleta biométrica em espaços privados pode reforçar práticas discriminatórias em vez de apenas gerar riscos difusos de privacidade.

Superadas as considerações sobre os limites éticos e sociais do uso da biometria, passa-se agora a examinar os riscos e responsabilidades jurídicas que recaem sobre os controladores desses dados.

3.3 Riscos e responsabilidades jurídicas

O uso inadequado de dados biométricos em condomínios e empresas pode gerar consequências jurídicas severas. O art. 42 da LGPD estabelece a responsabilidade objetiva do controlador pelos danos decorrentes do tratamento, independentemente de culpa. Isso significa que, havendo vazamento ou uso indevido dos dados, o condomínio ou a empresa poderá ser obrigado a indenizar o titular.

Um dos maiores riscos reside na imutabilidade do dado biométrico. Ao contrário de senhas ou chaves, que podem ser alteradas em caso de vazamento, os dados biométricos são permanentes, o que agrava as consequências de um incidente de segurança ou de uso indevido, tornando esse dado uma vulnerabilidade perene (ARTIGO 19, 2022). O controlador, seja ele o condomínio, o varejo ou a empresa de segurança, tem o dever de garantir a proteção, a criptografia e o não compartilhamento dessas informações para finalidades secundárias, evitando o desvio de finalidade.

A Autoridade Nacional de Proteção de Dados (ANPD) também pode aplicar sanções administrativas (art. 52 da LGPD), que vão desde advertências até multas de até 2% do faturamento da organização. Assim, a não conformidade representa risco não apenas reputacional, mas também financeiro.

O debate não é exclusivo do Brasil. O Parlamento Europeu (2021) classificou o reconhecimento facial à distância como tecnologia de alto risco, alertando que suas imprecisões “podem conduzir a resultados enviesados e ter efeitos discriminatórios”. Essa preocupação internacional reforça a necessidade de supervisão robusta em ambientes privados.

Na jurisprudência nacional, embora ainda incipiente no campo condominial, já se reconhece a ilicitude do uso da biometria sem consentimento. O Tribunal de Justiça de São Paulo tem condenado instituições bancárias ao pagamento de indenizações por falhas relacionadas a vulnerabilidades tecnológicas em sistemas de identificação. Exemplo disso foi o

caso em que o TJSP confirmou a condenação de um banco por falhas em seu sistema de segurança, impondo indenização por danos morais e materiais (TJSP, 2022).

Ainda que não envolva diretamente biometria em condomínios, esse precedente evidencia a crescente sensibilidade judicial quanto à responsabilidade por riscos tecnológicos. Nesse contexto, Doneda (2019) ressalta que a proteção de dados pessoais deve ser entendida como um direito fundamental autônomo, condição indispensável para a autodeterminação informativa e limite necessário às práticas abusivas de coleta e tratamento de dados. Complementarmente, estudo conduzido pela FGV (2024) reforça que os riscos específicos do uso da biometria — como vazamentos, reutilização indevida e falhas de segurança — impõem aos controladores o dever de adotar medidas proporcionais e cautelosas, sob pena de responsabilização civil e administrativa.

Dessa forma, a proteção de dados não deve ser reduzida a uma questão técnica, mas compreendida como elemento estruturante da cidadania. Aplicada ao setor privado, essa reflexão indica que a adoção de reconhecimento facial em condomínios e empresas só será legítima se equilibrar segurança e inovação com a preservação dos direitos fundamentais à privacidade, à igualdade e à dignidade humana (CF/88, art. 1º, III).

3.3.1 Biometria nas Relações Laborais: Subordinação e Direitos da Personalidade

No ambiente corporativo, a biometria é frequentemente utilizada para gestão de ponto eletrônico e controle de acesso a áreas restritas. Contudo, esse uso estabelece uma tensão permanente entre o poder diretivo do empregador e os direitos da personalidade do trabalhador.

A principal crítica jurídica concentra-se na validade do consentimento do empregado como base legal. Oliveira e Silva (2024) destacam que, em um contexto de subordinação hierárquica, o consentimento para a coleta de dados sensíveis (biometria) raramente é considerado livre e inequívoco, comprometendo a base legal. A recusa em fornecer o dado pode ser interpretada como um fator de risco ou insubordinação, limitando a autodeterminação informativa do titular.

A vigilância por meio de câmeras e biometria, quando excessiva ou desproporcional, pode violar o direito fundamental à privacidade e à dignidade da pessoa humana do trabalhador (OLIVEIRA e SILVA, 2024). Em função dessa controvérsia e do risco regulatório, algumas organizações têm optado por substituir os sistemas biométricos por alternativas menos invasivas, como cartões de acesso ou QR codes, em conformidade com o princípio da minimização dos dados (KREMER, 2023; CESeC e DPU, 2023).

A Autoridade Nacional de Proteção de Dados (ANPD) já se manifestou no sentido de que a aplicação dessas tecnologias pelo setor privado deve ser cautelosa, evitando usos que levem à discriminação. O uso de algoritmos de reconhecimento facial, por exemplo, é passível de erro e pode refletir e perpetuar aspectos discriminatórios, reforçando a necessidade de uma análise rigorosa do impacto na privacidade e nos direitos fundamentais dos titulares (ANPD, 2025; IDEC e INTERNETLAB, 2020).

Portanto, a biometria no ambiente laboral só se justifica quando estritamente necessária e proporcional, sob pena de violar não apenas a LGPD, mas também a própria dignidade da pessoa humana.

CONCLUSÃO

A análise desenvolvida evidencia que a privacidade não pode ser tratada apenas como proteção da intimidade, mas como requisito essencial para a autonomia individual e para a própria democracia. A partir de Mill, Arendt, Foucault e Zuboff, observa-se que o avanço tecnológico cria novas formas de controle que demandam limites éticos, jurídicos e políticos. A biometria, quando imposta sem alternativas, converte-se em violação de direitos fundamentais. No setor privado, a aplicação da LGPD é indispensável para assegurar transparência, proporcionalidade e minimização de dados. A adoção de boas práticas de governança da informação deve ser vista não apenas como obrigação legal, mas como pilar de cidadania e dignidade humana. Assim, o desafio contemporâneo consiste em compatibilizar segurança e inovação tecnológica com a preservação da liberdade, da igualdade e da dignidade, evitando que a sociedade se transforme em um grande panóptico digital. Em última análise, trata-se de um desafio civilizatório: assegurar que a inovação tecnológica caminhe lado a lado com a preservação da liberdade, da igualdade e da dignidade humana.

Referências

ALMEIDA, Siderly do Carmo Dahle de; SOARES, Tania Aparecida. Os impactos da Lei Geral de Proteção de Dados - LGPD no cenário digital. **Perspectivas em Ciência da Informação**, v. 27, n. 3, p. 26-45, jul./set. 2022.

ANAMELECHI, Ifeoma Uche. O panoptismo de Michel Foucault e as formas modernas de poder. **Revista Internacional de Filosofia**, v. 12, n. 2, p. 55-70, 2025.

ANPD. **Radar Tecnológico - nº 2: Biometria e Reconhecimento Facial.** Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/radar-tecnologico-biometria-anpd-1.pdf/view. Acesso em: 24 set. 2025.

ARENDT, Hannah. **A condição humana**. 13. ed. Rio de Janeiro: Forense Universitária, 2018.

ARAÚJO, Frederico; SILVA, João; SILVA JUNIOR, Marcos. Do panóptico da sociedade disciplinar aos dispositivos tecnopolíticos da sociedade de controle. **Revista de Direito, Estado e Tecnologia**, v. 5, n. 1, p. 105-120, 2021.

ARTIGO 19. **Quando corpos se tornam dados: tecnologias biométricas e liberdade de expressão**. Edição Brasileira: 2022. Disponível em: https://www.article19.org/wp-content/uploads/2023/06/Biometric-Report_Portuguese_13-06-23.pdf. Acesso em: 24 set. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Fiscalização. Brasília: ANPD, 2025. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/fiscalizacao-2. Acesso em: 24 set. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (Brasil). **Radar tecnológico: biometria e reconhecimento facial: estudos preliminares.** Fabiana S. P. Faraco Cebrian; Gustavo do Amaral Prudente; Marcelo Santiago Guedes; Maria Carolina Ferreira da Silva; Maria Luiza Duarte Sa; Thiago Guimarães Moraes. Brasília, DF: ANPD, 2024. (Radar tecnológico, n. 2).

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais.** Diário Oficial da União, Brasília, 15 ago. 2018.

BASTOS, Elísio Augusto Velloso; PANTOJA, Tiago Luis Souza; SANTOS, Sérgio Henrique Costa Silva dos. Os impactos das novas tecnologias da informação e comunicação no direito fundamental à privacidade. **Brazilian Journal of Development,** v. 7, n. 3, p. 29247-29267, 2021.

BOBBIO, Norberto. **A era dos direitos.** 6. ed. Rio de Janeiro: Campus, 1992.

BRANDÃO, Cláudio. O panoptismo e a normalização dos corpos em Michel Foucault. **Revista de Estudos Sociais,** v. 19, n. 40, p. 1-15, 2023.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Marco Civil da Internet.** Diário Oficial da União, Brasília, 24 abr. 2014.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais.** Diário Oficial da União, 15 ago. 2018.

CARDOSO, Caroline de Melo; RÉGIS, Jonathan Cardoso. Direito comparado: LGPD e o Marco Civil da Internet | **Comparative Law: LGPD and the Marco Civil Law. Revista de Direito,** Viçosa, v. 16, n. 1, 2024. DOI: https://doi.org/10.32361/2024160116495. ISSN 2527-0389.

CESeC; DPU. **Mapeando a vigilância biométrica.** Rio de Janeiro: CESeC/DPU, 2023.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** São Paulo: RT, 2019.

DUARTE, Daniel Edler; NUNES, Pablo; LIMA, Thallita G. L. **Estudos de vigilância.** Rio de Janeiro: CESeC, 2023. (Coleção Panorama).

DUARTE, Tatiana. Privacidade, liberdade e dignidade na sociedade contemporânea. **Revista de Filosofia e Política,** v. 8, n. 2, p. 45-62, 2020.

EUROPEAN PARLIAMENTARY RESEARCH SERVICE - EPRS, **Regulating facial recognition in the EU, 2021a.** Disponível em: Regulating facial recognition in the EU | Think Tank | European Parliament. Acessoe m 25 set. 2025.

FERREIRA, Daniela Assis Alves; PINHEIRO, Marta Macedo Kerr; MARQUES, Rodrigo Moreno. Privacidade e proteção de dados pessoais: perspectiva histórica. InCID: **Revista de Ciência da Informação e Documentação**, Ribeirão Preto, v. 12, n. 2, p. 151-172, set. 2021/fev. 2022. DOI: 10.11606/issn.2178-2075.v12i2p151-172.

FOUCAULT, Michel. **Vigiar e punir**: nascimento da prisão. 17. ed. Petrópolis: Vozes, 1983.

FUNDAÇÃO GETULIO VARGAS (FGV). **Biometria: Clínica de Direito Digital. White Paper.** São Paulo: FGV Direito SP, 2024.

IDEC; INTERNETLAB. **Reconhecimento Facial e o Setor Privado: Guia para a Adoção de Boas Práticas**. 2020. Disponível em: https://idec.org.br/sites/default/files/reconhecimento_facial_diagramacao_digital_2.pdf. Acesso em: 24 set. 2025.

JEFFERSON, Brian. **Digitize and Punish: Racial Criminalization in the Digital Age.** Minneapolis: University of Minnesota Press, 2020.

KOERNER, Andrei. Capitalismo e vigilância digital na sociedade democrática. **Revista Brasileira de Ciências Sociais**, v. 36, n. 105, p. 1-12, 2021. DOI: 10.1590/3610514/2020.
MILL, John Stuart. **Sobre a liberdade**. São Paulo: Companhia das Letras, 2010.

KREMER, Bianca. **Racismo Algorítmico.** Rio de Janeiro: CESeC, 2023.

MEIRELES, Adriana Veloso. Privacidade no século 21: proteção de dados, democracia e modelos regulatórios. **Revista Brasileira de Ciências Sociais**, v. 38, n. 112, 2023.

MILL, John Stuart. **Sobre a liberdade.** São Paulo: Companhia das Letras, 2010.

OLIVEIRA, Lourival José de; SILVA, Fabiano Fernando da. Biometria Facial e Tecnologias de Monitoramento à Luz dos Direitos da Personalidade do Trabalhador. **Revista da Faculdade de Direito da UFMG,** v. 84, p. 265-284, 2024.

PARLAMENTO EUROPEU. **Resolução legislativa sobre a proposta de regulamento em matéria de inteligência artificial (AI Act).** Bruxelas: Parlamento Europeu, 2021.

QUEIROGA, Rodrigo Alves de. O dispositivo do panóptico em Michel Foucault aplicado aos dispositivos do mundo virtual. **Revista de Filosofia da UNILA**, v. 5, n. 2, p. 1-20, 2022.

TRIBUNAL DE JUSTIÇA DE SÃO PAULO (TJSP). Banco deve indenizar cliente vítima de golpes por falha em sistema de segurança. São Paulo, 16 mar. 2022. Disponível em: https://www.tjsp.jus.br/Noticias/Noticia?codigoNoticia=93287. Acesso em: 28 set. 2025.

THOMAZ, Alan Campos Elias. Privacidade e proteção de dados na indústria financeira. In: PALHARES, Felipe (org.). **Temas Atuais de Proteção de Dados.** São Paulo: RT, 2020.

ZUBOFF, Shoshana. **A Era do Capitalismo de Vigilância.** Rio de Janeiro: Intrínseca, 2019.