INSTITUTO BRASILEIRO DE ENSINO, PESQUISA E DESENVOLVIMENTO
ESCOLA DE DIREITO E ADMINISTRAÇÃO PÚBLICA
MESTRADO ACADÊMICO EM DIREITO CONSTITUCIONAL

ANDRÉ DAMAS DE MATOS

A EXPEDIÇÃO DE MANDADOS DE GEOLOCALIZAÇÃO E SUA TENSÃO COM OS DIREITOS FUNDAMENTAIS

BRASÍLIA
2025

ANDRÉ DAMAS DE MATOS

A EXPEDIÇÃO DE MANDADOS DE GEOLOCALIZAÇÃO E SUA TENSÃO COM OS DIREITOS FUNDAMENTAIS

Dissertação de Mestrado, desenvolvida sob a orientação da Professora Dra. Clara Iglesias Keller.

BRASÍLIA

2025

Código de catalogação na publicação – CIP

M433e Matos, André Damas de

A expedição de mandados de geolocalização e sua tensão com os direitos fundamentais / André Damas de Matos. — Brasília: Instituto Brasileiro Ensino, Desenvolvimento e Pesquisa, 2025.

173 f. : il. color.

Orientador: Profª. Drª. Clara Iglesias Keller

Dissertação (Mestrado Acadêmico em Direito Constitucional) — Instituto Brasileiro Ensino, Desenvolvimento e Pesquisa – IDP, 2025.

1. Direito à privacidade. 2. Investigação criminal - provas - Brasil. 3. Marco civil da internet - Brasil. I.Título

CDDir 341.2732

Elaborada por Natália Bianca Mascarenhas Puricelli – CRB 1/3439

ANDRÉ DAMAS DE MATOS

A EXPEDIÇÃO DE MANDADOS DE GEOLOCALIZAÇÃO E SUA TENSÃO COM OS DIREITOS FUNDAMENTAIS

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação *Stricto Sensu* em Direito como requisito para obtenção do título de mestre em Direito Constitucional.

Data da Defesa: 30 de junho de 2025

BANCA EXAMINADORA

Professora Orientadora Dra. Clara Iglesias Keller
Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa-IDP

Professor Dr. Rodrigo Frantz Becker
Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa-IDP

Professor Dr. Ivar Alberto Glasherster Martins Lange Hartmann
Insper Instituto de Ensino e Pesquisa

À minha mãe, minha primeira educadora, que me ensinou com paciência e firmeza o valor do conhecimento, da honestidade e do cuidado. Muito do que sou começou nas suas mãos.

Ao meu pai, meu amigo, conselheiro e exemplo mais próximo de força, tranquilidade e generosidade; se continuo tentando ser melhor, é por tudo que aprendi ao seu lado.

À minha família, base constante da minha vida, razão de cada esforço e motivação maior de todos os meus atos. Este trabalho também é de vocês.

RESUMO:

O trabalho tem como foco examinar os aspectos constitucionais e legais relacionados ao fornecimento de dados pessoais para fins de individualização de cidadãos em investigações criminais mediante mandados de geolocalização, sob a perspectiva dos direitos à intimidade, à privacidade e à proteção de dados. Analisa-se o contexto de lacunas normativas no ordenamento jurídico brasileiro quanto à regulamentação específica para emissão desses mandados, o que tem exigido do Poder Judiciário a recorrer aos artigos 10 e 22 do Marco Civil da Internet (Lei n.º 12.965/2014) como base para autorizar esse tipo de medida investigativa. Ademais, o estudo discute o tensionamento existente entre os interesses relacionados à persecução penal e à segurança pública e a tutela dos direitos fundamentais. Aponta-se, ainda, para os riscos associados à normalização do acesso e do compartilhamento dessas informações, com reflexo na conformidade constitucional e na preservação da esfera privada e da dignidade dos indivíduos, em um cenário marcado pelo avanço das tecnologias e pelo fortalecimento de mecanismos de vigilância estatal.

Palavras-chave: Direitos da personalidade. Investigação criminal. Mandados de Geolocalização. Marco Civil da Internet. Proteção de dados.

ABSTRACT:

The research focuses on examining the constitutional and legal aspects related to the disclosure of personal data for the purpose of identifying individuals in criminal investigations through geolocation warrants, from the perspective of the rights to intimacy, privacy, and data protection. It analyzes the normative gaps within the Brazilian legal framework regarding specific regulations for the issuance of such warrants, which has led the Judiciary to rely on Articles 10 and 22 of the Brazilian Internet Bill of Rights (Law No. 12.965/2014) as a basis for authorizing this type of investigative measure. Furthermore, the study explores the tension between the interests of criminal prosecution and public security and the safeguarding of fundamental rights. It also highlights the risks associated with the normalization of access to and sharing of such information, raising concerns about constitutional conformity and the preservation of individuals' private sphere and dignity in a context marked by technological advancement and the strengthening of state surveillance mechanisms.

Keywords: Personality rights. Criminal investigation. Geolocation warrants. Brazilian Internet Bill of Rights. Data protection.

LISTA DE FIGURAS

SUMÁRIO

INTRODUÇÃO

1. APRESENTAÇÃO DO TEMA

O presente trabalho visa abordar o debate acerca da constitucionalidade dos mandados judiciais que delimitam o perímetro geográfico, em data e horário determinados, e requisitam o fornecimento de dados pessoais, inclusive aqueles denominados sensíveis, capazes de individualizar os cidadãos que estiveram na localidade durante o período fixado. Comumente denominadas *mandados de geolocalização ou geofence warrants*, essas ordens judiciais são expedidas sem o conhecimento prévio dos indivíduos afetados e dirigidas a empresas que detêm dados de localização por distintas vias técnicas, como registro de conexões com Estação Rádio Base (ERB's), no caso das operadoras de telefonia, ou por meio de coleta de dados em aplicativos e serviços digitais, no caso das empresas chamadas *big techs*[1].

Independentemente da fonte ou tecnologia de obtenção, o traço distintivo desses mandados é a requisição de informações relativas ao universo indeterminado de pessoas, muitas das quais sem qualquer vínculo de pertinência com a investigação em curso, o que suscita relevantes questionamentos sob a ótica dos direitos e garantias fundamentais. Embora a geolocalização possa ser adotada em diversos procedimentos judiciais como meio de produção de prova, para o fim proposto deste estudo, o tratamento dos dados obtidos pelos *geofence warrants* serviria para lastrear investigação criminal, visando, em tese, buscar a confirmação da autoria delitiva.

Dessa forma, a análise da constitucionalidade e legalidade da expedição dos mandados de geolocalização é realizada à luz da possível afronta aos direitos fundamentais à inviolabilidade da vida privada, à proteção da intimidade e, consequentemente, à dignidade da pessoa humana, todos assegurados pela Constituição Federal de 1988, em seu 5º, inciso X. Mais recentemente, com a promulgação da Emenda Constitucional n.º 115/2022, que consagrou a proteção de dados pessoais, inclusive no ambiente digital, como direito fundamental, por meio do art. 5º, inciso LXXIX da CF/88, essa discussão passou a adquirir uma nova densidade jurídica. A incorporação desse direito à proteção de dados reforça a necessidade de reavaliar os parâmetros constitucionais que regulam o acesso e o tratamento de informações pessoais no contexto das investigações criminais.

[1] A revista Forbes atribui ao jornal francês Le Monde a origem da nomenclatura Big Techs destinada a se referir às empresas do setor de tecnologia Google, Amazon e Meta, antiga Facebook. Sítio eletrônico: https://forbes.com.br/forbes-tech/2023/02/o-que-difere-as-big-techs-de-outras-empresas-de-tecnologia/. Acesso em 17 de setembro de 2023.

Estes direitos fundamentais, assegurados no bojo da Constituição Federal de 1988, impõem limites claros à interferência estatal na esfera privada dos indivíduos, e seus princípios permeiam os normativos infraconstitucionais que disciplinam a proteção da personalidade e dos dados pessoais. Nessa linha, a Lei Geral de Proteção de Dados (LGPD), editada após trinta anos da Carta Magna, em 2018, acrescentou novas camadas de segurança no tratamento de dados. Todavia, a novel lei possui restrições materiais a sua aplicabilidade no seu próprio texto, como disposto no seu artigo 4º que afasta sua disciplina quando o tratamento de dados tiver como finalidade a segurança pública ou do Estado e, principalmente, para *atividades de investigação e repressão de infrações penais*. Logo, tem-se que a LGPD, embora impregnada com os princípios voltados à salvaguarda dos dados, não se trata de um normativo que alcance diretamente o uso de dados geográficos no contexto das investigações criminais. De tal forma, a geolocalização se apresenta como uma tecnologia relevante e robusta no levantamento de informação dos cidadãos, porém controversa, que demanda uma análise aprofundada sobre sua compatibilidade com os direitos constitucionais.

A controvérsia em torno da utilização da geolocalização se estrutura a partir de duas perspectivas distintas quanto ao uso dessa ferramenta. A primeira delas insere-se no campo da proteção dos direitos da personalidade, especialmente o direito à privacidade e autodeterminação informativa, haja vista a preocupação com o simples potencial de o Estado acessar dados pessoais anteriormente produzidos pelos cidadãos ou, ainda, obtidos por meio do cruzamento de um amplo espectro de informações. Embora esses dados tenham sido legal e legitimamente gerados, o receio reside na possibilidade de que sua reengenharia reversa configure uma forma de vigilância perene.

Dada a amplitude do tema e da diversidade de implicações jurídicas envolvidas, impõe-se a delimitação do objeto da pesquisa, com vistas a preservar a coerência metodológica e permitir a concentração analítica na resposta ao problema a ser formulado. O recorte temático adotado restringe o estudo aos mandados judiciais de geolocalização voltados à obtenção de dados pretéritos, ou seja, àqueles que buscam informações relativas à localização geográfica de um dispositivo em momento anterior à data da decisão judicial. Consiste em um instrumento voltado à reconstrução de fatos já ocorridos, muitas vezes com o objetivo de esclarecer circunstâncias de um crime em investigação. Logo, excluem-se os mandados com efeitos prospectivos, isto é, aqueles que eventualmente autorizariam o monitoramento em tempo real ou a vigilância contínua de determinado espaço geográfico, os quais, por sua natureza, envolveriam discussões teóricas e práticas distintas ou oblíquas que extrapolariam os limites da presente proposta.

Os efeitos prospectivos da geolocalização guardam estreita relação com práticas de vigilância estatal ou *surveillance* permanente, aliadas aos denominados métodos de policiamento orientado por dados, conhecidos como *predictive policing.* Este fenômeno *da criminalização preditiva*, a qual pressupõe a adoção de medidas que visam antecipar comportamentos com base em padrões estatísticos, levanta questões éticas e acerca da compatibilidade do modelo constitucional garantista, especialmente no que se refere à presunção de inocência, considerando, ainda, o enviesamento da programação algorítmica[2].

Ademais, o monitoramento prospectivo pode culminar na configuração do flagrante preparado, situação em que as autoridades policiais, embora não induzam o agente à prática do crime, planejam e controlam previamente toda a execução dos atos delituosos, de modo que a consumação se torna inviável desde o início. Nessa hipótese, o bem jurídico protegido nunca esteve efetivamente sob risco, caracterizando-se como crime impossível, diante dessa ausência de lesão ou ameaça. A vedação a esse tipo de flagrante encontra respaldo na Súmula 145 do Supremo Tribunal Federal, segundo a qual "*não há crime quando a preparação do flagrante pela polícia torna impossível a sua consumação*"[3], reafirmando a necessidade de controle da atividade estatal no âmbito penal[4].

Por outro lado, o uso da geolocalização como mecanismo de vigilância para monitoramento eletrônico do cumprimento de medidas judiciais, estatuído na Lei n.º 12.258/2010, também será excluída do objeto deste estudo. Essas aplicações, embora juridicamente relevantes, apresentam função diversa daquela que investigada. É o caso, por exemplo, da utilização de dados de localização para fiscalização do cumprimento de medidas cautelares diversas da prisão, como as medidas protetivas impostas com base na Lei Maria da Penha ou, ainda, no contexto da execução penal, para garantir o cumprimento das condições dos regimes mais brandos, como semiaberto e domiciliar. Essas hipóteses, embora envolvam tecnologia de rastreamento, relacionam-se a mecanismos de controle judicial da liberdade já restringida ou condicionada e não à obtenção de elementos informativos para fins probatórios e investigação criminal propriamente dita.

Ao delimitar o estudo aos mandados de localização de natureza retrospectiva, busca-se evitar a dispersão da proposta teórica, resguardando a precisão conceitual e o rigor analítico

---

[2] FREITAS, Marcio Luiz Coelho de, **Privacidade no Direito Penal e o dilema da vigilância na era digital: a regulação da internet como instrumento de tutela de direitos fundamentais**, Tese de Doutorado, Universidade de Brasília, Brasília, 2022.

[3] BRASIL. Supremo Tribunal Federal. **Súmula n.º 145**. Disponível em: https://portal.stf.jus.br/jurisprudencia/sumariosumulas.asp?base=30&sumula=2119. Acesso: 30 mai. 2025.

[4] LOPES JR., Aury, Direito Processual Penal, 22. ed. Rio de Janeiro: SRV, 2025, p. 748.

necessários à construção da resposta ao problema de pesquisa. Visa-se, com isso, distinguir, com base em critérios normativos e funcionais, o uso da geolocalização como medida de reconstrução probatória de fatos passados do seu emprego no instrumento de vigilância estatal ou de execução penal, cuja análise demandaria tratamento específico e abordagens metodológicas próprias.

Essa linha argumentativa baseia-se na compreensão de que a vida privada está sendo progressivamente restringida por mecanismos de monitoramento cujos alcances e implicações não são plenamente compreendidos pela maioria da população. Portanto, consiste em uma crítica à banalização da vigilância em contextos democráticos, principalmente em face do avanço tecnológico e da expansão das capacidades de tratamento de dados por entidades públicas e privadas.

O segundo enfoque relacionado ao uso de mandados de geolocalização em processos criminais diz respeito ao seu fundamento legal, aos requisitos formais e ao momento processual adequado para a solicitação do levantamento dos dados pessoais. Por óbvio, ainda que a colisão entre os princípios fundamentais da dignidade da pessoa humana e da segurança pública, como ilustrado anteriormente, seja constante nesse debate, resta perquirir se, superado esse primeiro plano desse conflito, a utilização desses mandados observa as garantias processuais criminais.

A questão central, desta forma, consiste em saber se os mandados de geolocalização se configuram como instrumentos idôneos a dar suporte a investigações já devidamente instauradas ou se estariam sendo utilizados de forma antecipada e generalizada, como meios autônomos de produção de prova potencialmente convertendo-se na origem da justa causa para a persecução penal. Essa hipótese suscita sérias preocupações quanto ao risco de naturalização da medida e a sua eventual transformação em verdadeira expedição aleatória de elementos de prova.

Não obstante o ordenamento jurídico brasileiro não dispor de uma regulamentação ampla e sistemática sobre o uso de dados de geolocalização para fins de persecução penal, há previsão normativa pontual, de caráter excepcional, na Lei n.º 13.344/2016. Esse diploma, ao incluir o art. 13-B[5] no Código de Processo Penal, autoriza, no contexto do enfrentamento ao tráfico de pessoas, a requisição, por autoridades competentes, de informações, sinais e recursos

[5] BRASIL. **Decreto-Lei nº 3.689**, de 3 de outubro de 1941. Código de Processo Penal. "Art. 13-B: Se necessário à prevenção e à repressão dos crimes relacionados ao tráfico de pessoas, o membro do Ministério Público ou o delegado de polícia poderão requisitar, mediante autorização judicial, às empresas prestadoras de serviço de telecomunicações e/ou telemática que disponibilizem imediatamente os meios técnicos adequados – como sinais, informações e outros – que permitam a localização da vítima ou dos suspeitos do delito em curso".
Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 6 maio 2025.

técnicos que possibilitem a identificação da posição da vítima ou dos suspeitos durante a prática delitiva. Ressalta-se, contudo, que essa previsão normativa se aplica apenas a casos específicos e tem como fundamento a urgência da situação investigada, estando voltada à proteção da integridade física da vítima em situações de flagrante e privação de liberdade. Outrossim, a redação do mencionado dispositivo delimita que a obtenção desses dados se refere, em regra, ao *Cell-Site Location Information (CSLI),* isto é, aos registros de conexão do aparelho celular à Estação Rádio Base mais próxima, técnica de geolocalização que apresenta acurácia limitada, especialmente em regiões com baixa densidade de torres. A técnica de triangulação entre múltiplas torres, ainda que mais precisa, demanda infraestrutura adicional e, em regra, não está abrangida automaticamente pela autorização legal do art. 13-B do CPP.

De igual forma, não é incomum que decisões judiciais também adotem o artigo 22[6] do Marco Civil da Internet (Lei n.º 12.965/2014), como fundamento para a concessão de mandados de geolocalização. Ressalta-se que a prescrição do artigo citado possibilita a requisição judicial de registros de conexão e de acesso a aplicações de internet, bem como de dados cadastrais, os quais não contemplam os dados de localização em tempo real ou histórico, sobretudo aqueles derivados de tecnologias como GPS, triangulação de ERB's ou Wi-Fi *tracking*.

Cabe destacar, desde já, que os aspectos técnicos relacionados às diferentes formas de geolocalização, como o CSLI, a triangulação por ERB's e a coleta de dados via GPS, Wi-Fi, o Bluetooth por plataformas digitais, serão objeto de exame detalhado em capítulo próprio.

Emerge relevância na análise crítica da relação entre a precisão técnica dos métodos utilizados e o grau de intrusão nos direitos fundamentais à privacidade e à proteção de dados pessoais. Técnicas como o *Cell-Site Location Information (CSLI),* baseadas no registro passivo da conexão do dispositivo móvel à Estação Rádio Base mais próxima, possui um grau relativamente baixo de acurácia, o que resulta na delimitação de áreas geográficas mais amplas e imprecisas. Essa imprecisão, por sua vez, pode levar à inclusão de um número elevado de pessoas alheias à investigação criminal, ampliando sobremaneira os efeitos colaterais da medida sobre indivíduos sem qualquer vínculo com o fato delituoso.

[6] BRASIL. **Lei nº 12.965**, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Art. 22**. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet. Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade: I - fundados indícios da ocorrência do ilícito; II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e III - período ao qual se referem os registros. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 26 maio 2025.

Em contraposição, métodos mais sofisticados, com uma triangulação ativa entre múltiplas torres, uma coleta de dados oriundos de GPS, redes Wi-Fi e sinais Bluetooth, oferecem maiores exatidão na individualização da localização dos dispositivos móveis, mas implicam uma devassa mais intensa sobre a esfera privada dos titulares dos dados. Essa dualidade revela um impasse normativo: enquanto métodos menos invasivos demandam uma coleta mais abrangente e, portanto, mais indiscriminada, para alcançar a efetividade investigativa, os métodos mais precisos tornam-se, por sua própria natureza, mais sensíveis do ponto de vista jurídico-constitucional, exigindo, como consequência, critérios mais estritos de legalidade, necessidade e proporcionalidade.

No acompanhamento das discussões ocorridas entre os Ministros do Supremo Tribunal Federal durante o julgamento do Tema 1148, observou-se a recorrente menção aos requisitos esculpidos na Lei de Interceptação Telefônica, Lei n.º 9.296/96, para promover o juízo de adequação e necessidade dos fundamentos dos mandados de fornecimento de dados de geolocalização, como, por exemplo, a inexistência de outros meios disponíveis para obtenção da prova e gravidade do crime investigado. Todavia, esta lei ordinária, como o seu próprio preâmbulo aduz, tem a finalidade de regular o inciso XII, parte final, do art. 5º da Constituição Federal, o qual assegura o sigilo de comunicações telefônicas e de dados, e não abrange, de forma direta, o tratamento de dados pessoais sensíveis e os dotados de maior grau de intimidade, como os de geolocalização. Em seu turno, o artigo 22 da Lei n.º 12.965/2014 versa apenas sobre o registro de conexão e registros de aplicação na internet, cuja invocação como fundamento para concessão de mandados dessa natureza implica ampliação interpretativa que desconsidera as particularidades dos dados de geolocalização, bem como as limitações técnicas, as quais são reflexo da própria conceituação trazida pela norma.

Assim, a compatibilidade do deferimento de mandados de geolocalização com os preceitos constitucionais deve ser analisada à luz da proteção de dados pessoais, direito fundamental esculpido no artigo 5º, inciso LXXIX, da Constituição Federal, inserido pela Emenda Constitucional nº 115/2022. Ainda que a coleta de dados provenientes de plataformas digitais ou sinais via ERB’s possa, em determinadas circunstâncias, ser legítima, especialmente em hipótese de urgência ou risco à vida, o uso dessa técnica investigativa fora dessas hipóteses, e sem lei específica que estabeleça limites, salvaguardas e controle judicial rigoroso, pode configurar afronta à privacidade, à proteção de dados e à dignidade da pessoa humana.

Igualmente, por pertinência à delimitação do objeto a ser apreciado, cabe recordar que o período de redemocratização brasileira, marcado pela promulgação da Constituição Federal de 1988, representou uma mudança de paradigma nos procedimentos criminais. Essa

transformação foi particularmente relevante quanto à identificação de autoria, carreados nos autos de persecução penal estatal.

Antes da Carta Magna Cidadã, a obrigatoriedade de o investigado, no jargão policial, "tocar piano" era observada em face do rigor do artigo 6º, inciso VIII, do Código de Processo Penal de 1941, cujo comando normativo determinava à autoridade policial a proceder com a identificação do indiciado por meio do processo datiloscópico. Nesse mesmo diapasão, o Supremo Tribunal Federal editou[7], em 15 de dezembro de 1976, o enunciado n.º 568 de sua Súmula, sedimentando o entendimento no sentido de não ser configurado constrangimento ilegal a realização da identificação criminal, mesmo que o suposto autor estivesse civilmente identificado.

As teses guerreadas nas decisões judiciais, até então, não descolavam do contexto histórico do regime político militar instaurado entre os anos de 1964 e 1985, no qual a preponderância do Estado policialesco impunha, por obviedade, uma prevalência do princípio da segurança pública sobre os direitos fundamentais da liberdade, intimidade e de privacidade, sendo estes, por vezes, inclusive, frontalmente violados.

Não obstante estes precedentes desfavoráveis à proteção dos direitos da personalidade, compulsando as decisões da Suprema Corte Brasileira que ensejaram a edição do citado enunciado, por exemplo, no voto vencido proferido pelo Ministro Rodrigues Alckmin, no Recurso Extraordinário n.º 80.732/DF, verificam-se presentes os alicerces de ponderações acerca do caráter vexatório aos indivíduos na realização da identificação criminal. Tem-se, portanto, uma sinalização do reestabelecimento do núcleo de proteção do princípio da dignidade da pessoa humana fulcrado no indivíduo.

Ressalta-se que o direito da personalidade tem como atributo ser irrenunciável e intrínseco à existência do sujeito, tornando-o destinatário de respeito pelo Estado e demais membros da sociedade. Estas características obstam que estes demais agentes possam realizar atos ou tratamento degradantes e desumanos, bem como agir de forma que impeça ou limite a participação ativa do titular desse direito em sua comunidade[8]. Estes ideais presentes nesse conceito, os quais merecem constante revisitação para os seus aprimoramentos, foram encampados pela Assembleia Constituinte e resultaram na positivação da vedação da obrigatoriedade de identificação criminal aos civilmente identificados, salvo nas hipóteses

[7] BRASIL. Supremo Tribunal Federal. **Súmula n. 568**: " A identificação criminal não constitui constrangimento ilegal, ainda que o indiciado já tenha sido identificado civilmente" Disponível em: https://jurisprudencia.stf.jus.br/pages/search/seq-sumula568/false. Acesso em 24 abril 2024.

[8] SARLET, Ingo Wolfgang, **A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional**, 10. ed. Porto Alegre: Livraria do Advogado, 2009.

legais, cuja redação encontra-se estampada no inciso LVIII da CF/88: "*O civilmente identificado não será submetido a identificação criminal, salvo nas hipóteses previstas em lei*."

Este breve recorte temporal visa demonstrar que a relação de equilíbrio entre os princípios fundamentais relacionados aos direitos da personalidade, por vezes, experimenta viés de submissão em cotejo com princípios atrelados à segurança pública e defesa da coletividade. Contudo, este cenário provoca verdadeiro substrato para o fenômeno de *backlash* constitucional a suscitar o debate democrático, culminando em avanços quando há um diálogo mais estreito entre as manifestações judiciais, os movimentos sociais e a própria Constituição[9].

2. JUSTIFICATIVA DA PESQUISA

Busca-se perquirir até que ponto o uso de tecnologia empregada em técnicas de geolocalização em investigação criminal por parte das autoridades estatais está em conformidade com as garantias constitucionais previstas, especialmente aquelas que protegem a dignidade da pessoa humana. O presente estudo se torna, assim, pertinente na avaliação das garantias de que os métodos de investigação respeitem os direitos fundamentais dos cidadãos, em vez de se transformarem em instrumentos de controle desproporcional ou invasivo.

É inegável o avanço dos recursos tecnológicos na vida cotidiana e os impactos provocados nas relações sociais. Contudo, não é a primeira vez que se observa o fenômeno da influência das novas tecnologias na vida humana. Marshall Mcluhan[10], em sua obra: *Os meios de comunicação como extensões do homem,* já refletia sobre como a massificação dos meios de comunicação e a Era Eletrônica elevam o ser humano a uma nova realidade, ampliando o uso sensorial, como o tátil e auditivo, e remodelando agrupamentos e relações sociais. Haveria, portanto, uma ruptura dos paradigmas de meios de produção estritamente mecânicos em face da automação e o imediatismo das conexões propiciadas pelos sistemas elétricos. O que outrora foi modificado em virtude da inserção da tecnologia mecânica, como na Revolução Industrial, hodiernamente, é afetado pelo universo digital. O autor ainda destaca que estas mudanças se tornam imperceptíveis a partir do momento em que as pessoas perdem a capacidade de compreender que o "*meio é a mensagem*"[11].

---

[9] ZAGURSKI, Adriana Timoteo Dos Santos, **Backlash: Uma Reflexão Sobre Deliberação Judicial Em Casos Polêmicos**. REVISTA DA AGU, 2017.
[10] MCLUHAN, Marshall, **Os meios de comunicação: como extensões do homem**, [s.l.]: Editora Cultrix, 1974.
[11] *Ibid*.

A ausência da adequada dimensão dos valores associados aos dados pessoais e o potencial econômico intrínseco à exploração dessas informações[12] tornam necessária a análise sobre de que forma esses dados, por vezes sensíveis, podem ser captados e tratados. A crescente solicitação por autoridades estatais acerca da utilização de tecnologias de geolocalização nas investigações criminais exige a necessidade de reavaliar os limites constitucionais e os mecanismos de controle que regem a atuação estatal no âmbito das investigações quando estes meios são adotados.

Igualmente, o enfoque dessa dissertação reside na necessidade de se avaliar os desafios legais e sociais diante das novas tecnologias de vigilância, que podem ensejar a banalização da coleta de dados pessoais, de modo que seu resultado apresente as formas de o Estado Democrático de Direito seja adequadamente atuante em sua função garantidora das liberdades individuais em um ambiente cada vez mais digitalizado. Ao ponderar acerca da legalidade e a constitucionalidade dos procedimentos de geolocalização, o projeto não só contribui para a proteção dos direitos da personalidade, mas também reforça a importância de um sistema jurídico que esteja em constante adaptação aos novos desafios tecnológicos.

Por outro lado, admite-se que, no período da promulgação da Constituição de 1988, a efetivação do princípio do sigilo das comunicações e da não autoincriminação relacionava-se à proteção da exteriorização das informações produzidas por um indivíduo. Naquela época, seria adequado se considerar que a comunicação com terceiros fosse a única forma de produção espontânea de informação capaz de ser utilizada contra o próprio cidadão. Porém, atualmente, com a digitalização das informações e prestação de serviços, as atividades rotineiras produzem informação analisada por algoritmos sofisticados capazes de transformá-la em padrão e previsibilidade de comportamento, antecipação de necessidades, reforço de percepção, como a própria política por exemplo.

Essa configuração da limitação ao direito de não autoincriminação cogitada deve considerar a precária compreensão dos cidadãos que a transmissão e troca de dados com as operadoras de telefonia transcende o aspecto individual. Atualmente, as atividades relacionadas à prestação de serviços de telecomunicações são consideradas uma espécie de contrato existencial, uma vez que estão atrelados a valores atinentes à dignidade da pessoa humana[13] que necessita dos meios de comunicação e produção de dados, inclusive para exercício pleno

[12] ZUBOFF, Shoshana. **Big Other: Surveillance Capitalism and the Prospects of an Information Civilization.** Journal of Information Technology. v. 30, p. 75–89. 2015.
[13] AZEVEDO, Antonio Junqueira. **Entrevista: Antonio Junqueira de Azevedo. RTDC: Revista Trimestral de Direito Civil.** v. 9, n. abr./jun. 2008. p. 299–308, 2008.

da cidadania digital, seja para demandar serviços da Administração Pública, seja para exercício do sufrágio ou, ainda, o uso responsável das ferramentas de tecnologia[14]. Assim, o uso dos meios de comunicação torna-se indissociável da vida privada das pessoas e os dados produzidos no núcleo de sua intimidade deveriam ser preservados, considerando este aspecto essencialmente individual.

Logo, o presente trabalho tem o intuito de contribuir com subsídios a literatura jurídica, propondo uma análise acerca da constitucionalidade e a legalidade dos mandados de geolocalização. Além disso, pretende-se fomentar o debate sobre quais requisitos devem ser observados para legitimar uso e tratamentos de dados pessoais nas investigações criminais, sem que haja a violação aos direitos individuais no contexto de uma sociedade contemporânea cada vez mais dependente de dados digitais.

O evento relevante que ensejou a análise do tema suso estabelecido foi a publicação da decisão proferida pelo Ministro do Supremo Tribunal Federal, Alexandre de Moraes, no bojo do Inquérito n.º 4.879/DF[15], em face dos atos atentatórios à Democracia Brasileira e de vandalismo perpetrados aos edifícios sedes dos Três Poderes da República, em Brasília/DF, no dia 8 de janeiro de 2023.

A referida decisão no Inquérito n.º 4.879/DF traz as razões de decidir do Ministro Alexandre de Moraes que acolheu requerimentos da Advocacia-Geral da União e do Senador da República Randolfe Rodrigues, nos quais eram solicitadas medidas acautelatórias das investigações criminais. Esses pedidos se baseavam na necessidade premente de assegurar a investigação e adequação de medidas ante a gravidade das condutas típicas descritas nos artigos 2ª, 3º, 5º e 6º (atos terroristas da Lei nº 13.260, de 16 de março de 2016 e nos artigos 288 (associação criminosa), 359-L (abolição violenta do Estado Democrático de Direito) e 359-M (golpe de Estado), 147 (ameaça), 147-A, § 1º, III (perseguição), 286 (incitação ao crime), além de dano ao patrimônio público (artigo 163, III) todos do Código Penal Brasileiro.

Não obstante o noticiado deferimento de algumas medidas solicitadas, verifica-se, no corpo do *decisium*, que o requerimento do órgão de assessoramento jurídico da União desejava ampliar o espectro investigativo com o intuito de obter informações necessárias à individualização das pessoas presentes na Praça dos Três Poderes naquele dia 08 de janeiro de 2023. Esse requerimento pleiteava justamente que o Ministro Alexandre de Moraes

[14] NUNES, D. H.; DE SOUZA LEHFELD, L. C.. **Cidadania Digital: Direitos, Deveres, Lides Cibernéticas e Responsabilidade Civil no Ordenamento Jurídico Brasileiro.** Libertas: Revista de Pesquisa em Direito. v. 4, n. 2. 2018.

[15] BRASIL. Supremo Tribunal Federal. ***Inquérito n. 4.879/DF***. Decisão monocrática referendada. Disponível em: https://jurisprudencia.stf.jus.br/pages/search/sjur477045/false. Acesso em: 17 setembro 2023.

determinasse que as empresas de telecomunicação guardassem, pelo prazo de noventa dias, os dados necessários para *a definição ou identificação de geolocalização dos usuários e* registros de conexão das pessoas presentes no local objeto da investigação[16].

Muito embora o pedido de informações acerca da geolocalização estivesse contido na manifestação da AGU, as medidas que foram efetivamente deferidas pelo Ministro Relator, e que são relevantes ao estudo, foram determinações direcionadas à Polícia Federal e Tribunal Superior Eleitoral as quais, por sua natureza, visavam à obtenção e compartilhamento de dados pessoais contendo a identificação dos indivíduos ou aqueles que os pudessem identificá-los, mesmo que considerados sensíveis, como definido pela Lei Geral de Proteção de Dados – LGPD (Lei 13.709, de 14 de agosto de 2018). Por fidelidade ao teor da decisão, transcreve-se trecho pertinente ao caso para melhor ilustrar a discussão firmada[17]:

> Diante do exposto, DEFIRO OS REQUERIMENTOS E REPRESENTAÇÕES, nos termos do art. 282 e 319 do CPP, e:
> (...)
> DETERMINO, ainda:
> (...)
> 7) À POLÍCIA FEDERAL que obtenha (a) todas as imagens das câmeras do Distrito Federal que possam auxiliar no reconhecimento facial dos terroristas que praticaram os atos do dia 8 de janeiro, (b) junto a todos os hotéis e hospedarias do Distrito Federal, a lista e identificação de hóspedes que chegaram ao Distrito Federal a partir da última quinta-feira, bem como a filmagem do saguão (lobby) para a devida identificação de eventuais participantes dos atos terroristas;
> 8) AO TRIBUNAL SUPERIOR ELEITORAL, sob a coordenação do assessor da Presidência, Eduardo de Oliveira Tagliaferro, que utilize a consulta e acesso aos dados de identificação civil mantidos naquela CORTE, bem como de outros dados biográficos necessários à identificação e localização de pessoas envolvidas nos atos terroristas do dia 8 de janeiro. Os dados deverão manter o necessário sigilo.

Portanto, cotejando-se as medidas deferidas e as requisitadas, conclui-se, obviamente, que não houve deferimento da prestação de informações de geolocalização dos investigados. Esta nuance, embora não possa ser interpretada como um "silêncio eloquente" do Ministro Alexandre de Moraes, poderia suscitar o reconhecimento de haver certa contrariedade acerca da constitucionalidade do tema, inclusive porque, neste mesmo sentido, o Supremo Tribunal Federal já havia reconhecido, em 28 de maio de 2021, a existência de repercussão geral dos

---

[16] O requerimento da AGU se deu nos seguintes exatos termos: 7) Determinação às empresas de telecomunicações, em particular as provedoras de serviço móvel pessoal que guardem pelo prazo de noventa dias os registros de conexão **suficientes para a definição ou identificação de geolocalização dos usuários** que estão nas imediações da Praça dos Três Poderes e do Quartel-General do Distrito Federal para apuração de responsabilidade nas datas dos eventos criminosos.

[17] BRASIL. Supremo Tribunal Federal. **Inquérito n. 4.879/DF**. Ministro Alexandre de Moraes. Disponível em: https://jurisprudencia.stf.jus.br/pages/search?classeNumeroIncidente=%22Inq%204879%22&base=acordaos&sinonimo=true&plural=true&page=1&pageSize=10&sort=_score&sortBy=desc&isAdvanced=true. Acesso em 05 de maio de 2025.

limites para decretação judicial da quebra de sigilo de dados telemáticos, no âmbito de procedimentos penais, em relação a pessoas indeterminadas (Tema 1148)[18].

Avançando-se neste caminho, embora a detalhada análise dos fenômenos políticos da época não sejam o objeto específico deste trabalho, tem-se que o momento democrático brasileiro já se mostrava conturbado anos antes da realização da eleição de 2018, marco da consolidação da polarização política entre os grupos progressistas e conservadores. Ao longo da primeira década do século XXI, observe-se o início de um processo de desgaste do ciclo democrático associado à terceira onda de democratização. Esse processo se manifesta de forma progressiva, com a consolidação e expansão de regimes de perfil autoritário, como os da China e da Rússia, e a crescente instabilidade de democracias emergentes. O cenário se torna particularmente crítico com os desdobramentos da Primavera Árabe, cujos resultados, em muitos casos, reforçaram estruturas autoritárias ou deram lugar a novos arranjos estatais marcados por forte repressão e limitação das liberdades políticas. Esse contexto marca o esgotamento do vigor democratizante que havia caracterizado a ordem internacional nas décadas anteriores[19].

Dessa forma, ainda que não se tenha concretizado um golpe de Estado nos moldes clássicos[20], foi possível observar a fragilização constitucional brasileira a partir das manifestações populares e o acirramento da polaridade partidária experimentada no Brasil, em meados do ano de 2015, contexto que antecedeu o processo de impeachment da ex-presidente Dilma Rousseff. Esse quadro de crise institucional se intensificou com a eleição do ex-Presidente Jair Messias Bolsonaro, cujo discurso, embora marcado por declarações de "jogar dentro das regras da Constituição", apresentava traços populistas que também representavam riscos à democracia, na medida em que buscava desacreditar o processo eleitoral sob alegação de risco de fraude ou afirmação de captura das instituições pelo seu adversário político[21].

---

[18] BRASIL. Supremo Tribunal Federal. **Tema 1.148** da Repercussão Geral. Recurso Extraordinário n.º 1.301.250. Relatora Ministra Rosa Weber. Disponível em: https://portal.stf.jus.br/jurisprudenciaRepercussao/tema.asp?num=1148. Acesso em: 5 maio 2025.

[19] LORENZONI, Pietro Cardia. **Jurisdição Constitucional de crise: análise e proposta hermenêuticas para a jurisdição constitucional extraordinária brasileira**. Tese de Doutorado, Universidade do Vale do Rio dos Sinos - Programa de Pós-Graduação em Direito, São Leopoldo, 2022. Disponível em: <https://www.repositorio.jesuita.org.br/bitstream/handle/UNISINOS/12688/Pietro%20Cardia%20Lorenzoni_PROTEGIDO.pdf?sequence=1&isAllowed=y>. Acesso em: 16 jun. 2025.

[20] LANDAU, David. **Abusive Constitutionalism**. UC Davis Law Review**.** v. 47, p. 72, 2013.

[21] LORENZONI, Pietro Cardia. **Jurisdição Constitucional de crise: análise e proposta hermenêuticas para a jurisdição constitucional extraordinária brasileira**. Tese de Doutorado, Universidade do Vale do Rio dos Sinos - Programa de Pós-Graduação em Direito, São Leopoldo, 2022. Disponível em: <https://www.repositorio.jesuita.org.br/bitstream/handle/UNISINOS/12688/Pietro%20Cardia%20Lorenzoni_PROTEGIDO.pdf?sequence=1&isAllowed=y>. Acesso em: 16 jun. 2025.

Ainda que o discurso oficial fosse de respeito à legalidade - “dentro das quatro linhas da Constituição” -, os atos e declarações do ex-Presidente Bolsonaro frequentemente assumiam contornos de um “mau jogador” e, por isso, tumultuariam “o andamento da partida”[22]. Perceba-se que não é necessário agir contra as regras para causar a desestabilização do funcionamento regular do sistema democrático. A crise institucional se aprofundou apenas com o tensionamento deliberado das relações com o Poder Judiciário, por meio da deslegitimação de suas decisões e com a adoção de uma retórica polarizadora baseada na lógica do “nós contra eles”. Paralelamente, o uso reiterado de medidas provisórias contribuiu para a fragilização do Poder Legislativo, esvaziando o papel do Congresso Nacional como espaço legítimo de formulação deliberação e controle das políticas públicas[23].

Esse movimento de autocratização foi identificado pelo instituto V-Dem, que no relatório de 2018[24] já apontava sinais de degradação constitucional no Brasil, em sintonia com o declínio de indicadores democráticos no período. Embora os dados do relatório de 2023[25] revelem uma mobilização em defesa da democracia indiquem um possível ponto de inflexão com o início do terceiro mandato do Presidente Luiz Inácio Lula da Silva, o cenário continua a ser marcado por forte polarização política e crescente fragmentação da opinião pública, fatores que mantêm acentuados os desafios à consolidação do Estado Democrático de Direito[26].

---

[22] BOBBIO, Norberto, **As ideologias e o poder em crise: pluralismo, democracia, socialismo, comunismo, terceira via e terceira força**, 3.ª ed. Brasília: Editora Universidade de Brasília, 1994.

[23] **Governo edita mais medidas provisórias que gestões anteriores, mas menos MPs se convertem em lei**. Agência Câmara de Notícias. Disponível em: https://www.camara.leg.br/noticias/709849-governo-edita-mais-medidas-provisorias-que-gestoes-anteriores-mas-menos-mps-se-convertem-em-lei/. Acesso em: 21 dez. 2023.

[24] V-Dem Annual Democracy Report 2018. Democracy for All? Disponível em: https://v-dem.net/documents/17/dr_2018.pdf. Acesso em 26/10/2023.

[25] V-Dem Annual Democracy Report 2023. Defiance in the Face of Autocratization https://v-dem.net/documents/29/V-dem_democracyreport2023_lowres.pdf. Acesso em: 26 out.2023.

[26] ORTELLADO, Pablo; RIBEIRO, Márcio Moretto; ZEINE, Letícia, Existe polarização política no Brasil? Análise das evidências em duas séries de pesquisas de opinião, **Opinião Pública**, v. 28, n. 1, p. 62–91, 2022.

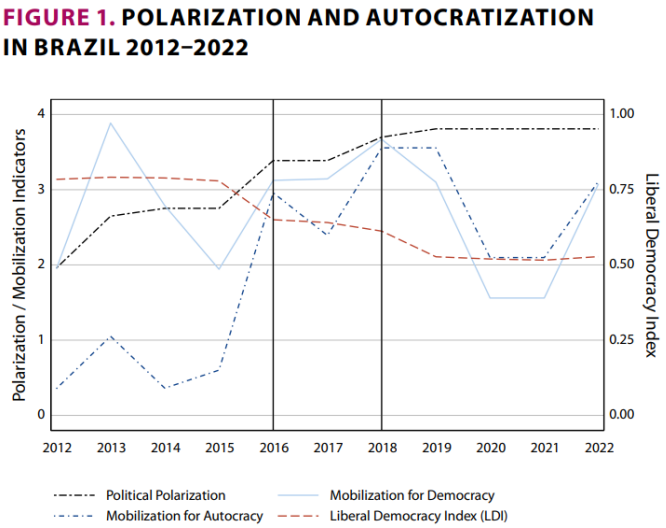

Figura 1 – Polarização e autocratização no Brasil (2012-2022)
Fonte: V-Dem Institute (2023)[11]

Nesse contexto, a preocupação que se tem para a estabilização política e a própria resiliência constitucional é o papel desempenhado pela Corte Constitucional, a qual poderia atuar visando a pacificação dos conflitos ou, num outro sentido, agravar o distanciamento da sensação de pertencimento e identificação majoritária aos ideais constitucionais ditados, no caso, pelo Supremo Tribunal Federal. Essa tendência, ativismo ou discricionariedade judicial[27] poder-se-ia consubstanciar como o substrato a guiar a interpretação jurídica a ser refletida nas decisões judiciais que se sucedem no cotejo da segurança nacional em face do direito à privacidade, principalmente acerca dos atos ocorridos no dia 08 de janeiro de 2023.

Feita a necessária digressão, no caso em análise, ainda que não tivessem sido deferidas as medidas a favor da geolocalização no bojo do Inquérito n.º 4.879/DF, os meios de comunicação propagaram amplamente notícias afirmando a sua determinação[2829]. E, por essa razão e a celeuma originada pela possibilidade de adoção deste percuciente instrumento de investigação estatal, justifica-se o estudo do tema em comento para se obter a exata dimensão e relevância desta determinação acautelatória, em confronto com os direitos e garantias individuais constitucionalmente estatuídas.

---

[27] STRECK, Lênio Luiz, **Verdade e consenso: constituição, hermenêutica e teorias discursivas**, [s.l.]: Saraiva Educação SA, 2014.
[28] **A mando de Moraes, manifestantes podem ser identificados pelos celulares.** Revista Oeste, 09 de janeiro de 2023. Disponível em: https://revistaoeste.com/brasil/a-mando-de-moraes-manifestantes-podem-ser-identificados-pelos-celulares/. Acesso em 17 set. 2023.
[29] **Moraes obriga empresas de telecomunicações a guardar registros de conexão e geolocalização de usuários**. CNN Brasil, 09 de janeiro de 2023. Disponível em: https://www.cnnbrasil.com.br/live-post/politica/moraes-obriga-empresas-de-telecomunicacoe-a-guardar-registros-de-conexao-e-geolocalizacao-de-usuarios/. Acesso em 17 set.2023.

3. PROBLEMA E PERGUNTA DE PESQUISA

O contexto no qual o estudo se desenvolve considera um cenário de rápida e contínua digitalização das atividades cotidianas dos indivíduos. Atualmente, a utilização espraiada de diversos meios telemáticos produz dados, mesmo que de maneira passiva, com as ferramentas dos smartphones, redes sociais, câmeras de segurança, transações online, dispositivos de geolocalização entre outros. Todas as ações, por suas próprias características, possuem um elevado grau de rastreabilidade, originando pegadas digitais que propiciam e fomentam o desenvolvimento de tecnologias de vigilância, seja de natureza privada ou mesmo estatal.

Em razão da facilidade de coleta e armazenamento de informações pessoais, por vezes exigidos até mesmo para prestação de serviços públicos, o risco de exploração destes dados e invasões à privacidade se torna exponencialmente ampliado. O avanço das tecnologias, como as ferramentas de big data e a vigilância digital em tempo real, permite que o Estado e empresas privadas reúnam, armazenem e analisem grandes quantidades de informações pessoais. O espectro de dados coletados origina uma verdadeira interconexão digital com esse quantitativo massivo de conteúdo, cuja finalidade é possibilitar o tratamento dessas informações para predizer preferências de consumo, hábitos de navegação, interações em redes sociais e até mesmo aspectos comportamentais, como padrões de deslocamento ou horários frequentes de atividades. O desafio a ser analisado se estabelece, em uma visão mais ampla, no uso indiscriminado dessas ferramentas e algoritmos que comprometem o direito à privacidade como também confronta princípios jurídicos fundamentais.

Portanto, restringindo o objetivo da presente dissertação, tem-se que o trabalho busca investigar se a expedição de mandados de geolocalização no âmbito das investigações criminais, sejam eles dirigidos a operadoras de telefonia (por meio de CSLI e ERB’s) ou a plataformas digitais (por meio de aplicativos, Wi-fi, Bluetooth), sem critérios claros de controle e requisitos bem definidos, afronta os direitos fundamentais à privacidade e à proteção de dados pessoais, garantidos pela Carta Magna e fomentados pela Lei Geral de Proteção de Dados.

Nesse sentido, a questão central que se propõe a responder é: A expedição de mandados judiciais de geolocalização com fundamento no artigo 22 do Marco Civil da Internet, para investigação de crimes diversos daqueles previstos nos artigos 13-A e 13-B do Código de Processo Penal, configura violação ao princípio da legalidade estrita e aos direitos fundamentais à privacidade e à proteção de dados pessoais, especialmente quando envolve pessoas não diretamente relacionadas à conduta delituosa?

Essa é a discussão que permeia o tema e expressa a essência do presente estudo: investigar a tensão existente entre o direito à privacidade e à proteção de dados pessoais de um lado e a necessidade do Estado de utilizar a geolocalização como ferramenta de investigação criminal. Noutro giro, outro objetivo é examinar os parâmetros jurídicos que permitam avaliar a constitucionalidade dessa prática identificando em que condições ela pode ser admitida sem violar os direitos fundamentais dos indivíduos.

4. OBJETIVOS

O objetivo geral estabelecido para a presente dissertação envolve, num primeiro estágio, o estudo do direito da personalidade, vez que a proteção de dados, inicialmente, foi concebida como decorrência do direito à privacidade. Em razão das premissas constitucionais estabelecidas, forçoso revisitar certos aspectos da estruturação constitucional deste direito fundamental para avançar sobre seus contornos entabulados no campo do Direito Civil. Em seu turno, como se sabe, a discussão iniciada por meio do artigo *The Right to Privacy* de Warren e Brandeis (1890)[30], o direito à privacidade vem evoluindo de sua acepção estritamente patrimonialista, centrando-se novamente no indivíduo, consubstanciando-se em verdadeira etapa da personificação do direito da privacidade.

Neste momento, seguindo-se o caminho proposto, demanda-se a análise do estado da arte do Direito Civil no que diz respeito ao direito da personalidade e sua conexão com o direito à proteção de dados. Essa depuração inicial tem como desiderato verificar se a proteção de dados está intrinsecamente contida no estudo do direito da privacidade ou, em uma compreensão mais dinâmica, se ela já estaria dotada de um grau de independência epistemológica a possibilitar uma interpretação no sentido de ser tratada como uma autodeterminação informacional do indivíduo, vez que seus atributos e características transcenderiam o direito de ser deixado a sós. Essa ponderação visa resgatar a importância da proteção de dados e reposicioná-la no âmbito do estudo do direito da personalidade. Estabelecendo-se a premissa e relevância do direito da proteção de dados, será possível aquilatar sua importância valorativa a ser sopesada em um cotejo com os princípios relacionados à segurança pública.

Partindo deste ponto, faz-se necessária a conceituação de geolocalização, bem como sua aplicação prática, especialmente, no âmbito das investigações criminais. Em seguida, a

[30] WARREN, Samuel; BRANDEIS, Louis. **The Right to Privacy.** Civilistica.com. v. 2, n. 3, p. 1–22, 2013. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/127>. Acesso em: 18 jun. 2025.

dissertação irá apreciar os fundamentos jurídicos das decisões que determinam a expedição de mandados de geolocalização ou de compilação dos dados que permitam a identificação do paradeiro dos dispositivos eletrônicos. Essa exploração jurisprudencial visa apurar se o Marco Civil da Internet está sendo empregado como supedâneo para o deferimento de tais medidas judiciais.

Construído o arcabouço teórico pretendido em cotejo com as discussões judiciais acerca do uso da ferramenta que permite a localização espacial, principalmente quanto aos seus requisitos, seguir-se-á a análise da validade desses mandados à luz dos direitos da personalidade, como a privacidade e a proteção de dados. Por conseguinte, serão examinados os critérios que respaldam o emprego da geolocalização e far-se-á a apuração sobre a adequação legal do instrumento. O trabalho, ainda, deverá conter aspectos do direito comparado sobre o uso de geolocalização em investigações criminais, bem como as inspirações da legislação estrangeira à LGPD e outros princípios que compõem o sistema de proteção de dados pretendido no ordenamento jurídico brasileiro.

Assim, torna-se adequado perquirir se a interpretação do Supremo Tribunal Federal, acerca da natureza dos dados pessoais sensíveis, se estáticos/registrais ou substanciais/conteúdo, está sendo acompanhada pela adequada revisitação da interpretação dos fundamentos constitucionais que consubstanciaram incialmente os princípios da proteção ao sigilo do teor das comunicações e da não autoincriminação.

Por fim, no decorrer da pesquisa, pretende-se a exposição crítica e analítica sobre a incidência da preservação dos direitos fundamentais à dignidade da pessoa humana afetos à proteção de dados no contexto das investigações criminais. A análise das repercussões jurídicas da violação de direitos fundamentais devido ao uso indevido da geolocalização será outra vertente a ser explorada, com a finalidade de expor como os mecanismos de controle judiciais tem sido implementados.

5. METODOLOGIA

A metodologia adotada neste estudo parte de uma abordagem dedutiva, estruturado inicialmente por meio de pesquisa bibliográfica qualitativa, com o objetivo de mapear o estado da arte sobre a temática da proteção de dados e sua interface com a persecução penal. Essa etapa envolverá a revisão crítica da literatura especializada, nacional e estrangeira, de modo a identificar os principais marcos teóricos e normativos que embasam a discussão. Em sequência,

proceder-se à análise detida de decisões paradigmáticas de Cortes constitucionais e superiores de diferentes ordenamentos jurídicos, notadamente dos Estados Unidos, de Portugal e da Itália.

As decisões da jurisprudência norte-americana são especialmente relevantes para a compreensão das tensões entre a generalidade dos mandados de localização e os limites impostos pela quarta emenda da Constituição dos Estados Unidos permitindo reflexões sobre a proporcionalidade e a exigência de individualização das medidas. No contexto português, destaca-se a evolução orgânica do sistema de proteção de dados, que se iniciou com uma legislação de caráter principiológico e culminou, em decorrência da incorporação de diretrizes europeias e da jurisprudência do Tribunal de Justiça da União Europeia, em uma regulamentação específica para o tratamento de dados no âmbito penal. Já a experiência italiana oferece subsídios valiosos em virtude das controvérsias havidas quanto à legitimidade do Ministério Público para requisitar diretamente dados pessoais sem autorização judicial, questão que guarda paralelismo com a controvérsia analisada pelo STF na ADI 5.642[31], relativa à reserva de jurisdição no ordenamento brasileiro.

Com base no escrutínio objetivo das decisões, será possível verificar se a congruência e propriedade dos mandados de geolocalização estão sendo efetuadas à luz do direito processual penal brasileiro, com o juízo de adequação para os meios de produção de provas, isto é, preenchimento dos requisitos necessários para o seu deferimento ou, por outro lado, se estes mandados de geolocalização estão sendo objeto de estudo sob o aspecto da colisão dos princípios constitucionais, a ensejar um exame de ponderação dos princípios, seguindo a Teoria da Argumentação de Robert Alexy (1978)[32]. Concluída esta etapa, acredita-se que será alcançado o objetivo primordial, podendo-se descrever se os mandados de fornecimento de dados de geolocalização estão consonantes com a Constituição Federal de 1988, quiçá se será necessário ajuste em seu emprego para que não suscite a afronta aos direitos da personalidade.

Contudo, a abordagem proposta não se descuida do recorte temático efetuado e o percurso da generalidade à especificidade do discurso apontada pelos quesitos a serem investigados. O que se quer evitar é trazer um compilado de informações e visões doutrinárias já sedimentadas ou um suporte exacerbado em manuais generalistas e seus discursos de autoridade, com conceituações clássicas, as quais pouco contribuem para a discussão

---

[31] BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade n.º 5.642.** Relator Ministro Edson Fachin. Julgamento em 18 abr. 2024. Disponível em: https://www.stf.jus.br/arquivo/cms/bibliotecaConsultaProdutoBibliotecaPastaFachin/anexo/ADI5642.pdf. Acesso em: 14 jun. 2025.

[32] ALEXY, Robert, **Teoria da argumentação jurídica: a teoria do discurso racional como teoria da fundamentação jurídica.**, 4ª. Rio de Janeiro: Forense, 2017.

substancial do tema, como muito bem pontuado por Luciano Oliveira em seu trabalho "Não fale do Código de Hamurabi!"[33].

O que se propõe é a revisitação dos enunciados, adotando-se o método arqueológico como proposta metodológica da busca do saber, como bem construído por Foucault em sua célebre obra "A Arqueologia do Saber"[34], partindo-se do acontecimento ocorrido na Praça dos Três Poderes, no dia 08 de janeiro de 2023, e analisando-se prospectivamente as camadas de cada discurso deste arquivo que compõe as relações entre os princípios inerentes aos direitos da personalidade em cotejo com a segurança pública.

6. ESTRUTURA DA DISSERTAÇÃO

A estruturação da dissertação foi concebida respeitando uma estratégia metodológica que, em um primeiro momento, apresentasse o contexto concreto das ferramentas de geolocalização e os seus impactos sobre a privacidade, oferecendo um panorama prático e atual do emprego dessa tecnologia em diversos aspectos da vida cotidiana. O primeiro capítulo, portanto, dedica-se a detalhar as ferramentas atinentes à geolocalização, destacando os procedimentos técnicos necessários para sua viabilidade e as nuances intrínsecas a cada uma das formas empregadas. A exposição sobre os diferentes usos da geolocalização, incluindo sua adoção enquanto perdurou a pandemia da COVID-19, sugere que o objetivo é demonstrar os seus fins legítimos, bem como, por outro lado, evidenciar as finalidades potencialmente problemáticas.

Em seguida, procedeu-se a revisão da literatura acerca da contingente proteção de direitos fundamentais nos ordenamentos jurídicos democráticos, marco teórico sobre o qual essa pesquisa se embasa. Em particular, explora-se a teoria de Robert Alexy, a qual dialoga com o pensamento de Ingo Wolfgang Sarlet, de Virgílio Afonso da Silva e, ainda, de Jane Reis Gonçalves Pereira. Essa linha de entendimento é estabelecida como pressuposto para análise dos direitos fundamentais, na medida em que o cerne do trabalho envolve a colisão entre o direito à privacidade e segurança pública. A distinção entre regras e princípios, bem como mecanismos de ponderação propostos pelos autores, é imprescindível para a harmonização das

[33] OLIVEIRA, Luciano, Não fale do Código de Hamurábi, **A pesquisa sócio-jurídica na pós-graduação em Direito**, 2004.
[34] FOUCAULT, Michel. **A Arqueologia do Saber**. Trad. Luiz Felipe Baeta Neves. 7. ed. Rio de Janeiro: Forense Universitária, 2009.

normas diante de sua colisão e, ainda, compreensão dos limites dos direitos fundamentais para apuração de como as cláusulas de restrição podem atuar na amplitude dos direitos fundamentais.

Os direitos da personalidade e suas características foram tratados em capítulo autônomo visando estabelecer a relação entre a proteção da privacidade e a evolução dos direitos fundamentais, principalmente quanto à autodeterminação informativa e sua categorização como direito autônomo. A apreciação dessas bases visa identificar a dimensão do direito à proteção de dados em relação ao direito da privacidade, considerando a sua evolução geracional. Essa digressão se justifica, inclusive, pelo fato de que a privacidade e a proteção de dados pessoais se originam de valores mais amplos da dignidade da pessoa humana, dos quais decorrem os limites impostos pelo ordenamento jurídico ao uso de dados pessoais em investigações criminais. Ademais, a abordagem legislativa, especialmente a Lei Geral de Proteção de Dados, incluindo a influência da legislação europeia, demonstra como o tema tem sido enfrentado no cenário jurídico externo.

No capítulo 4, a compreensão da investigação criminal e seus limites constitucionais reforçam a análise do contexto da expedição judicial de *geofence warrants* com o intuito de apurar como o Estado pode obter, por este meio, elementos probatórios para fins de comprovação da prática de conduta delituosa, sem violar, contudo, direitos fundamentais e dar amplitude material a suas garantias. A abordagem sobre a ausência de regulamentação específica e o controle judicial, mesmo que *a posteriori*, das medidas invasivas é imprescindível, pois justifica o estabelecimento do contexto constitucional, resgatando as hipóteses de como os direitos fundamentais podem ser limitados ou restringidos. Esse quarto capítulo, então, fomenta a discussão da constitucionalidade dos mandados de geolocalização, uma vez que expõe as dificuldades de equilibrar o interesse público de investigação com a proteção dos direitos individuais. A colação de jurisprudência internacional reforça a necessidade de um cotejo sobre a matéria, permitindo verificar como outros países enfrentam o debate acerca do uso de dados de localização.

A menção ao caso mais emblemático, qual seja, a apuração do homicídio da Vereadora carioca Marielle Franco, que originou o Tema 1148 do Supremo Tribunal Federal, evidencia o entendimento das Cortes brasileiras no sentido de os dados de geolocalização serem dados registrais estanques e que não estariam abarcados pelo sigilo das telecomunicações. No entanto, essa tese exige um exame criterioso, uma vez que os dados obtidos por meio de torres repetidoras de rádio-base podem revelar não apenas a sua localização, mas também a posição geográfica de indistintos dispositivos móveis conectados a elas. Dessa forma, essas informações não poderiam ser classificadas como dados registrais estáticos.

Por fim, a conclusão foi estruturada para sintetizar os principais resultados da pesquisa, responder ao problema proposto e apresentar considerações finais sobre a constitucionalidade dos mandados de geolocalização. A inclusão de uma reflexão sobre as contribuições acadêmicas e jurídicas da dissertação indica uma preocupação em não apenas analisar a questão sob a ótica normativa, mas também fomentar o debate sobre os impactos desse instrumento no ordenamento jurídico brasileiro.

CAPÍTULO 1: TECNOLOGIAS DE GEOLOCALIZAÇÃO: CONCEITOS DE MÉTODOS DE RASTREAMENTO E IMPACTOS NA ESFERA INFORMACIONAL

A abertura desse capítulo poderia ser apresentada com alguma afirmação dotada de obviedade e generalidade sobre o avanço ou impacto da tecnologia na vida das pessoas. No entanto, esta afirmação pouco ou nada acrescentaria à contextualização da discussão proposta nesse trabalho. Afinal, é a própria essência da tecnologia desenvolver conhecimentos ou mesmo técnicas e processos que possam ser utilizados para criação de instrumentos, ferramentas ou soluções voltadas a facilitar a vida das pessoas, definindo, inclusive, a complexidade de uma organização social[35].

Não seria ela, então, parte da força motriz do desenvolvimento da sociedade, juntamente com os fatores culturais, econômicos e políticos, responsáveis pelas transformações na forma como nos relacionamos, seja no âmbito social ou nos meios de produção? Essa dinâmica evolutiva impulsionada pela tecnologia exige um constante aperfeiçoamento e atualização das epistemes científicas que, por sua vez, servem de verdadeiros substratos para fomentar o estabelecimento de novas premissas voltadas ao estudo da organização social.

De fato, o avanço tecnológico não conduz, necessariamente, a um desenvolvimento homogêneo, mas atua como base para profundas transformações estruturais que reconfiguram a organização econômica, social e cultural das sociedades. Essa é a perspectiva adotada por Manuel Castells[36], ao tratar dos paradigmas tecnológicos, segundo a qual os sistemas evoluem gradualmente até que ruptura tecnológica introduza uma mudança qualitativa e inaugure um novo paradigma.

O sociólogo catalão Castells, em seu artigo "*La interacció entre les tecnologies de la informació i la comunicació i la societat xarxa: un procés de canvi històric*" identifica dois grandes momentos históricos nessa transição: o **industrialismo,** que se consolidou no século XIX e se estruturou em torno da capacidade das máquinas de gerar e distribuir energia de forma independente da natureza, e o **informacionalismo**, paradigma emergente do século XXI, centrado no processamento e na comunicação digital da informação, possibilitado pelo desenvolvimento da microeletrônica e das redes informáticas.

---

[35] LENSKI, Gerhard. **Power and Privilege: A Theory of Social Stratification**. New York: McGraw-Hill, 1966. Disponível em: <https://ia801402.us.archive.org/19/items/in.ernet.dli.2015.118923/2015.118923.Power-And-Privilege-A-Theory-Of-Social-Stratification.pdf>. Acesso em: 16 jun. 2025.

[36] CASTELLS, Manuel. **La interacció entre les tecnologies de la informació i la comunicació i la societat xarxa: un procés de canvi històric**. CONEIXEMENT I SOCIETAT, v. 1, p. 8–21, 2003. Disponível em: <https://catalunyaeuropa.net/desigualtats/admin/assets/uploads/files/d7541-la_interaccio_entre_les_tecnologies_de_l.pdf>. Acesso em: 28 abr. 2025.

No contexto abordado pelo autor, essa transição não se dá de forma uniforme ou linear. A substituição de um paradigma por outro ocorre na medida em que este novo modelo proporciona uma nova configuração e maior eficiência na geração de riqueza, poder e conhecimento, passando a estruturar não apenas os modos de produção e gestão, mas também as formas de interação, de experiência e de organização do espaço e do tempo.

Então, por melhor dizer, o caminhar tecnológico tem adequado as relações humanas e os comportamentos sociais ao longo do tempo, mas, a partir da Revolução Industrial, essa influência se tornou mais evidente, representando o marco do industrialismo definido por Castells. O surgimento das máquinas a vapor, a mecanização da produção e a urbanização acelerada redefiniram as formas de trabalho, os laços comunitários e a dinâmica familiar [37].

No século XX, com a automação, a ascensão da informática, essas transformações se ampliaram, culminando na era digital, onde a tecnologia passou a mediar grande parte das interações humanas e influenciar profundamente os hábitos de consumo, comunicação e aprendizado. Consolida-se, então, no século XXI o paradigma do informacionalismo que propiciaria a consolidação de uma nova estrutura social, denominada sociedade em rede, baseada na Revolução das Tecnologias da Informação que pressupõe um avanço na dinâmica do processamento da informação e a ressignificação das relações de poder e da própria produção de conhecimento:

> L'informacionalisme és un paradigma tecnològic, i no es refereix a l'organització social ni a les institucions, sinó a la tecnologia. L'informacionalisme proporciona la base per a un tipus determinat d'estructura social que jo anomeno la societat xarxa. Sense l'informacionalisme la societat xarxa no podria existir, però aquesta estructura social no ha estat produïda per l'informacionalisme, sinó per un patró d'evolució social més ampli. Més endavant tractaré l'estructura, la gènesi i la diversitat històrica de la societat xarxa, però primer em concentraré en la seva infraestructura material: l'informacionalisme com a paradigma tecnològic[38].

A geolocalização é, portanto, mais um ingrediente desse cenário na medida em que se apresenta como uma ferramenta capaz de proporcionar conveniência e personalização de serviços, ao mesmo tempo que que suscita debates acerca da privacidade e a segurança dos dados dos usuários. Sua aplicação abrange desde a orientação espacial, perpassando por navegação e mobilidade urbana, como em aplicativos de transporte, entregas, entretenimento, bem como estratégias de marketing digital, ao possibilitar a segregação de público-alvo e disparo de ofertas baseadas na localização do destinatário.

---

[37] MCLUHAN, Marshall. **Os meios de comunicação: como extensões do homem**. [s.l.]: Editora Cultrix, 1974.
[38] *Ibid.*, p. 10.

Entretanto, o uso extensivo da geolocalização também atrai preocupações éticas e jurídicas, especialmente no que tange ao monitoramento passivo de dados, a vigilância estatal perene em massa e a ausência de consentimento no compartilhamento de informações. Dessa forma, sua incorporação nas relações sociais e econômicas demanda um equilíbrio entre a tecnologia e sua conveniência e a proteção dos direitos fundamentais à proteção de dados e privacidade, alcançando-se a expectativa de privacidade esperada de seu uso ordinário. O desafio jurídico contemporâneo, portanto, consiste em assegurar que a inovação tecnológica não ultrapasse os limites éticos e constitucionais que garantem a dignidade e a autonomia informacional dos indivíduos. Assim, nesta seção, serão abordadas questões atinentes à ferramenta de geolocalização, seu conceito e formas de sua obtenção.

1.1. O CONCEITO E AS TECNOLOGIAS DE GEOLOCALIZAÇÃO

O uso de smartphones no cotidiano trouxe uma série de facilidades que otimizam tarefas diárias, tornando a experiência do usuário final mais eficiente e personalizada. No entanto, essa conveniência tem um custo: a concessão de informações pessoais às Bigtechs.

A justificativa apresentada por essas empresas é que, ao fornecerem dados pessoais, os usuários recebem serviços mais precisos e ajustados a suas necessidades. Contudo, a outra face dessa relação é a ampla utilização desses dados, a qual não está adstrita à melhoria da experiência do usuário, mas envolve sua comercialização e compartilhamento com parceiros de negócios. Essas informações são utilizadas para personalizar anúncios, induzir comportamentos e influenciar hábitos de consumo, apresentando um ciclo no qual os consumidores são bombardeados com informações para fazerem a “escolha certa”, sem a plena consciência desse poder de influência e de como seus dados foram utilizados.

A precisão e eficácia com que os serviços personalizados são entregues não apenas aumentam a fidelização do usuário, como também elevam significativamente o valor agregado das empresas de tecnologia, resultando em um mercado digital bilionário. Assim, essa dinâmica entre clientes e Bigtechs se estrutura sobre uma troca desigual, em que consumidores cedem dados relevantes em favor de uma conveniência, enquanto as empresas os monetizam de forma massiva, consolidando seu posicionamento no mercado e em relação ao comportamento do usuário.

Para fins da presente pesquisa, cumpre destacar que a obtenção de dados aptos a viabilizar a geolocalização do indivíduo pode ser analisada sob a ótica de sua origem, sendo possível classificá-la em duas categorias: **compulsória** e **consentida**.

A obtenção compulsória refere-se à coleta de dados de localização decorrente do uso de serviços considerados essenciais, como os serviços de telecomunicações ou de provimento de acesso à internet. Nessa hipótese, a localização de aparelhos móveis do usuário pode ser inferida por meio de registros gerados pelas estações rádio base (ERB's), que estão tecnicamente vinculadas à prestação contínua e obrigatória desses serviços, nos termos de contratos de natureza existencial firmados com as operadoras de telecom.

Por outro lado, a obtenção consentida ocorre mediante aceitação voluntária, ainda que presumida, das políticas de privacidade impostas por empresas provedoras de aplicações e plataformas digitais, as chamadas Bigtechs. Nesse caso, a instalação de aplicativos em dispositivos móveis e o consequente uso de funcionalidades baseadas em localização implicam, em regra na autorização para coleta e tratamento de dados. Esses dados, quando cotejados com outras informações associadas ao perfil do usuário, permitem a determinação de sua localização com alto grau de precisão.

Ainda que formalmente respaldada pelo consentimento, essa modalidade de obtenção de dados suscita importantes questionamentos quanto à real compreensão, voluntariedade e transparência do consentimento prestado, especialmente diante da complexidade e opacidade dos termos de uso e das políticas de privacidade usualmente adotadas por estas plataformas.

1.1.1 Geolocalização derivada de informação consentida.

Para o exato dimensionamento e contextualização do emprego da tecnologia de geolocalização, as Nações Unidas, com base em dados divulgados pela União Internacional das Telecomunicações – UIT, relataram que 78% da população mundial com 10 anos ou mais possuem um telefone celular[39], o que representa cerca de 5,78 bilhões de usuários únicos. Diante desse cenário, a afirmação de que o celular se tornou um dispositivo onipresente ganha cada vez mais relevância.

Seguindo esse contexto, a empresa Google se define como "*uma empresa diversificada de tecnologia cuja missão é organizar a informação mundial e torná-la universalmente acessível e útil*[40]". Em fevereiro de 2025, a Google detinha 79,92% do mercado global de

[39] ONU News. **Mais de três quartos da população mundial possuem um telefone celular**. 27 dez. 2023. Disponível em: https://news.un.org/pt/story/2023/12/1825432 . Acesso em 15 mar. 2025.

[40] GOOGLE LLC. ***Brief of Amicus Curiae Google LLC in Support of Neither Party Concerning Defendant's Motion to Suppress Evidence from a "Geofence" General Warrant (ECF No. 29)***. United States District Court for the Eastern District of Virginia, case *United States v. Chatrie*, 20 dez. 2019, p. 6-9. Disponível em: https://www.nacdl.org/getattachment/723adf0b-90b1-4254-ab82-e5693c48e951/191220-chatrie-google-amicus-brief.pdf. Acesso em: 15 de mar. de 2025

mecanismos de busca em desktops e 94,35% no segmento de buscas móveis, consolidando sua posição dominante no setor[41]. Esse monopólio informacional se traduz em aproximadamente 1,2 trilhões[42] de pesquisas anuais em todo o mundo, o que a torna capaz de direcionar 63,41% de todo o tráfego da internet.

Com base nessa plataforma e domínio de mercado, a Google oferece, além do sistema operacional Android, serviços como: o Google Maps, Google Drive, Gmail e aquele serviço que atrairá a atenção desse estudo, o Histórico de Localização. O Histórico de Localização seria *um serviço "opcional" que permite aos usuários registrar e armazenar um histórico detalhado de seus deslocamentos ao longo do tempo*[43]*"*. A adesão a este serviço se daria por expresso consentimento do usuário e poderia ser ativado ou desativado a qualquer momento. Importante ressaltar que estes serviços estão vinculados ao usuário por meio de sua conta de serviços Google, isto é, assim como os celulares, estes serviços seriam igualmente onipresentes nos smartphones.

Visando manter a fidedignidade das informações acerca do serviço de Histórico de Localização, serão utilizadas afirmações prestadas pelo Google LLC, no caso *United States of America v. Okello T. Chatrie, Case No. 3:19-cr-00130-MHL*. Apenas com o fito de contextualização, esse caso foi instaurado em 2019 para apuração de um assalto ocorrido em uma cooperativa de crédito, Call Federal Credit Union, na cidade de Midlothian, Virgínia - EUA.

Inicialmente, a polícia não conseguiu identificar o autor do crime, mas as câmeras de vigilância captaram a imagem de uma pessoa com um celular na mão durante os acontecimentos. Considerando o insucesso inicial, as autoridades investigativas requereram a expedição de um mandado de geolocalização (G*eofence Warrant*) destinado ao Google LLC, considerando a elevada probabilidade de o telefone utilizado pelo indivíduo nas filmagens possuir serviços da empresa de tecnologia que pudessem identificar o usuário. O resultado do mandado de geolocalização apontou que o celular de Chatrie esteve nas redondezas da cooperativa de crédito no momento do crime.

Em sua defesa, OKello T. Chatrie declarou-se inocente do assalto e pleiteou a invalidação das provas obtidas por meio do *geofence warrant.* Ele arguiu que o mandado

---

[41] Statcounter Global Stats. **Desktop Search Engine Market Share Worldwide**. Disponível em: https://gs.statcounter.com/search-engine-market-share/desktop/worldwide. Acesso em 15 mar. 2025.
[42] Internet Live Stats. **Google Search Statistics**. Disponível em https://www.internetlivestats.com/google-search-statistics/. Acesso em 15 mar. 2025.
[43] GOOGLE LLC. Brief of Amicus Curiae – tradução livre. Idem.

afrontou a 4ª Emenda Constitucional Americana[44] e que as provas obtidas deveriam ser descartadas em virtude de haver violado as expectativas esperadas de sua privacidade e localização em relação aos serviços do Google LLC, bem como, aduziu ainda, que o mandado carecia de justa causa e juízo de probabilidade. A Corte Distrital rejeitou o pedido, o qual foi mantido pela Corte Estadual da Virginia.

Citando o caso *Smith v. Maryland, 442 U.S. 735 (1979),* da Suprema Corte Americana dos Estados Unidos[45], os tribunais, embora preocupados com a invasão de privacidade dos usuários, fundamentaram sua decisão na aplicação da "*third-party doctrine*". Segundo essa doutrina, uma pessoa não pode reivindicar boa-fé ou exigir privacidade sobre informações que tenha voluntariamente fornecido a terceiros, os quais podem ser compelidos a entregá-los ao governo.

No caso em questão, considerando que o Histórico de Localização é um serviço que está desabilitado por padrão de fábrica nos celulares e que é necessária à sua habilitação ativa, após a confirmação em diversas etapas, Okello T. Chatrie teria voluntariamente entregue suas informações ao Google e, por esta razão, não poderia suscitar a tese de possuir uma expectativa razoável de manutenção de sua privacidade. Chatrie, ao final, retificou seu pronunciamento inicial e apresentou uma confissão de culpa condicional, sendo sentenciado a 141 meses de prisão e 3 anos de liberdade supervisionada.

Durante a instrução processual, o Google LLC atuou como *amicus curiae,* apresentando uma manifestação com o objetivo de publicizar sua preocupação com os contornos jurídicos para a expedição de mandados de geolocalização e esclarecer aspectos do procedimento e das informações obtidas em decorrência do cumprimento dessa ordem. Nesse documento, como mencionado anteriormente, são detalhados o funcionamento do serviço de Histórico de Localização e as peculiaridades sobre os serviços oferecidos pela Bigtech[46]:

> As set forth below, the LH information at issue in geofence requests such as the one in this case differs in significant respects from the cell site location information

[44] The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. UNITED STATES. **Constitution of the United States of America. Fourth Amendment**. Disponível em: https://constitution.congress.gov/constitution/amendment-4/. Acesso em 07 mai. 2025.

[45] ESTADOS UNIDOS. *Smith v. Maryland*, 442 U.S. 735 (1979). Supreme Court of the United States. Disponível em: Disponível em: https://supreme.justia.com/cases/federal/us/442/735/ Acesso em 20 mar. 2025.

[46] GOOGLE LLC. *Brief of Amicus Curiae Google LLC in Support of Neither Party Concerning Defendant's Motion to Suppress Evidence from a "Geofence" General Warrant (ECF No. 29)*. United States District Court for the Eastern District of Virginia, case *United States v. Chatrie*, 20 dez. 2019, p. 6-9. Disponível em: https://www.nacdl.org/getattachment/723adf0b-90b1-4254-ab82-e5693c48e951/191220-chatrie-google-amicus-brief.pdf. Acesso em: 15 de mar. de 2025.

("CSLI") at issue in *Carpenter v. United States, 138 S. Ct. 2206 (2018)*, and other types of data that courts have considered in Fourth Amendment cases. For example, rather than a record created and stored by Google as an automatic result of using a Google service, Google LH information is created, edited, and stored by and for the benefit of Google users who opt into the service and choose to communicate their location information to Google for storage and processing. Moreover, LH information can often reveal a user's location and movements with a much higher degree of precision than CSLI and other types of data. And rather than targeting the electronic communications of only a specific user or users of interest, the steps Google must take to respond to a geofence request entail the government's broad and intrusive search across Google users' LH information to determine which users' devices may have been present in the area of interest within the requested timeframe.

(…)

Google "Location History" information is essentially a history or journal that Google users can choose to create, edit, and store to record their movements and travels. Google's users activate and use LH for many reasons. By enabling and using LH, a Google user can keep a virtual journal of her whereabouts over a period of time. For most Google users, this journal is captured in the "Timeline" feature of the Google Maps app. See Fig. 1. The Timeline feature allows the user to visualize where she has traveled with her phone and when over a given period—in essence, a journal.

(…)

By using Google LH, the user can access other benefits on her Google device or applications as well. For example, she can obtain personalized maps or recommendations based on places she has visited, get help finding her phone, and receive real-time traffic updates about her commute.

(…)

When the device-location setting is activated, the mobile device automatically detects its own location, which the device ascertains based on GPS and Bluetooth signals, Wi-Fi connections, and cellular networks.

(…)

In sum, LH functions and saves a record of the user's travels only when the user opts into LH as a setting on her Google account, enables the "Location Reporting" feature for at least one mobile device, enables the device-location setting on that mobile device, permits that device to share location data with Google, powers on and signs into her Google account on that device, and then travels with it.

(…)

The user thus controls her Google LH data—unlike, for instance, the CSLI at issue in Carpenter or cellular data obtained via a "tower dump." As the Supreme Court explained in Carpenter, CSLI consists of time-stamped records that are automatically generated by and for the wireless carrier whenever a mobile device connects to a cell site (i.e., the physical radio antennas that make up the cellular network). 138 S. Ct. at 2211-2212. Wireless carriers collect and maintain CSLI records "for their own business purposes," such as identifying weak spots in the network or determining when to apply roaming charges. Id. at 2212. When law enforcement seeks access to CSLI, it is thus asking the wireless carrier to produce its own business records showing when a particular device connected to a cell site within a particular period of time. A request for a "tower dump" likewise seeks the wireless carrier's own business records—in that case, identifying every phone that connected to a particular cell site (or "tower") in a particular period.

Mobile device users cannot opt out of the collection of CSLI or similar records, nor can they retrieve, edit, or delete CSLI data. Google LH information, by contrast, is stored with Google primarily for the user's own use and benefit—just as a user may choose to store her emails on Google's Gmail service and her documents on Google Drive. Google LH information is controlled by the user, and Google stores that information in accordance with the user's decisions (e.g., to opt in or out, or to save, edit, or delete the information), including to enhance the user's experience when using other Google products and services.

Evidencia-se, portanto, que o Histórico de Localização opera de maneira distinta dos dados de localização de torres de celular (Estação Rádio Base) ou Cell-Site Location Information – CSLI, analisados pela Suprema Corte Americana no caso Carpenter v. United States (2018). Nesse sentido, enquanto os registros das ERB's e CSLI são gerados automaticamente pelas operadoras de telefonia móvel sempre que um celular se conecte a uma torre, os dados do Histórico de Localização só seriam criados se os usuários consentissem na ativação desse serviço do Google, podendo editá-los ou excluí-los. Ou seja, ao contrário do CSLI e ERB, cuja coleta de informações é realizada automaticamente pelas operadoras de telefonia, o usuário não possui qualquer controle das informações, fato este que poderia suscitar a avocação da tese da razoável expectativa de privacidade frente a estas operadores de telefonia.

De outro lado, o Histórico de Localização tende a ser mais preciso do que os registros produzidos pelas torres (ERB e CSLI), na medida em que, além desses equipamentos, o serviço utiliza outras fontes como GPS, redes Wi-Fi e sinais de Bluetooth, o que permite a geração de um relatório mais detalhado e acurado.

Diante das peculiaridades proporcionadas pelo Histórico de Localização, que seria um diário digital de viagens, o Google argumenta que os relatórios produzidos com base nessas informações não deveriam ser tratados da mesma maneira que os registros das torres de celular. A Bigtech sustenta que, enquanto o Histórico de Localização é compilado com o consentimento do usuário, os relatórios das Estações Rádio Base (ERB's) elaborados pelas operadoras de telefonia, são produzidos independentemente da vontade do titular, com base no acesso à rede de telecomunicações móveis.

1.1.2 Geolocalização derivada de informação compulsória

Dando continuidade à análise das tecnologias capazes de fornecer dados de geolocalização de usuários de telefonia móvel, destaca-se que, conforme informado em documento técnico da empresa Google LLC, os registros gerados por Estações Rádio Base das operadoras, quando acionadas por aparelhos celulares que ingressaram em sua área de cobertura, também podem ser utilizados para inferir a localização aproximada de um dispositivo.

A identificação da localização geográfica de dispositivos móveis pode ser realizada por duas metodologias principais: por meio da obtenção do relatório de informações de localização por estação rádio base (Cell-Site Location Information – CSLI) ou pela triangulação dos sinais emitidos entre múltiplas estações rádio base (ERB's). Em ambas as modalidades, a fonte de

informação é gerada a partir da comunicação do aparelho celular com a rede de telecomunicações, ainda que de maneira automática e inconsciente por parte dos usuários, possibilitando a determinação da posição geográfica com base nas antenas e equipamentos operados pelas empresas de telefonia móvel.

O método CSLI foi detalhado no caso United States of America v Curtis (nº 17-1833), no qual a Corte de Apelação descreveu-o como "*a informação de localização gerada por uma operadora de telefonia celular que indica com qual torre de celular um determinado telefone estava se comunicando no momento em que uma comunicação foi realizada*[47] *(United States os America v. Curtis, 2018, p.2)*". Como o relatório CSLI se refere à conexão de um dispositivo com uma única torre, sua precisão geográfica é limitada, uma vez que o telefone emissor pode estar situado em qualquer ponto dentro do raio de cobertura da torre utilizada.

De outro modo, a técnica baseada na triangulação dos sinais de radiofrequência, emitidos e recebidos por diferentes ERB's, permite uma estimativa de localização consideravelmente mais precisa. Embora ainda não alcance a acurácia dos sistemas de posicionamento global por satélite (GPS), esse método revela a capacidade de rastreamento contínuo de dispositivos móveis, independentemente da ativação explícita dos serviços de localização pelo usuário, evidenciando riscos relevantes associados à vigilância passiva e não consentida.

Em tese de Doutorado defendida por Valine Silva Casteldelli[48], o funcionamento da Estação Rádio Base como tecnologia apta a fornecer informações de geolocalização foi abordado de forma didática e objetiva, permitindo que os conhecimentos jurídicos advindos de outras áreas das Ciências pudessem dialogar com os aspectos jurídicos envolvidos. A autora concentra sua análise justamente no artigo 13-B do Código de Processo Penal, dispositivo que, como já mencionado, constitui a única previsão normativa expressa no ordenamento processual penal brasileiro sobre o uso de tecnologias para a localização geográfica de vítimas e suspeitos de crimes relacionados ao tráfico de pessoas.

Contudo, algumas observações críticas devem ser feitas a referida pesquisa. A defesa da tese ocorreu em 2021, momento anterior à promulgação da Emenda Constitucional nº 115/2022, que inseriu expressamente a proteção de dados pessoais inclusive nos meios digitais

---

[47] UNITED STATES OF AMERICA v. CURTIS, nº 17-1833, United States Court of Appeals for the Seventh Circuit, decisão de 24 agosto de 2018. Disponível em: https://law.justia.com/cases/federal/appellate-courts/ca7/17-1833/17-1833-2018-08-24.html. Acesso em: 26 abr. 2025.

[48] CASTELDELLI, Valine Silva, **Convenção de Palermo, tráfico de pessoas e geolocalização via sinais da estação rádio base: a gênese do art. 13-b do código de processo penal e a inserção sub-reptícia da violação à intimidade e vida privada na persecutio criminis brasileira**, Tese de Doutorado, Universidade Federal de Santa Catarina, Florianópolis, 2021.

no rol dos direitos e garantias fundamentais previstos no artigo quinto da Constituição Federal. Importa ressaltar que o artigo 13-B do CPP tem como escopo específico a localização de vítimas e suspeitos nos crimes de tráfico de pessoas. O texto legal não faz referência à utilização da geolocalização para fins de identificação da autoria criminal, o que limita seu alcance no processo penal.

E, ainda que se pudesse argumentar que os dados obtidos por meio das ERB's não violariam o direito ao sigilo das comunicações - uma vez que tais relatórios não revelam o conteúdo das mensagens trocadas, mas apenas registros técnicos -, o estudo deixou de contemplar a análise do novo direito fundamental à proteção de dados pessoais, por força da ausência da contemporaneidade entre a promulgação da Emenda e a elaboração da tese.

Remetendo-se novamente à discussão da geolocalização por informação compulsória, bem como valendo-se da judiciosa análise e descrição técnica contida na tese de Doutorado defendida por Valine Silva Casteldelli[49], tem-se que Portaria 219/2018 da Anatel[50] define, para os procedimentos de fiscalização da agência, o equipamento Estações Rádio Base (ERB's) como: "*É a estação de radiocomunicações de base do SMP* [Serviço Móvel Pessoal] *usada para radiocomunicação com Estações Móveis*". Por sua vez, o normativo dispõe que a Estação Móvel é *a "estação de telecomunicações do SMP que pode operar quando em movimento ou estacionada em lugar não especificado*", ou seja, nesses casos, os aparelhos de telefonia celular.

Em outros termos, as estações rádio base (ERB's) são estruturas fixas equipadas com antenas e dispositivos responsáveis por intermediar os sinais de comunicação entre os aparelhos celulares, denominados estação móveis (EM's), e a rede da operadora de telefonia. Cada ERB possui uma área geográfica de cobertura delimitada, dentro da qual é capaz de estabelecer conexões com dispositivos móveis que se encontrem em seu raio de alcance.

Ao receber um sinal emitido por um aparelho celular, a ERB realiza a comunicação de dados e encaminha a transmissão a uma central de comutação, a partir da qual os dados são processados e direcionados ao destino final da rede. Esse processo é parte essencial da infraestrutura de telecomunicações e permite, ainda que de forma indireta, a inferência da

---

[49] *Ibid.*

[50] BRASIL. Agência Nacional de Telecomunicações. **Portaria nº 219, de 09 de fevereiro de 2018**. Aprova o Procedimento de Fiscalização para Verificação da Disponibilidade de Rede, Ressarcimento por Interrupções e Comunicação de Interrupções para o Serviço Telefônico Fixo Comutado e Serviço Móvel Pessoal, no âmbito do Termo de Ajustamento de Conduta.. Disponível em: https://informacoes.anatel.gov.br/legislacao/procedimentos-de-fiscalizacao/975-portaria-219. Acesso em 5 abr. 2025.

localização aproximada do usuário, a depender da coordenada geográfica da ERB (Cell Id) com a qual dispositivo esteja conectado[51].

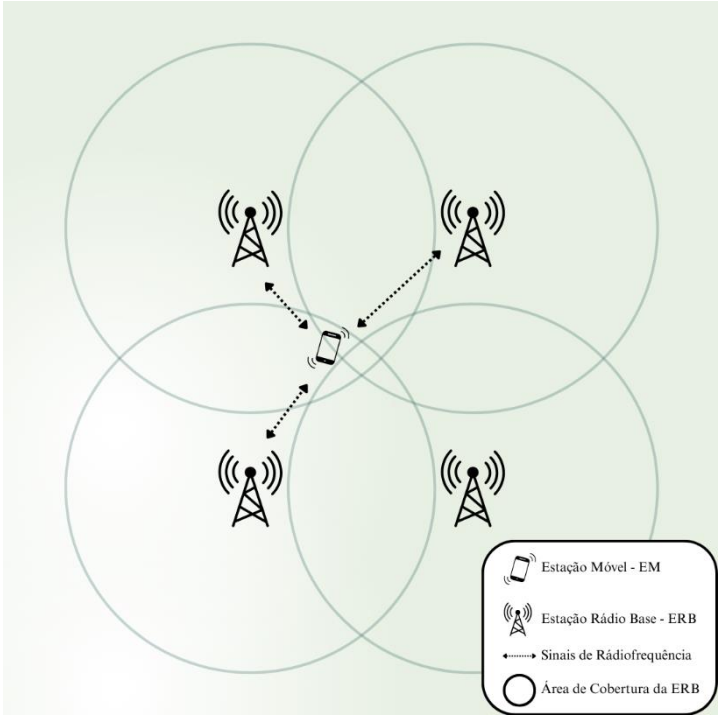

Figura 2 – Esquema ilustrativo de funcionamento da geolocalização por ERB
Fonte: Elaborado pelo autor (2025)

No momento em que um aparelho celular é utilizado, ele emite sinais de radiofrequência que são captados pela Estação Rádio Base mais próxima. O sistema de telecomunicações é capaz de estipular a localização geográfica aproximada do dispositivo com base na intersecção entre os círculos de cobertura gerados por essas emissões de radiofrequência. Importa destacar que esse procedimento não envolve a interceptação do conteúdo das comunicações, mas sim o tratamento de sinais técnicos, também chamado de metadados de localização, que podem ser utilizados para inferir o local onde o indivíduo se encontra.

Como alerta Casteldelli, a geolocalização por ERB é uma funcionalidade que não foi originalmente concebida para fins investigativos, mas que se manifesta como decorrência lógica e técnica intrínseca ao funcionamento da infraestrutura de telecomunicações, cuja dinâmica de operação pressupõe a troca de sinais entre os dispositivos móveis e as ERB's da rede[52]. Aliada a essas razões e com base no arcabouço regulatório da ANATEL, a autora conclui:

[51] CASTELDELLI, Valine Silva. **Convenção de Palermo, tráfico de pessoas e geolocalização via sinais da estação rádio base: a gênese do art. 13-b do código de processo penal e a inserção sub-reptícia da violação à intimidade e vida privada na persecutio criminis brasileira**. Tese de Doutorado, Universidade Federal de Santa Catarina, Florianópolis, 2021.
[52] *Ibid*.

> Consequentemente, a partir da exposição das normativas da Agência Nacional de Telecomunicações, verifica-se que nas portarias, resoluções e atos de sua rubrica são abordadas definições técnicas, tão somente com a finalidade de regulamentação administrativa do uso de sinais da Estação Rádio Base como viabilizadora do sistema de telecomunicação. À vista disso não há normativas afetas à ANATEL que tratem da utilização das informações dos sinais da Estação Rádio Base com fins jurídicos, quiçá processuais penais ou qualquer menção sobre o princípio da reserva legal para o fornecimento, pelas empresas de telefonia, das informações sobre a geolocalização de pessoas que se encontrariam em qualquer tipo de relação jurisdicional ou submetida à investigação criminal[53].

1.1.2.1 Localização por IP

Considerando a relevância que o Marco Civil da Internet (Lei n.º 12.295/2014) atribui ao endereço IP enquanto elemento de identificação de usuários, deve-se considerar as possibilidades e limitações da sua utilização para fins de determinação geográfica. Ainda que o endereço IP possa, em determinadas circunstâncias, fornecer indícios acerca da região de origem da conexão, especialmente país ou cidade, essa informação não equivale ou corresponde, de forma imediata, à identificação precisa do endereço físico do usuário. Esse endereço IP é um dado que permite apenas uma inferência aproximada de localização, cuja exatidão depende do cruzamento com outras bases de dados e sofre limitações quanto a sua precisão em níveis mais detalhados, como bairro ou mesmo número postal do endereço[54].

Conforme o artigo 5°, inciso III, da referida Lei, o endereço IP é definido como o "*código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais*"[55]. De forma simplificada, o endereço IP é um identificador digital, temporário, atribuído pelos provedores de conexão ao dispositivo que requisita acesso à rede, a partir das faixas numéricas de endereços que lhes são delegadas. Essas faixas, no caso do protocolo IPv4, consistem em endereços de 32 bits, que permitem cerca de 4 bilhões de cominações possíveis para a formação de um endereço específico. A autoridade global responsável por essa distribuição é a IANA (*Internet Assigned Numbers Authority*), que por sua vez, delega essa competência, na América Latina e Caribe, para LACNIC (*Latin America and Caribbean Network Information Centre*). Em seu turno, a LACNIC repassa faixas de endereços IP's para os Provedores de Conexão no Brasil. A partir de uma análise sistemática dessas

---

[53] *Ibid*., p. 61.
[54] LACNIC – Latin American and Caribbean Network Information Centre. Geolocalização de IPs. Disponível em: https://www.lacnic.net/1042/3/lacnic/acerca-do-lacnic. Acesso: 24 mai.2025.
[55] BRASIL. **Lei n.° 12.965/2014, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 24 mai. 2025.

faixas, associando blocos de ID das localidades com base em bancos de dados públicos ou entidades privadas, pode-se inferir, com razoável grau de confiança, a cidade de origem da conexão. Todavia, a precisão quanto ao bairro, à rua ou ao domicílio é altamente incerta, de modo que não se pode considerar o endereço IP, isoladamente, como um dado de geolocalização exata.

Barreto e Brasil[56] chamam a atenção para a limitação da precisão geográfica associada ao endereço IP, destacando que é comum o compartilhamento do sinal de internet entre usuários localizados em áreas próximas. Nessas situações, o mesmo endereço IP atribuído dinamicamente pela provedora de conexão pode ser utilizado por múltiplos dispositivos ou pessoas distintas. Essa circunstância compromete a exatidão na identificação da origem da conexão, podendo conduzir a erros na associação entre o IP registrado e o indivíduo efetivamente responsável pelo acesso à rede.

Assim, considerando o escopo do presente trabalho com o objetivo de apresentar uma conceituação sintética e precisa, a técnica de geo-*fencing* ou geolocalização pode ser compreendida como um procedimento de delimitação espacial orientado à identificação de dispositivos eletrônicos que tenham emitido ou recebido dados em uma determinada área. Essa delimitação ocorre por meio da análise de sinais provenientes de diferentes fontes, tais como sistema de posicionamento global (*Global Positioning System*[57]*)*, Cell-Site Location Information (CSLI), a triangulação de sinais de Estação Rádio-Base (ERB), Conexões à rede Wi-Fi, Bluetooth ou, ainda, endereços IP. A partir da consolidação dessas informações, é possível inferir a provável origem geográfico da emissão de dados e, por conseguinte, vincular os dispositivos eletrônicos aos respectivos titulares, o que conferiria a essa metodologia significativa utilidade como meio de prova de presença física em investigações ou procedimentos criminais.

1.2. APLICAÇÕES DAS TECNOLOGIAS DE GEOLOCALIZAÇÃO – PANDEMIA COVID-19

[56] BARRETO, Alesandro Gonçalves. **eBook: Manual de Investigação Cibernética: à luz do Marco Civil da Internet**. 1. ed. Rio de Janeiro: Brasport, 2016. Disponível em: <https://www.editorabrasport.com.br/investigacao-cibernetica-e-book>. Acesso em: 12 jun. 2025, p. 13.

[57] **What is GPS?** Disponível em: https://www.gps.gov/systems/gps. The Global Positioning System (GPS) is a U.S.-owned utility that provides users with positioning, navigation, and timing (PNT) services. This system consists of three segments: the space segment, the control segment, and the user segment. The U.S. Space Force develops, maintains, and operates the space and control segments. Acesso em: 07 maio de 2025.

No dia 11 de março de 2020, a Organização Mundial de Saúde - OMS, por meio de seu Diretor-Geral, Tedros Adhanom Ghebreyesus, declarou a caracterização de uma pandemia – a COVID-19. Tratava-se de uma doença respiratória viral e inflamatória, com grande velocidade de transmissão, que surpreendia o mundo em razão do elevado número de fatalidades[58].

Como forma de contenção à disseminação da COVID-19, a OMS recomendou o distanciamento físico entre indivíduos e a restrição de viagens desnecessárias[59]. Em alguns casos, países optaram por medidas mais restritivas de locomoção e contenção comunitária, como o lockdown[60]. Diante desses desafios, a tecnologia apresentou-se como instrumento fundamental para auxiliar os Estados na gestão da crise sanitária.

A utilização de dados de geolocalização passou a desempenhar papel estratégico, sendo aplicada para finalidades distintas. Em primeiro lugar, viabilizou o rastreamento de pessoas contaminadas e o alerta àqueles que mantiveram contato próximo com elas. Além disso permitiu a geração de indicadores sobre a concentração e a movimentação de indivíduos em espaços públicos, fornecendo subsídios para a adoção de medidas destinadas a evitar aglomerações e reduzir o risco de transmissão.

Em estudo publicado na *Revista Brasileira de Direitos Fundamentais & Justiça*, Zanatta et al.[61] analisam a utilização de tecnologias de informação e comunicação no enfrentamento da pandemia da COVID-19 e seus reflexos sobre o regime de proteção de dados pessoais no Brasil. A partir da observação das principais ferramentas de coleta e tratamento de dados adotadas em nível global, os autores examinam como essas práticas suscitaram controvérsias jurídicas. No desenvolvimento do artigo, são destacadas três formas de aproveitamento das tecnologias de rastreamento ou proximidade.

A primeira modalidade de utilização de dados é produção de mapas de calor. A partir dos princípios técnicos empregados na localização por meio de Cell-Site Location Information

---

[58] WHO. WHO Director-General's opening remarks at the media briefing on COVID-19 – 11 March 2020. Genebra: Organização Mundial da Saúde, 2020. Disponível em: https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020. Acesso em: 26 abril de 2025.

[59] WHO. WHO Director-General's opening remarks at the media briefing on COVID-19 – 11 March 2020. Genebra: Organização Mundial da Saúde, 2020. Disponível em: https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020. Acesso em: 26 abril de 2025.

[60] WILDER-SMITH, Annelies; FREEDMAN, David O.. **Isolation, quarantine, social distancing and community containment: pivotal role for old-style public health measures in the novel coronavirus (2019-nCoV) outbreak.** Journal of Travel Medicine, v. 27, 2020.

[61] ZANATTA, Rafael Augusto; BIONI, Bruno Ricardo; IGLESIAS KELLER, Clara; *et al*. **Os dados e o vírus: tensões jurídicas em torno da adoção de tecnologias de combate à Covid-19**. Revista Brasileira de Direitos Fundamentais & Justiça, v. 14, p. 231–256, 2020. Disponível em: <https://doi.org/10.30899/dfj.v14i1.1031>. Acesso em: 26 abr. 2025.

ou pela triangulação de sinais de Estação Rádio Base, torna-se possível analisar padrões de deslocamento, medir a densidade populacional em determinadas regiões em tempo real e, por conseguinte, aferir o nível de isolamento social. Essa ferramenta revela-se de grande relevância para avaliação espacial do comportamento coletivo, entretanto, sua utilização pressupõe a adoção de rigorosos procedimentos de anonimização dos dados pelas empresas de telecomunicação. Ausência dessa cautela pode ensejar a identificação dos padrões individuais de comportamento, comprometendo a privacidade dos titulares dos dados.

Além da elaboração de mapas de calor, duas outras modalidades de utilização de dados foram empregadas com a finalidade de rastrear indivíduos que, potencialmente, poderiam ter sido expostos ao vírus em função da proximidade com pessoas contaminadas. Para esse rastreamento, duas tecnologias distintas poderiam ser utilizadas: uma baseada na mesma lógica aplicada à criação de mapas de calor, porém com acurácia aprimorada na localização por meio da triangulação das informações das Estações Rádio Base (ERB's), e outra fundamentada na tecnologia Bluetooth, que seria hábil a detectar a proximidade de aparelho móvel de diferentes indivíduos[62].

No modelo baseado em Bluetooth, os dispositivos celulares identificavam a proximidade física com outros aparelhos dentro de um raio de alcance determinado. Caso um dos usuários posteriormente testasse positivo para a COVID-19, as pessoas que estiveram em contato próximo com ele receberiam um alerta informativo, recomendando a adoção de medidas de precaução ou, até mesmo, quarentena (*Contact tracing)*. Em diversas implementações ao redor do mundo, os aplicativos desenvolvidos para esse fim buscaram preservar o anonimato dos usuários, emitindo alertas sem revelar a identidade dos contaminados e, em alguns casos, sem sequer informar o local preciso do contato, apenas o risco potencial de contágio. Esses mecanismos de rastreamento, assim como a produção de mapas de calor, exigem a adoção de medidas de anonimização dos dados, sob pena de grave violação dos direitos a proteção dos dados e a privacidade dos titulares. Ainda assim, o uso dessas tecnologias coloca em evidência um cenário de colisão de princípios constitucionais, entre o direito à privacidade e a necessidade de preservação da saúde pública[63].

Com base nos modelos de coleta e análise de dados de localização, destacando-se no Brasil o uso da tecnologia de CSLI[64], uma iniciativa foi amplamente discutida pela doutrina e

---

[62] *Ibid*.
[63] PINHEIRO, Guilherme Pereira; PINHEIRO, Alexandre Pereira. **COVID-19 e geolocalização: entre a saúde e a proteção de dados pessoais**. Revista Jurídica, v. 24, 2022. Disponível em: <https://doi.org/10.20499/2236-3645.RJP2022v24e132-2252>. Acesso em: 28 abr. 202.
[64] *Ibid*.

jurisprudência durante a pandemia da COVID-19. No Estado de São Paulo, foi instituído o sistema de monitoramento inteligente de São Paulo (SIMI-SP), resultado da cooperação técnica entre o governo estadual e as prestadoras de serviços de telefonia móvel. O funcionamento do sistema consistia no fornecimento, pelas operadoras, de dados brutos sobre o volume de conexões realizadas com as Estações Rádio Base (antenas de telefonia celular), o que permite mensurar o adensamento demográfico em determinadas regiões e, assim, avaliar o grau de cumprimento do isolamento social imposto pelas autoridades sanitárias.

Em caso de descumprimento das medidas de isolamento, mensagens de alerta eram enviadas para os aparelhos localizados nas áreas com maior concentração populacional, com o intuito de conscientizar a população acerca da necessidade de distanciamento. Importante destacar que, no âmbito dessa iniciativa, não havia o fornecimento ou tratamento de dados pessoais identificáveis dos titulares dos aparelhos, de modo que a geração dos relatórios já respeitava os princípios gerais da Lei Geral de Proteção de Dados, como a finalidade, a necessidade e anonimização dos dados[65], muito embora a *vactio legis* do mencionado normativo tenha se encerrado por etapas em agosto de 2021[66].

Embora existam diversas aplicações da tecnologia de geolocalização que suscitam discussões relevantes no âmbito da proteção de dados pessoais, como, por exemplo, no direito do trabalho, em que a ferramenta é utilizada para aferir a assiduidade e cumprimento da jornada laboral, gerando conflitos entre o princípio da proteção de dados e a autonomia da vontade e do consentimento, a menção ao uso da geolocalização durante a pandemia da COVID-19 revela-se particularmente significativa.

A época, o cenário jurídico brasileiro relativo à proteção de dados ainda era claudicante. A Emenda Constitucional nº 115/2022, que positivou expressamente a proteção de dados como direito fundamental, ainda não havia sido promulgada. A Lei Geral de Proteção de Dados, como mencionado, encontrava-se em período de *vacatio legis*. E, por fim, a tutela dos dados pessoais

---

[65] ZANATTA, Rafael Augusto; BIONI, Bruno Ricardo; IGLESIAS KELLER, Clara; *et al*. **Os dados e o vírus: tensões jurídicas em torno da adoção de tecnologias de combate à Covid-19.** Revista Brasileira de Direitos Fundamentais & Justiça, v. 14, p. 231–256, 2020. Disponível em: <https://doi.org/10.30899/dfj.v14i1.1031>. Acesso em: 26 abr. 2025.

[66] A Lei entrou em vigor de maneira escalonada:
-Em 28 de dezembro de 2018, quanto aos arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B, que tratam da constituição da Autoridade Nacional de Proteção de Dados – ANPD e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade – CNPD;
- Em 18 de setembro de 2020, quanto aos demais artigos da Lei, com exceção dos dispositivos que tratam da aplicação de sanções administrativas; e
- Em 1º de agosto de 2021, quanto aos arts. 52, 53 e 54, que tratam das sanções administrativas.
BRASIL. ANPD. **Perguntas Frequentes – LGPD**. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/perguntas-frequentes/perguntas-frequentes/1-lei-geral-de-protecao-de-dados-pessoais-lgpd/1-3-quando-a-lgpd. Acesso em: 5 abr. 2025.

era extraída a partir de uma interpretação sistemática da Constituição, conferindo o tratamento constitucional implícito ao tema[67]. Como advertiram Clara Iglesias Keller e Jane Reis Gonçalves Pereira[68], esse contexto fragilizava a efetividade da proteção jurídica, especialmente diante da utilização expressiva de tecnologias de rastreamento durante a crise sanitária e a falta de respostas governamentais:

> As duly pointed out by some scholars, Brazil's GDPR-inspired data protection law does provide for fundamental rights that could help design these policies while still protecting individuals – a task that is challenged by the lack of a structured Data Protection Authority, but still, not impossible. However, even the application of this framework is currently threatened by legislative proposals to postpone the validity of the law. Initially fixed for next August, there is at least one bill of law under congress appreciation since last year proposing its postponement (possibly motivated by difficulties in structuring the data protection authority), a claim that has now been reinforced by the COVID-19 pandemic.

Assim, o enfrentamento da pandemia de COVID-19 fomentou o debate acerca do uso de tecnologias de coleta e tratamento de dados em face da necessidade de proteção de informações pessoais. A posterior criação da ANPD, as manifestações judiciais do STF e a entrada em vigor da LGPD em sua integralidade fortaleceram a imposição de molduras normativas a serem observadas para a legalidade e legitimidade à proteção de dados e seu tratamento[69].

---

[67] SARLET, Ingo Wolfgang. **Proteção de dados pessoais como direito fundamental na Constituição Federal brasileira de 1988: contributo para a construção de uma dogmática constitucionalmente adequada**. Direitos Fundamentais e Justiça, v. 14, 2020. Disponível em: <https://dfj.emnuvens.com.br/dfj/article/view/875>. Acesso em: 22 abr. 2025.

[68] KELLER, Clara Iglesias; PEREIRA, Jane Reis Gonçalves. **Data protection in times of Covid-19: the risks for surveillance in Brazil**. **Internet Policy Review**, 2020. Disponível em: <https://policyreview.info/articles/news/data-protection-times-covid-19-risks-surveillance-brazil/1462>. Acesso em: 28 abr. 2025.

[69] ZANATTA, Rafael Augusto; BIONI, Bruno Ricardo; IGLESIAS KELLER, Clara; *et al*. **Os dados e o vírus: tensões jurídicas em torno da adoção de tecnologias de combate à Covid-19**. **Revista Brasileira de Direitos Fundamentais & Justiça**, v. 14, p. 231–256, 2020. Disponível em: <https://doi.org/10.30899/dfj.v14i1.1031>. Acesso em: 26 abr. 2025.

CAPÍTULO 2: DIREITOS FUNDAMENTAIS: ESCOPO, LIMITES E CONFLITOS

2.1 RELEVÂNCIA DO ESTUDO DA TEORIA DOS DIREITOS FUNDAMENTAIS

Consoante a abordagem inaugural do tema, inarredável a conclusão da necessidade de uma revisitação das teorias acerca dos direitos fundamentais. Isso porque o nominado cotejo, conflito ou ponderação de princípios constitucionais, a depender do fenômeno e terminologia adotada, será exigido para enfrentamento da controvérsia sobre a utilização de geolocalização em investigações criminais.

De um lado, como dito alhures, encontram-se o princípio da proteção de dados, como decorrente da evolução das dimensões dos direitos da personalidade, bem como privacidade[70], aliados aos princípios da legalidade e devido processo legal que pautam o desenvolvimento do processo penal, todos insertos numa concepção de direitos de defesa contra o Estado na teoria dos status de Jellinek, frente aos princípios atinentes à segurança pública.

Neste sentido, embora se reconheça a relevância de distintas abordagens teóricas sobre os direitos fundamentais, adota-se como principal referência a teoria desenvolvida por Robert Alexy, notadamente no que se refere à ponderação de princípios, conforme exposta em sua obra "Teoria dos Direitos Fundamentais" (1986), traduzida por Virgílio Afonso da Silva[71]. A análise dialoga criticamente com a doutrina nacional, especialmente com as contribuições do próprio Virgílio Afonso da Silva e de outros doutrinadores do Direito Brasileiro, Jane Reis Gonçalves Pereira e Ingo Wolfgang Sarlet[72], cujas obras enriquecem a compreensão dos fundamentos, da eficácia e das funções dos direitos fundamentais no Estado Constitucional.

---

[70] SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional**. 10. ed. Porto Alegre: Livraria do Advogado, 2009.

[71] ALEXY, Robert, **Teoria dos direitos fundamentais**, [s.l.]: Malheiros São Paulo, 2008.

[72] A opção por dialogar prioritariamente com autores brasileiros decorre de uma escolha metodológica voltada ao foco e à delimitação da pesquisa. Entretanto, reconhece-se que o tema dos direitos fundamentais e suas aplicações em direitos específicos é objeto de amplo e profundo debate na doutrina nacional e estrangeira. Além dos autores já referidos no corpo do texto, merecem menção, no cenário brasileiro, **Daniel Sarmento** (Teoria dos direitos fundamentais igualdade constitucional: uma leitura; Direitos fundamentais e as relações privadas), **Ricardo Lobo Torres** (Tratado de Direito Constitucional Financeiro e Tributário), **Juliana Cesario Alvim Gomes** (Por um constitucionalismo difuso: cidadãos, movimentos sociais e o significado da Constituição), **Laura Schertel Mendes** (Privacidade, proteção de dados e defesa do consumidor) e **Adilson Moreira** (Pensando como um negro: ensaio de hermenêutica jurídica). No âmbito internacional, destacam-se as contribuições de **José Carlos Vieira de Andrade** (Direitos fundamentais e jurisdição constitucional), **Jônatas Machado** (Liberdade de expressão: dimensões constitucionais da esfera pública no sistema social) e **Susan Möller Okin** (Justice, gender, and the family) e diversos outros autores e autoras que oferecem perspectivas fundamentais para o aprofundamento do tema, com enfoque que incluem análise de igualdade, da proteção de dados, da liberdade de expressão, do direito à não discriminação e da justiça de gênero, além de promoverem maior pluralidade de visões sobre os direitos fundamentais.

Em seus ensaios, Alexy indica que a elaboração de uma teoria integrativa para os direitos fundamentais exige a abordagem de uma teoria estrutural analítica que perpasse pelos "*conceitos de direitos fundamentais, suas influências no sistema jurídico e na fundamentação no âmbito dos direitos fundamentais com vistas às tarefas práticas de uma teoria integrativa"*[73]. Como tal, esta reflexão enfrenta desafios consideráveis face as terminologias multifacetadas dos conceitos e os influxos porventura provenientes de ideologias, valores e, até mesmo, jurisprudenciais com suas bases empíricas e axiológicas, a exemplo daquelas exaradas pelo Tribunal Constitucional Federal Alemão.

A Teoria dos Direitos Fundamentais estrutural tem como principal objetivo conceder um refinamento conceitual e coerência na fundamentação dos direitos fundamentais, elementos essenciais para uma teoria integrativa, estabelecendo-se um *common ground* para a edificação de uma teoria cuja sistemática origine uma análise conceitual adequada, sem se afastar da consideração entre os elementos normativos e empíricos. De fato, partindo-se dessa premissa, uma visão sistemática evitaria arbitrariedades diante de sua objetividade e, ao mesmo tempo, garantiria a flexibilidade necessária para abarcar a dinâmica dos casos concretos.

Assim, a proposta de Robert Alexy representa um marco nos alicerces da construção de uma teoria dos direitos fundamentais integrativa, ao lançar uma estrutura analítica e normativa que que contribuem para a clareza conceitual e a fundamentação racional. No entanto, há desafios a serem transpassados, especialmente quanto à compatibilização do rigor analítico-conceitual e o seu "tratamento lógico" com a capacidade de abarcar os aspectos axiológicos e dinamicidade dos direitos fundamentais.

Nesse intuito, para os fins da presente dissertação, a definição dos direitos fundamentais, a delimitação de suas hipóteses de restrição e, por fim, a estrutura do procedimento de sopesamento e ponderação assumem papel fulcral na análise proposta. Esses elementos serão fundamentais para sustentar, de forma sistemática e coerente, os argumentos desenvolvidos ao longo do trabalho, na busca por compreender a constitucionalidade da utilização de dados de geolocalização no âmbito das investigações criminais.

---

[73] ALEXY, Robert. **Teoria dos direitos fundamentais**. Trad. Virgílio Afonso da Silva. 5ª ed. São Paulo : Malheiros Editora, 2008, p. 43.

2.2 CONCEITO DE DIREITOS FUNDAMENTAIS: DEFINIÇÃO E CARACTERÍSTICAS DOS DIREITOS FUNDAMENTAIS NA TEORIA DE ALEXY.

A lógica do estabelecimento de elementos analítico-conceituais já se insere na própria definição de norma, pois seria a conceituação fulcral da Ciência do Direito. Por conseguinte, essa definição, nas palavras de Robert Alexy[74], deve ser apta a retratar as "*decisões sobre o objeto e o método da disciplina*". E, por decorrência dessa razão, conforme exposto na construção do sistema, as normas deveriam consolidar a base rígida sobre os quais as validades das teorias se desenvolveriam, mas, também, deveriam possuir a maleabilidade para acomodar o sentido mais amplo concedido ao seu conceito.

Seguindo-se essa mesma compreensão, tem-se uma relevante distinção contida na relação entre direitos fundamentais e normas de direitos fundamentais. Muito embora a existência de um direito fundamental dependa de uma norma correspondente que o garanta, o inverso nem sempre se comprova, isto é, nem toda norma de direito fundamental equivale a um direito fundamental específico. Essa ausência de ambivalência impacta diretamente a interpretação constitucional, evitando-se que a norma de direitos fundamentais não seja cingida apenas a um respectivo direito fundamental e, por outro lado, este não seja tratado como mera abstração ou princípios políticos desprovidos de eficácia jurídica.

Consistente com esse entendimento, Jane Gonçalves Reis Pereira[75] estabelece como premissa que a norma de direito fundamental é resultado da atividade interpretativa sobre um enunciado textual, sendo o produto do sentido semântico desse enunciado. A partir da concepção semântica de norma adotada, é possível distinguir dois tipos de normas de direitos fundamentais conforme o grau de complexidade da atividade interpretativa: as normas expressamente estatuídas e as normas adscritas. As primeiras correspondem aos casos em que o conteúdo normativo pode ser diretamente extraído do texto constitucional, por meio de uma interpretação literal, com mínima intervenção do intérprete. Já as normas adscritas decorrem de um processo hermenêutico mais elaborado, em que o sentido normativo é construído a partir da identificação de conceitos indeterminados, da interpretação sistemática de múltiplos dispositivos constitucionais ou mesmo da identificação de direitos implícitos.

---

[74] *Ibid*., p. 52.

[75] PEREIRA, Jane Reis G. **Interpretação constitucional e direitos fundamentais**. 2. ed. Rio de Janeiro: Saraiva Jur, 2017. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788553600281/>. Acesso em: 30 abr. 2025.

Essa concepção se coaduna com a distinção estabelecida por Alexy, para quem enunciado poderia ser identificado como o texto ou excerto que contenha o comando ou se extraia a diretiva. Citando, Hans J. Wolff e Otto Bachof[76], Alexy adere ao conceito do termo norma significar o *"conteúdo (sentido) imperativo expresso por um 'enunciado jurídico*'". Mais adiante, o autor conclui que a sua proposta para o conceito de norma se coaduna com a ideia de Hans Kelsen, no sentido de se designar algo que "*deve ser ou acontecer, especialmente que uma pessoa deve se comportar de uma determinada maneira*", apenas destacada dos elementos metalinguísticos (vontade, ato de vontade)[77].

Fixadas essas premissas, há que se perquirir os critérios que fazem um enunciado normativo seja considerado uma disposição de direito fundamental. Um critério apontado como pertinente de análise seria aquele proposto por Carl Schmitt[78], para quem haveria um elemento *substancial* ou *estrutural no direito fundamental,* ou seja, os direitos fundamentais seriam "*apenas aqueles direitos que constituem o fundamento do próprio Estado e que, por isso e como tal, são reconhecidos pela Constituição*".

O apontamento a ser efetuado a este critério adotado está atrelado à vinculação dos direitos fundamentais à própria essência do Estado. Estes direitos estreitamente identificados seriam nominados *direitos fundamentais em sentido estrito.* Nesse aspecto, só estariam abrangidos entre os direitos fundamentais de um Estado "Liberal" aqueles direitos individuais voltados à "liberdade".

Ingo Wolfgang Sarlet reconhece a relação indissociável entre a conceituação dos direitos fundamentais e as estruturas constitucionais e estatais que lhes dão suporte. Para o autor, os direitos fundamentais, para além de seu aspecto meramente formal, integram o núcleo material das Constituições, funcionando como sua "base e fundamento" e orientando a conformação do Estado de Direito. Nessa perspectiva, os direitos fundamentais projetam a sua dimensão negativa da atuação estatal, ao estabelecer limites ao poder incidente, e densificam os valores materiais que os informam. Ao promoverem as liberdades individuais, os direitos fundamentais conferem legitimidade à atuação do Estado que os garante e contribuem para a conformação da ordem jurídica[79].

---

[76] WOLFF HJ, BACHOF O: **Verwaltungsrecht** I, 345 (9th ed, 1974), p. 115 *apud* ALEXY, Robert. **Teoria dos direitos fundamentais**. Trad. Virgílio Afonso da Silva. 5ª ed. São Paulo : Malheiros Editora, 2008, p. 53.

[77] ALEXY, Robert. **Teoria dos direitos fundamentais**. Trad. Virgílio Afonso da Silva. 5ª ed. São Paulo : Malheiros Editora, 2008, p. 53.

[78] Carl Schmitt, "Grundrechte und Grundpflichten (1932)", in, do mesmo autor, Verfassungsrechtliche Aufsiitze, 2' ed., Berlin: Duncker & Humblot, 1973, p. 190.

[79] SARLET, **A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional**, p. 60.

Alexy, em seu turno, propõe admitir ser possível a existência de direitos fundamentais puramente estrutural, isto é, reputar-se-ia como norma de direito fundamental apenas aqueles que garantissem direitos subjetivos expressamente positivados na Constituição alemã, no caso. A preocupação daí decorrente se quedaria justamente em como interpretar as normas que possuíssem "*conexão sistemática ou textual com as normas que garantem direitos subjetivos*"[80].

Para resolver este novo impasse acerca da restrição conceitual das normas de direito fundamental apenas àquelas identificadas como descritas nos enunciados da Constituição, cujo comando normativo é diretamente estabelecido, o jurista alemão sugere a categorização de "normas de direitos fundamentais atribuídas". Com o intuito de conceber maior amplitude ao rol das normas entendidas como de direito fundamental, são criadas as relações de refinamento ou fundamentação para estabelecer uma conexão entre uma norma de direito fundamental anterior (positivada) com a norma posterior, da qual se extrai o seu fundamento de validade. Esse liame busca suprir a necessidade de delimitação semântica diante da abertura estrutural promovida pelos enunciados das normas de direito fundamental, possibilitando, assim, o surgimento das denominadas normas de direito fundamental atribuídas[81].

Virgílio Afonso da Silva[82] adota uma abordagem mais pragmática quanto à definição dos direitos fundamentais em sua obra Direito Constitucional Brasileiro. Sua concepção é predominantemente formal, o que pode ser considerada, em certa medida, reducionista. Para o autor, são direitos fundamentais aqueles expressamente previstos e positivados na Constituição Federal de 1988, notadamente os compreendidos entre os artigos 5º e 17, independentemente das teorias que lhes dão fundamento. Ainda assim, o autor reconhece que esse rol não é exaustivo admitindo a possibilidade de reconhecimento de direitos fundamentais não expressamente previstos no texto constitucional à luz do disposto no §2º do artigo 5º da CF/88, destacando a relevância de outras fontes normativas, como os tratados internacionais de direitos humanos.

Essa dinâmica das relações para estabelecimento do conceito de normas de direito fundamental pode ser transplantada para a análise do caso proposto no presente trabalho. Inicialmente, considerando as dimensões dos direitos fundamentais constantes da teoria geral

---

[80] ALEXY, Robert. **Teoria dos direitos fundamentais**. Trad. Virgílio Afonso da Silva. 5ª ed. São Paulo : Malheiros Editora, 2008, p. 68.

[81] ALEXY, Robert. **Teoria dos direitos fundamentais**. Trad. Virgílio Afonso da Silva. 5ª ed. São Paulo : Malheiros Editora, 2008, p.ALEXY, **Teoria dos direitos fundamentais,** p.72.

[82] SILVA, Virgílio Afonso da. **Direito constitucional brasileiro**. São Paulo: Edusp. 2021.

dos direitos fundamentais de Ingo Sarlet[83], antes da positivação do direito constitucional da proteção de dados por meio da Emenda Constitucional n.º 115/2022, tinha-se que a garantia do adequado tratamento das informações pessoais decorria do direito da privacidade. O Direito da Privacidade, por sua vez e nesse contexto, era interpretado em seu viés patrimonialista conjugado com o direito de ser deixado a só, debate inaugurado com a edição do artigo *The Right to Privacy* de Warren e Brandeis[84] (1890).

De forma objetiva, considerando que o Direito à Privacidade será examinado em capítulo próprio, o enquadramento do direito à proteção de dados, especialmente em sua relação com outros direitos fundamentais, como a segurança pública, tem sido historicamente tratado como um desdobramento da privacidade. Essa visão tradicional, que vincula a proteção de dados exclusivamente a uma dimensão da norma fundamental constitucional expressamente assegurada na Constituição Federal, pode restringir sua compreensão como direito autônomo.

Ao analisar as decisões proferidas pelas Cortes, observa-se que a ponderação entre direitos fundamentais frequentemente resulta na restrição do direito à proteção de dados, sob o argumento de que o núcleo essencial da norma constitucional tutelada seria a privacidade, e não a garantia da autodeterminação informativa. Essa abordagem, embora ainda recorrente, merece reflexão crítica, pois a Emenda Constitucional nº 115/2022 conferiu expressamente ao direito à proteção de dados o status de direito fundamental autônomo, indicando um possível deslocamento de sua fundamentação exclusivamente na privacidade para um conceito mais amplo, que abarca a tutela da identidade digital e da autodeterminação informacional dos indivíduos.

Entretanto, a constitucionalização desse direito não parece ter promovido, até o momento, mudanças significativas na forma como os tribunais enfrentam a ponderação entre a proteção de dados e outros direitos. Como se observa no voto proferido pelo Ministro Edson Fachin do Supremo Tribunal Federal na ADI 5.642, a interpretação predominante ainda tende a considerar a proteção de dados como uma decorrência do direito à privacidade, particularmente ao tratar de registros de dados estáticos, em oposição a situações que envolvem a manipulação indevida de dados pessoais sensíveis. Essa concepção pode gerar um viés interpretativo que subestima a autonomia do direito à proteção de dados, relegando sua tutela à

[83] SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional**. 10. ed. Porto Alegre: Livraria do Advogado, 2009.
[84] WARREN, Samuel; BRANDEIS, Louis. **The Right to Privacy**. Civilistica.com, v. 2, n. 3, p. 1–22, 2013. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/127>. Acesso em: 18 jun. 2025

necessidade de demonstração de violação direta à privacidade, o que nem sempre reflete a complexidade das ameaças contemporâneas à informação pessoal.

Dessa forma, a evolução da jurisprudência brasileira ainda precisa consolidar a distinção entre privacidade e proteção de dados, reconhecendo que este último não se resume à salvaguarda de informações pessoais contra exposições indevidas, mas também envolve o direito de o indivíduo controlar o uso e a circulação de seus dados. A manutenção da interpretação restritiva pode comprometer a efetividade da proteção de dados como direito fundamental, especialmente em um cenário em que o tratamento massivo de informações por entes públicos e privados impacta diretamente a autonomia e a liberdade individual. Nesse sentido que a sistematização da Teoria de Robert Alexy promove um adequado enquadramento e valoração das normas de direito fundamental.

2.3 PRINCÍPIOS E REGRAS

A separação conceitual entre regras e princípios no contexto das normas de direitos fundamentais revela-se indispensável para o desenvolvimento crítico das teorias constitucionais. Essa diferenciação não apenas contribui para a compreensão das diversas funções desempenhadas por essas categorias normativas, mas também orienta a definição de critérios mais precisos para a solução de conflitos e para o exame das restrições dos direitos impostos aos direitos fundamentais, permitindo maior rigor na aplicação dos mecanismos de ponderação e proporcionalidade. De fato, não são raras as ocasiões nas quais haveria a identificação das normas de direitos fundamentais como princípios, bem como haver sua referência como se tratasse de regras, principalmente neste último caso quando o intuito era conceber força normativa aos enunciados positivados na Constituição. Para Robert Alexy[85], a classificação de normas abrangeria tanto os princípios, quanto as regras, na medida em que seus enunciados disciplinam o *dever ser*.

Assim, muito embora sejam inúmeras as tentativas de descrever elementos distintivos entre essas duas espécies de normas, a pluralidade de critérios inviabilizaria tal tarefa. A exemplo, poder-se-ia afirmar que o princípio seria uma norma dotada de uma generalidade mais elevada, em contraposição às regras, cuja generalidade seria considerada mais baixa, isto é, seriam normas com maior especificidade em seu espectro de incidência. Josef-Esser, citado por

---

[85] ALEXY, Robert. **Teoria dos direitos fundamentais**. Trad. Virgílio Afonso da Silva. 5ª ed. São Paulo : Editora Malheiros, 2008, p. 87.

Alexy[86], diria que "*princípio (...) não é, ele mesmo, 'diretiva', mas fundamento, critério e justificação da diretiva*" (*Grundsatz und Norm*, p. 51).

Contudo, seguindo o entendimento do autor, a teoria mais adequada para subsidiar a distinção entre regra e princípio seria aquela baseada na diferença qualitativa dos institutos. Então, para Alexy, nos exatos termos de sua teoria, princípios são mandamentos de otimização (...) *"que ordenam que algo seja realizado na maior medida possível dentro das possibilidades jurídicas e fáticas existentes"*, (...) cujo "*âmbito das possibilidades jurídicas é determinado pelos princípios e regras colidentes*"[87].

Por sua vez, as regras são submetidas a um caráter binário de aplicação: ou são aplicadas em sua integralidade, ou não se aplicam. Em sua obra *Levando os Direitos a Sério*, Ronaldo Dworkin[88] igualmente ressalta essa diferença entre princípio jurídico e as regras ao afirmar que estas "*são aplicáveis à maneira do tudo-ou-nada (...) ou a regra é válida, e neste caso a resposta que ela fornece deve ser aceita, ou não é válida, e neste caso em nada contribui para a decisão*". Conclui-se, portanto, que o juiz, ao aplicar a regra de incidência, deve verificar objetivamente sua subsunção à hipótese vertente, restringindo-se ao enunciado da norma e a sua adequação ao fato. A margem de discricionariedade do juiz na apreciação de outros aspectos é limitada, vez que eventuais exceções à regra devem ser expressamente previstas em seu enunciado, do contrário, a norma seria considerada incompleta em sua descrição[89].

Essa linha de pensamento, também desenvolvida por Jane Reis Gonçalves Pereira[90], conduz à compreensão de que o princípio deve ser entendido como um *standard* cuja observância não se justifica por razões de conveniências políticas, econômicas ou sociais, mas por refletir uma exigência fundada em valores inerentes à moralidade, justiça ou equidade, tornando sua análise sistemática em uma ponderação axiológica sem uma resposta exata a ser obtida.

Robert Alexy ressalta que, para ambas as espécies normativas, o exercício da lógica deôntica, na análise do *dever ser* em relação às obrigações, permissões ou proibições, não podem resultar em concretizações estanques ou isoladas e incompatíveis entre si, bem como considerando o próprio sistema de normas de mesma natureza nas quais estão inseridas. A

---

[86] *Ibid*., p. 51.
[87] *Ibid*., p. 90.
[88] DWORKIN, Ronald. **Levando os direitos a sério**. Tradução: Nelson Boeira. São Paulo: Martins Fontes, 2002.
[89] *Ibid*., p. 26.
[90] PEREIRA, Jane Reis G. **Interpretação constitucional e direitos fundamentais**. 2. ed. Rio de Janeiro: Saraiva Jur, 2017. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788553600281/>. Acesso em: 30 abr. 2025.

harmonização para a aplicação dessas normas constitui elemento diferenciador entre regras e princípios, diante da distinção de procedimentos exigidos para sua efetivação.

Ademais, é imperioso observar a especificidade da terminologia empregada para descrever o choque entre os princípios e entre as regras. No caso dos princípios, ocorrendo a *colisão* dessas normas, ambos poderão permanecer válidos, mas necessita-se haver a ponderação no cotejo de cada um deles, conforme as circunstâncias fáticas. Por outro lado, quando se versar acerca do confronto entre regras, verifica-se o estabelecimento de um *conflito* aparente de regras, cuja solução acarreta a invalidação de uma das normas em favor outra, em face de sua incompatibilidade, ressalvada uma excepcionalidade formalmente estatuída.

Diante dessa premissa, na ausência da cláusula de exceção, a superação do conflito pode ser alcançada por meio da aplicação de critérios de especialidade, priorizando a norma mais específica, ou de temporalidade, dando prevalência à norma posterior. Contudo, a questão, ao fim e ao cabo, possui desfecho no âmbito de validade das normas, vez que as regras não podem ser válidas e contraditórias ao mesmo tempo.

De fato, no caso dos princípios, na sua acepção de mandamentos de otimização, a colisão implica na submissão de uma dessas normas em relação a outra confrontada, sem necessariamente, acarretar a sua invalidação. Adota-se para a solução, o critério de precedência de um princípio sobre o outro, considerando-se o seu peso na incidência do caso em hipótese. Robert Alexy[91] faz remissão à obra de Ronald Dworkin[92] ao afirmar que os princípios possuem *dimensão* de peso ou importância, com o fito de determinar a sua precedência diante da *colisão.* Nas palavras do jurista estadunidense tem-se que:

> Quando princípios se intercruzam, aquele que vai resolver o conflito tem de levar em conta a força relativa de cada um. Esta não pode ser, por certo, uma mensuração exata e o julgamento que determina que um princípio ou uma política particular é mais importante que outra frequentemente será objeto de controvérsia.
> Não obstante, essa dimensão é uma parte integrante do conceito de um princípio, de modo que faz sentido perguntar que peso ele tem ou quão importante ele é[93].

Conclui-se que o saneamento das colisões entre princípios demanda um processo de ponderação acurado, no qual considera-se a dimensão de peso ou a sua relevância nas hipóteses de incidência. Esse processo, que dialoga, em parte, com a teoria de Ronald Dworkin, pressupõe um julgamento que, embora não possa ser realizado objetivamente, estando no âmbito de discricionariedade do juízo, deve garantir decisões jurídicas que equilibrem os valores

---

[91] ALEXY, Robert. **Teoria dos direitos fundamentais**. Trad. Virgílio Afonso da Silva. 5ª ed. São Paulo : Editora Malheiros, 2008.
[92] DWORKIN, Ronald. **Levando os direitos a sério**. Tradução: Nelson Boeira. São Paulo: Martins Fontes, 2002.
[93] *Ibid.*, p. 42–43.

constitucionais em debate. Essa medida visa garantir a máxima efetividade dos princípios na maior medida possível, diante no cenário jurídico apresentado.

2.4 RESTRIÇÕES E LIMITES AOS DIREITOS FUNDAMENTAIS

O estudo da restrição dos direitos fundamentais será relevante para o dimensionamento adequado dos aspectos negativos das garantias dos direitos fundamentais que impedem a intervenção do Estado em busca da concretização de seu *jus puniendi*. Não obstante o enunciado constitucional de que ninguém será obrigado a fazer ou deixar de fazer, senão em virtude de lei, o princípio da legalidade, pilar do Estado Democrático de Direito, apresenta-se tanto em sentido amplo, como princípio estruturante do direito material e processual penal, quanto em sentido restrito, associado a reserva legal, determinando a prévia descrição da conduta criminosa e, consequentemente, sua sanção. E, nesse cenário, quando se trata do emprego de novas tecnologias, como a geolocalização, há uma lacuna normativa que impacta a higidez dos procedimentos carreados pelas autoridades estatais responsáveis pela persecução penal, além de promoverem a insegurança aos indivíduos que podem ter seus direitos à privacidade e proteção de dados violados.

A obtenção de elementos probatórios lícitos e legítimos é fundamento basilar do devido processo legal, porém a ausência de disciplina específica sobre a coleta e uso de dados de geolocalização exige, para o uso dessa ferramenta, a restrição ou limite do direito fundamental à proteção de dados. Por essa razão, para o debate das questões constitucionais atinentes ao Direito Processual Penal na presente dissertação, torna-se imperioso a contextualização da Teoria da Restrição a Direitos Fundamentais. Estabelecidas as premissas teóricas, será possível analisar se as restrições acontecem de forma arbitrária ou fundamentadas, obedecendo critérios de proporcionalidade, necessidade e adequação.

Dessa forma, a Teoria da Restrição dos Direitos Fundamentais insere-se num arcabouço mais amplo que permite a apuração sobre os limites e condições nas quais o Estado pode restringir direitos fundamentais, cotejando-se o interesse público da segurança frente a salvaguarda das liberdades individuais.

Nesse sentido, Robert Alexy constrói sua teoria da restrição a direitos fundamentais considerando o caráter *prima facie* dos princípios e regras. O caráter *prima facie* dos princípios decorre especialmente da própria definição alhures referida, no sentido de serem mandamentos de otimização, melhor dizer, *exigem que algo seja realizado na maior medida possível dentro*

das possibilidades jurídicas e fáticas existentes, eles não contêm um mandamento definitivo, mas apenas prima facie[94].

Considerando estas possibilidades, a incidência dos princípios deve pressupor que esta norma compreende valores e fundamentos que podem ser contrapostos por outras normas de igual envergadura axiológica e de sentido oposto. Por conseguinte, este cotejo determina a amplitude alcançada pelos princípios. Forçoso concluir, por tanto, que os princípios possuem, à primeira vista, uma validade verificada de plano, mas que pode ser mitigada por outros igualmente válidos e aplicáveis nas mesmas circunstâncias específicas.

No contexto retratado do estudo, os princípios à privacidade e proteção de dados possuem validade *prima facie*, contudo não são absolutos ou incondicionais, na medida em que podem colidir com o princípio da segurança pública, podendo-se cogitar a preponderância deste último face àqueles, desde que justificada por razões concretas, como a gravidade do crime investigado, o interesse público envolvido e a necessidade da medida para a proteção da ordem pública.

Sob essa perspectiva acerca da extensão do alcance dos princípios, de forma natural, estabelecem-se as discussões sobre a teoria da restrição dos direitos fundamentais, a qual aprofunda-se sobre a análise sobre o método e em que medida essas restrições podem ser legitimamente impostas aos princípios. Ao fixar a premissa do caráter *prima facie* dos princípios, Alexy busca estruturar a coerência e a integridade do sistema.

Buscando a epistemologia da restrição de direitos fundamentais, Alexy desenvolve razão semelhante àquela contida na relação entre os princípios da identidade e da não-contradição para a definição de um elemento, dentro do estudo da filosofia.

A lógica, como área da filosofia, possui como um de seus conceitos fundamentais para a elaboração de suas proposições o princípio da identidade, segundo o qual um objeto seria igual a ele mesmo, isto é, um elemento só pode ser idêntico a si, não podendo ser outra coisa. Por essa razão, a própria definição do objeto e sua essência trazem todas as características capazes de descrevê-lo. Negar a sua unidade seria desconstruir sua identidade.

De outro lado, o princípio da não-contradição seria a proposição necessária para confirmar a razão lógica trazida para o princípio da identidade. Consoante aquele primeiro princípio, um objeto não pode "ser e não ser" ao mesmo tempo, isto é, uma proposição "A" não poderia ser simultaneamente verdadeira e falsa, ou "não-A". Como arrebatava Aristóteles: "*é impossível que o mesmo seja atribuído e não seja atribuído ao mesmo tempo a um mesmo e*

[94] ALEXY, Robert. **Teoria dos direitos fundamentais**. Trad. Virgílio Afonso da Silva. 5ª ed. São Paulo : Editora Malheiros, 2008, p. 104.

conforme o mesmo aspecto"[95]. Assim, haveria duas possibilidades de definição do objeto: (i) Ele poderia ser definido pelos seus próprios atributos; ou (ii) por coerência lógica e exclusão, o objeto seria o remanescente de tudo aquilo que não fosse o objeto (não-A).

Imbuído dessa lógica, Alexy sustenta que, para admitir a existência de uma restrição a um direito, é necessário pressupor: (i) um direito originalmente pleno e sem limites; (ii) uma restrição imposta a esse direito; e (iii) um direito resultante dessa restrição, agora modificado em seu alcance. Essa estrutura lógica, conforme defendida por Alexy e Sarlet, fundamenta a **teoria externa** da restrição dos direitos fundamentais. Ainda que os direitos fundamentais sejam apresentados no ordenamento jurídico já em sua forma restringida, é necessário concebê-los, inicialmente em sua forma plena, isto é, sem limitações. Nesse sistema, a contenção do direito só se revelaria necessária para harmonizar os direitos dos indivíduos e coletivos, bem como para garantir a compatibilização do sistema normativo.

Ingo Sarlet, ao discorrer sobre a teoria externa, atribui a ela o entendimento de haver *um direito em si, ilimitado, que, mediante a imposição de eventuais restrições, se converte em um direito limitado.* Dessa forma, ele ressalta a distinção do caráter *prima facie* original do direito e o direito restringido que dele resulta[96].

Por outro lado, a **teoria interna** apregoa não haver a distinção entre o direito e sua restrição. Nessa perspectiva, o direito já possui um conteúdo determinado, cujas limitações são imanentes ao seu próprio núcleo normativo. Por conseguinte, enquanto a teoria externa discute a amplitude e limitação do direito a partir da imposição de restrições de modo a harmonizar as zonas de contato, a teoria interna foca na determinação prévia de seu conteúdo normativo, cujas fronteiras implícitas delimitam a sua incidência, mitigando a necessidade de adequação das normas. Logo, a discussão não se volta à amplitude ou extensão do direito, mas sim o seu próprio conteúdo.

Estabelecidas as teorias, Ingo Sarlet[97], ao tratar de limites aos direitos fundamentais, faz menção, citando Jorge Reis Novaes, a um sentido mais amplo sobre limite e aduz que estes são "*ações ou omissões dos poderes públicos ou de particulares que dificultem, reduzam ou eliminem o acesso ao bem jurídico protegido, afetando seu exercício (aspecto subjetivo) e/ou diminuindo deveres estatais de garantia e promoção (aspecto objetivo)".*

---

[95] ARISTÓTELES, **Clássicos da Filosofia: Cadernos de Tradução n.º 14Metafísica, livros IV e VI**, Campinas: Editora Unicamp, 2003.
[96] SARLET, **A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional**.
[97] *Ibid.*, p. 387.

Em seu turno, Robert Alexy demonstra predileção pela teoria externa, embora teça argumentos analisando exemplos da Constituição alemã sob o enfoque de ambas as teorias, como forma de perquirir a mais adequada. Com base nesse viés, o jurista filósofo alemão define restrição a direitos fundamentais como "***normas*** *que restringem uma posição prima facie de direito fundamental"*[98]. Partindo dessa premissa, parte a investigar as características dessa norma e sua adequação à Constituição. O ponto fulcral vindicado é que essa norma restritiva, obrigatoriamente, deve ser compatível com a Carta Magna. Essas normas, então, podem ser classificadas como de duas espécies: (i) *normas de competência, que estabelecem reserva legal, isto é, não são restrições per si, apenas autorizam, em abstrato, a restringibilidade*; e (ii) *normas restritivas mandatórias ou proibitivas*, que estabelecem, de forma peremptória, aquilo que Alexy defini como uma "*não-liberdade ou a um não-direito definitivo*", restringindo a extensão *prima facie* do direito fundamental afetado.

Em obra intitulada "*Interpretação constitucional e direitos fundamentais",* Jane Reis Gonçalves Pereira destaca, ao versar sobre o limite dos limites dos direitos fundamentais que, hodiernamente, consolidou a compreensão de que as restrições aos direitos fundamentais só poderiam ser instituídas por meio de uma *lei em sentido formal*, essa concebida como resultado de um processo legislativo exercido por uma autoridade constitucionalmente competente para tanto. Esse entendimento aplicar-se-ia tanto para os limites expressamente dispostos na Constituição, bem como aqueles "*implicitamente autorizados*"[99]. Nas exatas palavras da autora que expressão seu entendimento:

> No sistema constitucional brasileiro, como se sabe, não há um conjunto de preceitos regulando especificamente a questão das limitações aos direitos fundamentais. Não obstante, o art. 5o, II, da Constituição Federal estampa, de forma genérica, o princípio da legalidade na sua dimensão de reserva da lei. Além disso, é possível extrair a exigência de lei formal em matéria de direitos fundamentais dos dispositivos constitucionais que regulam a participação do Executivo na atividade legislativa. (...) Além disso, a reserva de lei é uma consequência lógica da circunstância de a Constituição exigir, em relação aos direitos expressamente sujeitos à reserva legal, a forma legislativa. Como já se destacou, se tal exigência é aplicável nas hipóteses em que a Constituição autoriza expressamente a edição de lei restritiva, seria ilógico entendê-la dispensável quanto às restrições não expressamente autorizadas pela Constituição[100].

Considerando os diversos aspectos abordados nesta seção, poder-se-ia afirmar que não se cogita a tese de existir de um direito fundamental de caráter absoluto. Virgílio Afonso da

---

[98] ALEXY, Robert. **Teoria dos direitos fundamentais**. Trad. Virgílio Afonso da Silva. 5ª ed. São Paulo : Editora Malheiros, 2008, p. 281–282.

[99] PEREIRA, Jane Reis G. **Interpretação constitucional e direitos fundamentais**. 2. ed. Rio de Janeiro: Saraiva Jur, 2017. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788553600281/>. Acesso em: 30 abr. 2025, p. 344.

[100] *Ibid*., p. 347–348.

Silva[101] observa que o Supremo Tribunal Federal tem reiteradamente afirmado que a aplicação dos direitos fundamentais pode e deve envolver restrições quando colocados em situação de colisão com outros direitos de mesma natureza. Porém, o autor adverte que não se deve presumir, de modo irrestrito, a possibilidade de limitação de todos os direitos fundamentais. Em certos casos, o caráter absoluto de determinados direitos decorre da própria interpretação conferida pela coerência e unidade da Constituição. Entre os exemplos de direitos reconhecidos como dotados de caráter absoluto, o autor menciona, além da vedação à tortura e da proibição à extradição de brasileiro nato, as garantias da reserva legal e da anterioridade penal, cujo caráter inflexível tem sido reafirmado pelo próprio STF. Ainda que esse posicionamento seja objeto de controvérsia doutrinária, eles se mostram particularmente relevante para os objetivos deste trabalho, uma vez que a resposta ao problema de pesquisa proposto pressupõe, em um primeiro momento, a identificação de uma colisão entre princípios em sentido estrito, seguida da necessidade, condicionada excepcional, de restrição à proteção de dados pessoais, sob controle judicial e à luz da proporcionalidade.

Assim, as reflexões sobre os limites dos direitos fundamentais tornam-se especialmente relevantes diante da ausência de norma específica que regulamente o uso de dados de localização para fins de instrução criminal e confirmação de autoria. Como já afirmado, há apenas a ressalvada para àquelas hipóteses previstas no art. 13-B do Código de Processo Penal, incluídos pela Lei n.º 13.344/2016, para a identificação da localização da vítima e de suposto agressor no caso dos crimes com privação de liberdade. Assim, a definição dos parâmetros legítimos de restrição ao direito da proteção de dados dependeria, necessariamente, na aplicação criteriosa da teoria dos limites e observação do princípio da legalidade e regular processo penal.

2.5 TRATAMENTO DA COLISÃO DOS DIREITOS FUNDAMENTAIS

Antes de se avançar na análise das técnicas de resolução de colisão entre princípios constitucionais, é necessário esclarecer em que circunstâncias se configura, efetivamente, uma colisão entre direitos fundamentais. Conforme destacam Mendes e Branco[102], as colisões ocorrem quando o exercício de direitos por diferentes titulares, ambos amparados por normas constitucionais, leva a necessidade de delimitação recíproca de seus alcances.

---

[101] SILVA, Virgílio Afonso da. **Direito constitucional brasileiro**. São Paulo: Edusp. 2021.
[102] MENDES, Gilmar Ferreira; COELHO, Inocêncio Mártires; BRANCO, Paulo Gustavo Gonet, **Curso de Direito Constitucional**, 2. ed. São Paulo: Saraiva, 2008.

Importa ressaltar que a Constituição deve ser compreendida como um sistema normativo uno e coerente, cujas normas se integram harmonicamente. Assim, não se trata de uma contradição normativa entre direitos fundamentais, mas sim de um conflito prático na aplicação simultânea de pretensões jurídicas igualmente protegidas. Em determinadas situações, no entanto, os autores indicam que não se verifica uma colisão verdadeira, mas sim apenas um conflito aparente, quando a conduta em análise não está abarcada pelo âmbito de proteção do direito fundamental invocado. Nesses casos, a questão a ser enfrentada consiste em determinar se a liberdade de ação reivindicada se insere, de fato, no âmbito de proteção constitucional do direito fundamental alegado.

Jane Reis Gonçalves Pereira[103], na mesma linha, sustenta que as colisões entre os direitos fundamentais configuram antinomias entre normas constitucionais do tipo parcial-parcial. Por sua natureza constitucional, esses conflitos não admitem a aplicação dos critérios tradicionais de solução de antinomias normativas, como a hierarquia, a especialidade ou anterioridade temporal. Sendo do tipo parcial-parcial, a representação gráfica da área de incidência de cada norma, bem como de sua sobreposição, pode ser ilustrada por Diagramas de Venn[104], nos quais a zona de interseção indica precisamente o ponto de colisão normativa. Fora dessa área de interseção, permanecem as zonas de atuação autônoma das normas, nas quais não há conflito.

Ademais, conforme destaca Gilmar Ferreira Mendes, Ministro Decano do Supremo Tribunal Federal, em sua obra "*Direitos fundamentais e controle de constitucionalidade*", o âmbito de proteção de um direito fundamental pode ser definido como:

> O âmbito de proteção de um direito fundamental abrange os diferentes pressupostos fáticos e jurídicos contemplados na norma jurídica (v.g., reunir-se sob determinadas condições) e a consequência comum, a proteção fundamental. Descrevem-se os bens ou objetos protegidos ou garantidos pelos direitos fundamentais. Nos direitos fundamentais de proteção ou de defesa cuida-se de normas sobre elementos básicos de determinadas ações ou condutas explicitadas de forma lapidar: propriedade, liberdade de imprensa, inviolabilidade do domicílio, dentre outros[105].

---

[103] PEREIRA, Jane Reis G. **Interpretação constitucional e direitos fundamentais**. 2. ed. Rio de Janeiro: Saraiva Jur, 2017. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788553600281/>. Acesso em: 30 abr. 2025.

[104] Um Diagrama de Venn é uma ilustração que usa círculos sobrepostos para mostrar a relação lógica entre dois ou mais conjuntos de itens. Círculos que se sobrepõem têm algo em comum, enquanto círculos que não se sobrepõem não compartilham nenhuma característica dos outros círculos. KENTON, Will. What Is a Venn Diagram? Meaning, Examples, and Uses. 2024 Disponível em: https://www-investopedia-com.translate.goog/terms/v/venn-diagram.asp?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt&_x_tr_pto=sge. Acesso em 30 de abril de 2025.

[105] MENDES, Gilmar Ferreira, **Direitos fundamentais e controle de constitucionalidade: estudos de direito constitucional**, 4. ed. São Paulo: Saraiva, 2011, p. 34.

Assim, dentro dessa moldura teórica, é possível identificar as colisões de direitos fundamentais em sentido estrito, caracterizadas pelo confronto entre dois direitos fundamentais titularizados por sujeitos distintos, cujos interesses contrapostos ou antagônicos ensejam limitações a satisfação plena do outro.

Por outro lado, configuram-se como colisões em sentido amplo aquelas em que um direito fundamental subjetivo se contrapõe a um princípio constitucional objetivo, relacionado a bens e valores que se projetam à coletividade como um todo. Nessa segunda categoria que se insere o conflito entre direito fundamental à proteção de dados pessoais, expressão da autodeterminação informativa, e o interesse estatal na persecução penal. Embora haja um direito fundamental subjetivo apenas em relação ao direito à proteção de dados, ambos os polos possuem natureza principiológicas, exigindo a sua otimização, conforme as possibilidades fáticas e jurídicas do caso concreto. A superação desse tipo de colisão demanda a utilização do método da ponderação, orientado pelo princípio da proporcionalidade pela busca da máxima concretização dos valores constitucionais envolvidos[106].

Cumpre destacar, como adverte Jane Reis Gonçalves Pereira[107], que a ponderação de direitos fundamentais não se confunde, e tampouco pode ser reduzida, à técnica hermenêutica do raciocínio jurídico dialético destinado à interpretação e solução dos casos concretos. A ponderação, enquanto método de resolução de colisão entre normas principiológicas, pressupõe a realização de um juízo de otimização, por meio do qual se avalia a adequação e utilidade da restrição imposta a um dos direitos em conflito, bem como a existência de meios alternativos que permitam a realização do fim legítimo e com o menor sacrifício ao outro direito envolvido. Por fim, é necessário considerar a relevância ou peso de cada direito em cotejo com o grau de interferência necessário para sanear a colisão.

Essa é uma descrição sucinta e objetiva da lei da colisão, proposta por Robert Alexy[108], a qual se constitui como método para solução de colisão de direitos fundamentais. Nesse modelo teórico, os mandamentos de otimização podem ser satisfeitos em diferentes graus, conforme as circunstâncias fáticas e jurídicas do caso concreto.

De fato, reconhece-se um espaço para o exercício de um juízo discricionário tanto na avaliação da necessidade de intervenção como na possibilidade de atuação do legislador. Essa

---

[106] ALEXY, Robert. **Teoria dos direitos fundamentais**. Tradução: Virgílio Afonso da Silva. 5ª ed. São Paulo : Editora Malheiros, 2008; PEREIRA, **Interpretação constitucional e direitos fundamentais**.

[107] PEREIRA, Jane Reis G. **Interpretação constitucional e direitos fundamentais**. 2. ed. Rio de Janeiro: Saraiva Jur, 2017. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788553600281/>. Acesso em: 30 abr. 2025.

[108] ALEXY, Robert. **Teoria dos direitos fundamentais**. Tradução: Virgílio Afonso da Silva. 5ª ed. São Paulo : Editora Malheiros, 2008.

margem de conformação, inclusive, serve de fundamento às críticas acerca da falta de parâmetros objetivos à lei de colisão. Contudo, essa discricionariedade está voltada apenas à consecução e busca de um objetivo atribuído a um direito fundamental, bem como quanto à eleição dos meios a serem empregados para essa atuação, verificando-se, inclusive, a sua adequação. Por decorrência lógica, essa liberdade decisória vinculada à proporcionalidade também se manifestaria no processo de sopesamento dos princípios em questão.

A partir desse raciocínio, afasta-se a concepção segundo a qual a aplicação dos princípios deveria sempre observar os seus pontos máximos possíveis, uma vez que esse entendimento restringiria o juízo de ponderação, obrigando a adotar uma única resposta correta. Ao revés, o modelo proposto por Alexy permite soluções distintas e proporcionais, considerando, novamente, as circunstâncias fáticas e jurídicas que irão determinar a intensidade da restrição e a adequação dos meios para promover os princípios envolvidos.

Logo, o modelo proposto deverá orientar o juízo de ponderação entre os direitos fundamentais envolvidos no fornecimento de dados aptos à identificação da geolocalização de indivíduos para a instrução criminal, especialmente a proteção de dados pessoais e segurança pública. Portanto, faz-se necessário tecer algumas considerações acerca dos elementos que compões esse crivo do sopesamento. Nessa ideia, reiteram-se os testes de adequação e de necessidade, bem como a análise da proporcionalidade em sentido estrito, elementos fundamentais à avaliação da solução adotada.

Mantendo-se o pressuposto central da Teoria dos Direitos Fundamentais de que "*princípios são normas que ordenam que algo seja realizado na maior medida possível dentro das possibilidades jurídicas e fáticas existentes*"[109], verifica-se que, no plano da adequação, a própria lógica de otimização inerente aos direitos fundamentais, por si só, eliminaria os meios que não seriam os mais adequados e permitiria o direcionamento à máxima adequação.

Dessa forma, quando uma medida não contribui para a concretização de um dos princípios envolvidos e, ao mesmo tempo, impõe restrição ao outro, ainda que tecnicamente fundamentada, essa medida não satisfaz o requisito da adequação. Nessa hipótese, essa medida deixa de promover efetivamente um dos princípios em disputa e atua apenas como objeção ao princípio contraposto, falhando, portanto, na tarefa de justificar a restrição imposta. Por decorrência, a otimização possível desses princípios impede a adoção de medidas que não seriam úteis ou cuja restrição imposta não sirva para maximização do outro princípio em colisão.

[109] *Ibid*., p. 588.

Nessa perspectiva, ao tratar da análise da utilidade ou identidade das medidas restritivas de direitos fundamentais, Jane Reis Gonçalves Pereira[110] propõe o refinamento do juízo de adequação a partir da identificação de duas dimensões complementares: a idoneidade forte e a idoneidade negativa ou débil. A primeira refere-se a aptidão do meio adotado para realizar de forma plena o fim constitucionalmente legítimo almejado. Já a segunda, mais restrita, corresponde à situação em que a medida contribui apenas parcialmente para a consecução desse objetivo, sem, no entanto, ser totalmente ineficaz. Essa classificação permite reconhecer que, para efeitos de controle de constitucionalidade, não se exige uma eficácia absoluta da medida, mas sim que ela não seja manifestamente inadequada.

O subprincípio da adequação, assim, opera como um crivo negativo, afastando apenas medidas que se revelem incapazes de contribuir minimamente para o fim pretendido. Trata-se de um juízo que, embora técnico, preserva certa margem de conformação ao legislador e ao intérprete constitucional, sobretudo diante do princípio da reserva do possível e da complexidade dos fins estatais. Esse espaço de liberdade decisória se evidencia nas palavras da própria autora, ao destacar que a exigência de adequação não equivale a uma obrigação de plena eficácia, mas a rejeição de meios arbitrários ou notoriamente inaptos:

> Essa postura liga-se à necessidade de conferir certo espaço de manobra ao Legislativo, já que, não raro, é impossível determinar com segurança absoluta se o meio é ou não totalmente adequado. Por isso, o conceito fraco de adequação é consentâneo com a noção de que os Tribunais só devem declarar a inconstitucionalidade de uma medida quando for possível atestar com total certeza e objetividade que aquela não contribui para a implementação do fim, noção esta que deflui dos princípios democrático e da separação de poderes.
> Assim, o controle judicial do requisito da idoneidade deve pautar-se por uma "lógica de evidência", isto é, os Tribunais devem invalidar decisões legislativas apenas naqueles casos em que se revelem manifestamente inadequadas para obtenção dos fins colimados[111].

Em seu turno, o exame da necessidade é aquele utilizado para escolha dos meios que, embora haja uma adequação intrínseca a eles, deve ser escolhido aquele que promova a menor intervenção possível. Para Alexy, essa busca pela máxima realização alinha-se à concepção da eficiência de Pareto, segunda a qual, "*uma posição pode ser melhorada sem que uma outra seja piorada*"[112]. Ou ainda, "*um meio deve ser considerado desnecessário quando há outra forma igualmente eficaz de atingir o fim que acarrete uma restrição mais leve ao direito fundamental*

---

[110] PEREIRA, Jane Reis G. **Interpretação constitucional e direitos fundamentais**. 2. ed. Rio de Janeiro: Saraiva Jur, 2017. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788553600281/>. Acesso em: 30 abr. 2025, p. 369.
[111] *Ibid.*, p. 370–371.
[112] ALEXY, Robert. **Teoria dos direitos fundamentais**. Tradução: Virgílio Afonso da Silva. 5ª ed. São Paulo : Editora Malheiros, 2008.

em jogo"[113]. A aplicação deste teste de necessidade, ao fim e ao cabo, visa balizar a atuação do legislador, vedando a adoção de meios que impõem restrições ou sacrifícios inúteis, bem como excessivos para consecução do fim constitucionalmente legítimo. Destarte, o exame de adequação é um juízo voltado a estabelecer se os meios são aptos ou idôneos para o alcance do resultado. De outro lado, o teste de necessidade visa perquirir se há meio igualmente eficaz, que imponha um sacrifício menos gravoso para atingir o fim já pré-estabelecido.

A esse raciocínio alia-se a proporcionalidade em sentido estrito, ou lei do sopesamento, teoria igualmente sedimentada pelo Tribunal Constitucional Federal, qual seja, "*quanto maior for o grau de não-satisfação ou de afetação de um princípio tanto maior terá que ser a importância da satisfação do outro*"[114]. Também é dizer: "*é preciso determinar se o atendimento à finalidade buscada pela medida restritiva compensa os prejuízos que desta advenham para os direitos fundamentais"*[115].

A denominada "lei do sopesamento", conforme formulada por Robert Alexy, estrutura-se em três etapas sucessivas. No primeiro momento, deve ser aferir o grau de comprometimento ou restrição de uma das normas principiológicas envolvidas na colisão. Em seguida, examina-se o peso ou relevância constitucional da concretização do princípio contraposto. Na última etapa, deve-se perquirir se a intensidade do sacrifício imposto ao primeiro princípio pode ser justificada pela relevância da efetivação do outro, considerando-se os elementos fáticos e jurídicos do caso concreto[116].

Em seu turno, Jane Reis Gonçalves Pereira[117] afirma que o resultado desse raciocínio, ao avaliar a conveniência da mitigação de um dos princípios em favor da realização de outra finalidade constitucional, consiste na fixação de uma relação de precedência entre as normas em colisão. A norma considerada mais relevante passa, então, a ocupar o papel de premissa maior na estrutura argumentativa adotada pelo intérprete.

---

[113] PEREIRA, Jane Reis G. **Interpretação constitucional e direitos fundamentais**. 2. ed. Rio de Janeiro: Saraiva Jur, 2017. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788553600281/>. Acesso em: 30 abr. 2025, p. 379.

[114] ALEXY, Robert. **Teoria dos direitos fundamentais**. Tradução: Virgílio Afonso da Silva. 5ª ed. São Paulo : Editora Malheiros, 2008, p. 593.

[115] PEREIRA, Jane Reis G. **Interpretação constitucional e direitos fundamentais**. 2. ed. Rio de Janeiro: Saraiva Jur, 2017. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788553600281/>. Acesso em: 30 abr. 2025, p. 381.

[116] ALEXY, Robert. **Teoria dos direitos fundamentais**. Tradução: Virgílio Afonso da Silva. 5ª ed. São Paulo : Editora Malheiros, 2008, p. 594.

[117] PEREIRA, Jane Reis G. **Interpretação constitucional e direitos fundamentais**. 2. ed. Rio de Janeiro: Saraiva Jur, 2017. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788553600281/>. Acesso em: 30 abr. 2025, p. 382–386.

A sistemática dessa operação consiste em atribuir níveis de intensidade a restrição imposta a um direito fundamental, classificando a como leve, moderada ou grave. De forma correlata, também se categoriza a relevância da realização do princípio contraposto nesses mesmos graus. Esse escalonamento recíproco, tanto da gravidade da intervenção quanto da importância da finalidade constitucional oposta, confere racionalidade a estrutura ao juízo de proporcionalidade em sentido estrito, conforme delineado pela lei de sopesamento formulada por Robert Alexy[118].

Assim, assimilando-se estas teses jurídico-filosóficas das normas de direito fundamental estabelecidas por Robert Alexy como premissas interpretativas, impõe-se uma análise mais rigorosa da utilização dos dados de geolocalização no âmbito da persecução penal. Esse exame torna-se especialmente relevante quando a medida é capaz de atingir terceiros não diretamente vinculados à investigação.

Em um primeiro plano, a legalidade da medida deve ser aferida à luz da teoria dos limites dos limites, que impõe restrições formais e materiais as intervenções nos direitos fundamentais. Em um segundo plano, considerando-se a existência de uma colisão entre normas principiológicas, ainda que em sentido amplo, mais especificamente entre o direito fundamental à proteção de dados e o interesse público na segurança da coletividade, a medida deverá ser submetida ao método da ponderação. Essa interpretação deve observar os subprincípios da adequação, da necessidade e da proporcionalidade em sentido estrito, a fim de assegurar a máxima realização possível dos valores condicionais em tensão.

[118] ALEXY, Robert. **Teoria dos direitos fundamentais**. Tradução: Virgílio Afonso da Silva. 5ª ed. São Paulo : Editora Malheiros, 2008.

CAPÍTULO 3: DOS DIREITOS DA PERSONALIDADE À AUTODETERMINAÇÃO INFORMATIVA, UMA VISÃO DOS DIREITOS FUNDAMENTAIS.

Como etapa do percurso teórico proposto neste trabalho, apresentar-se-á uma abordagem geral dos direitos fundamentais, com o objetivo de demonstrar que a complexidade conceitual dessa categoria jurídica exige uma análise aprofundada de sua episteme. Essa exigência decorre do fato de que a definição dos direitos fundamentais está intimamente vinculada à evolução histórica das percepções das necessidades para a concretização material da dignidade da pessoa humana.

Os avanços interpretativos quanto aos fundamentos desses direitos justificam a revisitação do conceito e das características dos direitos da personalidade, dentre os quais se insere o direito à privacidade. A partir dessa base, propõe-se o aprofundamento do debate jurídico acadêmico sobre a autonomia do direito à proteção de dados pessoais, o qual passa a ser destacado de uma perspectiva meramente privada para uma concepção centrada na autodeterminação informativa. Nesse novo paradigma, o indivíduo adquire a capacidade de exigir o adequado tratamento de suas informações pessoais, inclusive frente a ente públicos e privados, reafirmando sua condição de sujeito de direitos no contexto da sociedade da informação.

No entendimento de Ingo Wolfgang Sarlet[119], a despeito das possíveis divergências de terminologia, os direitos fundamentais sofreram um processo de evolução gradativa e aglutinativa, tanto em relação ao seu conteúdo e escopo, quanto aos seus titulares, a sua aplicabilidade e a sua concretização. Essa evolução é resultado da interligação entre os direitos fundamentais e os contextos sociais, políticos e tecnológicos de cada época histórica.

Esse processo evolutivo, destaca-se, deve ser compreendido sob uma perspectiva de complementariedade sucessiva, a qual reconhece os direitos fundamentais como integrantes de um único sistema normativo em constante aperfeiçoamento. Trata-se, portanto, de uma evolução que não se dá por sobreposição ou substituição de direitos, mas por ampliação e reforço do seu conteúdo normativo. Com base nessa compreensão, Sarlet propõe o abandono da tradicional classificação em gerações de direitos fundamentais, defendendo, em seu lugar, a ideia de que esses direitos coexistem em distintas dimensões, determinadas pelo seu processo histórico de positivação nas Constituições e pelas transformações dele decorrentes[120].

---

[119] SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional**. 10. ed. Porto Alegre: Livraria do Advogado, 2009.
[120] *Ibid*.

Nesse contexto, os direitos fundamentais de primeira dimensão são identificados com as liberdades individuais reconhecidas nas primeiras constituições escritas[121], exigindo-se para sua proteção uma limitação contra a intervenção estatal. Esses direitos são o direito à vida, à integridade física e à privacidade, que têm como objetivo principal delimitar uma esfera de atuação negativa do Estado.

Como alertam Mendes e Branco[122], a pluralidade conceitual dos direitos fundamentais no campo jurídico-acadêmico são decorrências de embates epistemológicos e ontológicos das diferentes concepções filosóficas do Direito, sejam elas jusnaturalistas, positivistas, idealistas ou realistas. Essa dificuldade na unidade filosófica acerca desta categoria jurídica acaba arrefecendo a digressão acerca do fundamento de uma base absoluta filosófica ou dogmática para sua conceituação e justificação. Busca-se, então, abandonar uma definição essencialista e adotar uma concepção material que investigue a razão pela qual um direito deveria ser considerado como "fundamental", a merecer previsão constitucional.

Nesse panorama, a materialização da dignidade da pessoa humana é alçada a pressuposto para a noção de classificação de um direito fundamental. No entanto, a própria contextualização de dignidade é permeada por um elevado grau de subjetividade e indeterminação conceitual, o que contribui para a constante expansão do catálogo dos direitos fundamentais. Essa abertura interpretativa permite uma pluralidade de reconhecimento de direitos abrangendo não apenas aqueles expressamente previstos no texto constitucional, mas também os implícitos identificáveis por meio da interpretação sistemática do ordenamento constitucional.

Ademais, os direitos fundamentais são construções históricas e contextuais, cuja definição e aplicabilidade variam conforme as circunstâncias sociais, políticas e culturas de cada época. Por essa razão, não se apresentam como um conjunto homogêneo ou dotado de critérios absolutos e universais que os definam. Ao contrário, sua identificação está diretamente relacionada à evolução dos valores que compõem o conteúdo material da dignidade da pessoa humana[123].

A transformação para o reconhecimento do direito à autodeterminação informativa e da proteção de dados é um exemplo contemporâneo dessas modificações, originando-se em contraponto ao aumento da proliferação do acesso de dados pessoais e seu tratamento

---

[121] *Ibid*.
[122] MENDES, Gilmar Ferreira; COELHO, Inocêncio Mártires; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional**. 2. ed. São Paulo: Saraiva, 2008.
[123] *Ibid*.

banalizado. Portanto, o direito à privacidade, originalmente concebido como um direito de barreira à intervenção estatal, demanda, hoje, a positivação de direitos e a ação do Estado para a efetiva proteção da inviolabilidade dos dados e a garantia de que os indivíduos possam exercer controle sobre suas informações pessoais. Assim, a evolução do conceito do direito da personalidade reflete um movimento de complementação entre as diferentes gerações de direitos fundamentais, sem substituição, mas com expansão de sua proteção e escopo.

3.1. EVOLUÇÃO DO DIREITO DA PERSONALIDADE. TEORIA JURISPRUDENCIAL ALEMÃ.

Nesse contexto de construção evolutiva da dogmática dos direitos da personalidade, destaca-se a jurisprudência constitucional alemã, que percorre de forma coerente as diferentes etapas de transformação desse direito fundamental. O Tribunal Constitucional Alemão[124] adota como critério interpretativo a análise material das demandas concretas do indivíduo, compreendendo que a constitucionalidade de um direito não se esgota na sua positivação formal, mas existe sua vinculação direta à dignidade da pessoa humana. Essa perspectiva permite a identificação e o reconhecimento de novos direitos fundamentais, mesmo quando não expressamente previstos, desde que correspondam a exigências de proteção da personalidade diante dos desafios impostos por contextos sociais tecnológicos em constante mutação.

Nesse panorama, resgata-se a contribuição de Robert Alexy[125] no desenvolvimento da sua teoria sobre as normas de direitos fundamentais atribuídas, especialmente no que se refere às relações de fundamentação e concretização entre normas constitucionais. A partir dessa perspectiva, é possível compreender que a evolução histórica do direito da personalidade, da liberdade geral de ação até a autodeterminação informativa, passa pela construção e verificação das relações de refinamento ou fundamentação que estabelecem a conexão sistemática ou textual com as normas que garantem direitos subjetivos, vinculando-se com uma norma de direito fundamental anterior (positivada), especialmente com o art. 2º, §1º da Lei Fundamental da Alemanha:

> Artigo 2
> [Direitos de liberdade]

[124] As traduções das fontes em língua alemã utilizadas ao longo deste trabalho foram elaboradas com o apoio de tradutores automáticos (como o Google Tradutor), com revisão técnica realizada pelo próprio autor, a fim de assegurar fidelidade ao conteúdo original.
[125] ALEXY, Robert. **Teoria dos direitos fundamentais**. Tradução: Virgílio Afonso da Silva. 5ª ed. São Paulo : Editora Malheiros, 2008.

> (1) Todos têm o direito ao livre desenvolvimento da sua personalidade, desde que não violem os direitos de outros e não atentem contra a ordem constitucional ou a lei moral.
> (2) Todos têm o direito à vida e à integridade física. A liberda-de da pessoa é inviolável. Estes direitos só podem ser restringidos em virtude de lei.

Ao abordar a construção histórica do conceito de autodeterminação informativa, Laura Schertel Mendes[126], com base em sua tese de doutorado defendida na Universidade Humboldt de Berlim, revisita os principais marcos jurisprudenciais da Corte Constitucional Alemã que delinearam, de forma progressiva, a consolidação do direito geral da personalidade. A autora demonstra como a formulação desse direito fundamental foi moldada por transformações sociais e tecnológicas, revelando-se como resposta à crescente sofisticação das dinâmicas sociais e ao avanço das tecnologias de informação, as quais intensificaram a exposição da esfera de privacidade dos indivíduos.

O primeiro marco relevante foi o reconhecimento de que o direito fundamental ao "livre desenvolvimento da personalidade" deveria ser interpretado da forma mais ampla, no âmbito de uma concepção mais abrangente da "liberdade geral de ação". Nessa perspectiva, a proteção da personalidade estaria inserida numa norma aberta de liberdade, não vinculada a um direito fundamental específico previamente positivado, mas decorrente do próprio exercício da autonomia individual. Essa construção teórica foi consolidada pelo Tribunal Constitucional Federal da Alemanha na análise dos julgamentos dos casos paradigmáticos sobre o auxílio em investimentos (BVerfGE 4, 7 [15][127], de 1954), e, especialmente, na decisão conhecida como caso Elfes (BVerfGE 6, 32)[128], que discutiu a emissão de passaporte e liberdade de locomoção dentro do território alemão[129].

Todavia, como já mencionado, a jurisprudência do Tribunal Constitucional Federal da Alemanha passou a reconhecer que a proteção conferida pela cláusula da liberdade geral de ação não era suficiente para abarcar todas as situações relacionadas ao desenvolvimento da personalidade. À medida que os casos se tornaram mais complexos, tornou-se necessária uma diferenciação interpretativa mais refinada, com base no artigo 2º, §1º da Lei Fundamental. A Corte passou, então, a distinguir os casos que envolviam a liberdade geral de ação,

---

[126] MENDES, Laura Schertel Ferreira, Autodeterminação informativa: a história de um conceito, **Revista de Ciências Jurídicas Pensar**, v. 25, n. 14, p. 1–18, 2020.
[127] ALEMANHA. Bundesverfassungsgericht (BVerfG). BVerfGE 4, 7 [15]. Disponível em: https://www.servat.unibe.ch/dfr/bv004007.html. Acesso em: 9 abr. 2025.
[128] ALEMANHA. Bundesverfassungsgericht (BVerfG). BVerfGE 6, 32. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1957/01/rs19570116_1bvr025356en.html. Acesso em: 9 abr. 2025.
[129] MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. **Revista de Ciências Jurídicas Pensar**, v. 25, n. 14, p. 1–18, 2020.

compreendida como a possibilidade genérica de agir conforme a própria vontade, daqueles que diziam respeito diretamente à expressão e à preservação da personalidade individual, exigindo, para estes últimos, um grau mais elevado de proteção constitucional. Ademais, a proteção ao desenvolvimento da personalidade era demasiadamente frágil em relação à ação de terceiros[130].

Inaugura-se, nesse momento, o segundo marco no direito no desenvolvimento do direito da personalidade, caracterizado pela consolidação da proteção à intimidade e à esfera privada como barreira contra a interferência tanto do Estado quanto de terceiros. Essa evolução torna-se particularmente evidente na decisão proferida pelo Tribunal Constitucional Federal Alemão no caso do microsenso (BVerfGE 27, 1 (6))[131], cujo objeto versava sobre a análise da constitucionalidade da coleta de dados no âmbito de uma pesquisa estatística nacional. O questionário não se limitava a informações básicas, como sexo, idade e estado civil dos residentes, mas incluía também dados considerados, à época, de menor relevância, como as viagens de férias e lazer. O objetivo declarado era obtenção de subsídios para análises econômicas e sociológicas, com reflexos nos setores de turismo e transporte.

Embora o Tribunal Constitucional Alemão tenha reconhecido a constitucionalidade da medida, por entender que se tratava de dados de caráter predominantemente público, passíveis de observação externa e que não adentravam pormenorizadamente no núcleo da intimidade, o mais relevante é que, a partir desse julgamento, algumas premissas fundamentais foram expressamente firmadas, como: (i) "a Constituição assegura a cada cidadão um espaço inviolável de organização privada da vida, imune à interferência do poder público (BVerfGE 6, 32 [41], 389 [433]); (ii) "o indivíduo, para exercer de forma livre e responsável sua personalidade, deve dispor de um "espaço interior" em que "possa pertencer a si mesmo", "se recolher", e ao qual "o mundo exterior não tenha acesso".

Com o intuito de garantir a precisão interpretativa e a clareza expositiva do entendimento desenvolvido pela Corte alemã, procede-se a transcrição de excerto da decisão:

> A pesquisa por amostragem obrigatória sobre o tema "viagens de férias e de lazer" não violou o artigo 1º, § 1º, nem o artigo 2º, § 1º da Lei Fundamental, tampouco outras disposições da Constituição alemã.
> 1. a) De acordo com o artigo 1º, § 1º da Lei Fundamental (Grundgesetz – GG), a dignidade da pessoa humana é inviolável e deve ser respeitada e protegida por toda autoridade estatal.
> No sistema de valores da Constituição, a dignidade humana ocupa o lugar de valor supremo (BVerfGE 6, 32 [41]). Tal como todas as demais disposições constitucionais, essa afirmação da dignidade humana também domina a interpretação do art. 2º, § 1º

[130] *Ibid*.
[131] ALEMANHA. Bundesverfassungsgericht (BVerfGE) 27, 1 (6). Decisão do Tribunal Constitucional Federal. Disponível em: https://www.servat.unibe.ch/dfr/bv027001.html. Acesso em: 9 abr. 2025.

> GG. O Estado não pode, por nenhum ato — nem mesmo por meio de lei —, violar a dignidade da pessoa ou comprometer, além dos limites estabelecidos no art. 2º, § 1º, o núcleo essencial da liberdade individual. Com isso, a Constituição assegura a cada cidadão um espaço inviolável de organização privada da vida, imune à interferência do poder público (BVerfGE 6, 32 [41], 389 [433]).
>
> b) À luz dessa concepção de ser humano, a pessoa possui, na sociedade, um direito ao reconhecimento de sua dignidade e ao respeito social.
> É incompatível com a dignidade humana tratar o indivíduo como mero objeto do Estado (cf. BVerfGE 5, 85 [204]; 7, 198 [205]). Seria inadmissível, à luz da dignidade da pessoa, que o Estado reivindicasse para si o direito de registrar compulsoriamente a personalidade humana em sua totalidade e catalogá-la — ainda que sob a forma anônima de uma pesquisa estatística —, tratando o indivíduo como uma coisa sujeita a inventário em todos os aspectos possíveis.
> Tal penetração no âmbito da personalidade individual, mediante um acesso abrangente às condições pessoais dos cidadãos, é vedada ao Estado também porque o indivíduo, para exercer de forma livre e responsável sua personalidade, deve dispor de um "espaço interior" em que "possa pertencer a si mesmo", "se recolher", e ao qual "o mundo exterior não tenha acesso" — um espaço em que se possa "ser deixado em paz e ter o direito à solidão" (Wintrich, Die Problematik der Grundrechte, 1957, p. 15 e seguintes; ver também Dürig, em Maunz-Dürig, GG, 2ª ed., nota 37 ao art. 1).
> Nesse espaço, o Estado pode interferir mesmo por meio de uma simples coleta neutra de informações, caso esta seja capaz de inibir o livre desenvolvimento da personalidade por meio da pressão psicológica causada pela atenção pública.
>
> c) No entanto, nem toda coleta estatística sobre dados pessoais e condições de vida fere a dignidade humana ou compromete o direito à autodeterminação no núcleo mais íntimo da vida pessoal.
> Como cidadão relacionado e vinculado à comunidade (cf. BVerfGE 4, 7 [15, 16]; 7, 198 [205]; 24, 119 [144]), todo indivíduo deve aceitar, em certa medida — como, por exemplo, no caso de um censo populacional —, a necessidade de levantamentos estatísticos sobre si mesmo, como condição prévia para o planejamento racional da atuação estatal.
>
> Uma pesquisa estatística sobre a pessoa pode, portanto, ser percebida como degradante e como uma ameaça ao direito à autodeterminação, quando adentra uma esfera da vida humana que, por sua própria natureza, possui um caráter sigiloso, e, assim, transforma esse espaço interior em material passível — e até mesmo necessário — de ser explorado estatisticamente. Nesse ponto, até mesmo o Estado da sociedade industrial moderna encontra limites para a "despersonalização" administrativa. (tradução livre e trechos sem destaques no original).

De fato, como já destacado, evidencia-se o movimento da jurisprudência constitucional alemã no sentido de cindir a "liberdade geral de ação" do "live desenvolvimento da personalidade". No caso analisado, não se trata de mera proteção à liberdade de comportamento humano, mas sim da tutela do núcleo essencial da intimidade contra interferência de terceiros, incluindo-se, nesse espectro, o próprio Estado. Reafirma-se, com isso, o fortalecimento da concepção de que a privacidade integra o conteúdo da personalidade, consolidando-se como um direito de defesa. Essa proteção se articula à necessidade de ponderação quanto à natureza dos dados e informações pessoais, especialmente no que diz respeito à sua vinculação ou inserção intrínseca na esfera privada das pessoas.

Percebe-se, então, a sedimentação progressiva dos contornos do direito à privacidade, os quais, posteriormente, contribuíram para a formulação do conceito apresentado por Tércio Sampaio Ferraz, citado por Mendes e Branco[132], nos seguintes termos:

> Um direito [direito à privacidade] subjetivo fundamental, hoje o titular é toda pessoa, física ou jurídica, brasileira ou estrangeira, residente ou em trânsito no país; cujo conteúdo é a faculdade de constranger os outros ao respeito e de resistir à violação de que ele é próprio, isto é, das situações vitais que, por si só a ele lhe dizerem respeito, deseja manter para si, ao abrigo de sua única discricionária decisão; e cujo objeto é a integridade moral do titular[133].

Laura Schertel Mendes, com base nos estudos de Marion Albers[134], destaca que a jurisprudência constitucional alemã passou a incorporar como referência a teoria das esferas proposta por Heinrich Hubmann, no intuito de estruturar a proteção do direito da personalidade de forma mais sistemática. Segundo essa teoria, a personalidade poderia ser representada por círculos concêntricos, nos quais a intensidade da proteção jurídica aumenta à medida que se avança em direção ao núcleo mais interno da vida pessoal.

A estrutura da teoria identificaria três esferas essenciais: (i) a esfera do segredo (*Geheimsphäre*), concebida nessa teoria como absolutamente inviolável, na qual se inserem aspectos como o pensamento, sentimentos e convicções pessoais, cuja preservação guardariam estreita relação com a dignidade da pessoa humana. Estes elementos estariam salvaguardados intervenções e críticas; (ii) a esfera da intimidade (*Intimsphäre*) que estaria atrelada as relações familiares, crenças e relações pessoais, bem como hábitos relacionados aos aspectos da vida privada; (iii) a esfera privada (*Privatsphäre*), que está relacionada a posição do indivíduo na sociedade, abrangendo seus comportamentos em espaços públicos, cuja proteção é mitigada em face de outros bens jurídicos tutelados.

Apesar de representar um avanço na sistematização da tutela da personalidade, a teoria das esferas propostas por Hubmann apresenta limitações, sobretudo no que se refere à delimitação objetiva das informações que integram cada um dos círculos representados. Essa dificuldade decorre da subjetividade inerente à forma como cada indivíduo percebe e atribui valor aos seus próprios dados e atributos. Em razão dessa subjetividade, a previsibilidade

---

[132] MENDES, Gilmar Ferreira; COELHO, Inocêncio Mártires; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional**. 2. ed. São Paulo: Saraiva, 2008, p. 378.

[133] FERRAZ, Tércio Sampaio. **Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado.** Cadernos de Direito Constitucional e Ciência Política, n.1, p.77, *apud* MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. Curso de direito constitucional. 2ª ed. São Paulo: Saraiva, 2008. p. 378.

[134] ALBERS, Marion. **Informationelle selbstestimmunb.** Baden-Baden: Nomos, 2005 *apud* MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. **Revista de Ciências Jurídicas Pensar**, v. 25, n. 14, p. 1–18, 2020.

jurídica na aplicação da teoria, especialmente nos casos situados nas zonas limítrofes entre as esferas, acaba comprometida, evidenciando a dificuldade prática do critério proposto pelo jurista[135].

Contudo, como adverte Laura Schertel Mendes[136], embora a teoria das esferas seja alvo de críticas e tenha sua aplicação relativizada pelo Tribunal Constitucional Federal Alemão em decisões posteriores, ela introduziu ponderações fundamentais sobre os princípios da relatividade e da contextualização na proteção da personalidade. Esses princípios exigem que a utilização e a finalidade do tratamento de informações pessoais sejam analisadas à luz das circunstâncias concretas, reconhecendo a subjetividade inerente à classificação e ao conteúdo dos dados. Essa perspectiva contribuiu diretamente para o desenvolvimento do conceito de autodeterminação informativa, ao enfatizar que a proteção de dados deve levar em conta não apenas o tipo de informação, mas também o modo como ela se relaciona com a identidade e a autonomia do titular.

Trilhando a perspectiva do desenvolvimento do direito da personalidade apresentada pela autora, observa-se que, após a incorporação da noção de privacidade ao aspecto protetivo da dignidade da pessoa humana, compreendida como seu fundamento constitucional, emerge o direito geral da personalidade. Esse novo marco teórico-jurisprudencial surge como superação da concepção restritiva centrada exclusivamente no direito de ser deixado a sós, avançando para uma proteção mais ampla dos atributos do indivíduo. Sua consolidação ocorre por meio de decisões do Tribunal Constitucional Federal Alemão ao referendar outras decisões baseadas em princípios fundamentais do direito e interpretações da legislação nacional, com o objetivo de assegurar garantias efetivas a personalidade humana.

Tomou-se como referência o célebre julgamento do caso Soraya (BVerfGE 34, 269)[137], no qual o Tribunal Constitucional Federal Alemão reconheceu o direito da ex-esposa do Xá do Irã à reparação por danos morais, diante da divulgação de uma entrevista fictícia que afrontava sua esfera privada. Embora a controvérsia envolvesse a interpretação e aplicação de normas do direito privado, o Tribunal Constitucional Alemão entendeu ser necessária à sua manifestação

---

[135] MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. **Revista de Ciências Jurídicas Pensar**, v. 25, n. 14, p. 1–18, 2020.
[136] *Ibid*.
[137] ALEMANHA. Bundesverfassungsgericht (BVerfGE) 34, 269. Decisão do Tribunal Constitucional Federal. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1973/02/rs19730214_1bvr011265en.html. Acesso em: 12 abr. 2025.

para assegurar que as interpretações infraconstitucionais observassem os valores imanentes aos direitos fundamentais, em especial no que se refere ao direito da personalidade[138].

Outro caso que teria sedimentado a mudança de paradigma no processo de consolidação do direito geral da personalidade como garantia fundamental autônoma, foi o caso Eppler (BVerfGE 54, 148)[139]. Nessa decisão, o Tribunal Constitucional Alemão fixou diversas premissas acerca da posição sistemática do direito geral da personalidade e em relação a outros direitos fundamentais, bem como suas características essenciais. O julgado também fez referência à teoria das esferas de Hubmann, como forma de estruturar os diferentes níveis de proteção conferidos à personalidade em razão do conteúdo da informação afetada e do grau de exposição do indivíduo:

> 2. A) não se verificando, portanto, violação a direitos fundamentais específicos, resta como parâmetro de análise apenas o direito geral da personalidade, constitucionalmente garantido pelos arts 2º, §1º, em combinação com o art. 1º,§º da Lei Fundamental (Grundgesetz – GG).
>
> Esse direito atua como uma liberdade "não nominada", que complementa as liberdades específicas ("nominadas"), como a liberdade de consciência ou de expressão, as quais também protegem elementos constitutivos da personalidade. **Sua função é, a luz do princípio constitucional supremo da "dignidade da pessoa humana" (art. 1º, §1º GG), assegurar a esfera pessoal mais restrita da vida privada e garantir a preservação de suas condições essenciais, as quais não são completamente abrangidas pelas garantias tradicionais e concretas de liberdade**. Tal necessidade mostra-se especialmente relevante diante das transformações sociais contemporâneas e das novas ameaças daí decorrentes a proteção da personalidade humana.
>
> Como evidência a vinculação com o art. 1º, §1º GG**, o direito geral da personalidade previsto no art. 2º, §1º da Constituição incorpora um elemento de "livre desenvolvimento da personalidade", que se distingue do elemento "ativo" dessa liberdade - representando pela liberdade geral de ação (cf. BVerfGE 6, 32). Em razão disso, os requisitos para a configuração da violação ao direito geral da personalidade devem ser mais restritivos do que aqueles aplicáveis à Liberdade geral de ação: ele se aplica apenas a intervenções aptas a afetar de modo significativo a esfera mais íntima da personalidade** (cf. BVerfGE 34, 238 [247] - gravação clandestina; BGHZ 24,72 [81]; 27, 284 [287]).
>
> Dada a natureza particular do direito geral da personalidade, tanto a jurisprudência do Tribunal Constitucional Federal quanto a do Tribunal Federal de Justiça (Bundesgerichtshof) não definiram de forma exaustiva o conteúdo desse direito protegido, mas vêm desenvolvendo suas manifestações conforme as circunstâncias de cada caso concreto.
>
> São reconhecidos, como bens juridicamente tutelados pelo direito geral da personalidade, a esfera privada, a esfera secreta e a esfera íntima (cf. BVerfGE 27, 1 [6] – Mikrozensus; 27, 344 [350 e ss.] – autos de divórcio; 32, 373 [379] – prontuário

[138] MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. **Revista de Ciências Jurídicas Pensar**, v. 25, n. 14, p. 1–18, 2020.

[139] **ALEMANHA.** *Bundesverfassungsgericht (BVerfGE) 54, 148* – Caso Eppler. Decisão do Tribunal Constitucional Federal. Disponível em: https://servat.unibe.ch/dfr/bv054148.html. Acesso em: 12 abr. 2025.

> médico; 34, 238 [245 e ss.] – gravação clandestina; 47, 46 [73] – aulas de educação sexual; 49, 286 [298] – transexualidade), a honra pessoal, o direito de dispor sobre a própria imagem pública (BVerfGE 35, 202 [220] – caso Lebach), o direito à própria imagem e à palavra falada (BVerfGE 34, 238 [246]), e, sob determinadas circunstâncias, o direito de não ter atribuídas declarações que não foram proferidas (cf. BVerfGE 34, 269 [282 e ss.] – caso Soraya)
> Essas manifestações do direito fundamental à personalidade devem ser devidamente observadas sempre que se trate de decisões judiciais que envolvam a ponderação entre interesses conflitantes regulados pelo direito privado (cf. BVerfGE 35, 202 [221]).
> (...)
> Também o direito geral da personalidade, garantido pelo art. 2º, § 1º da Lei Fundamental (Grundgesetz – GG), pode proteger contra a imputação de declarações não proferidas. Isso se verifica, por exemplo, quando há a violação de um bem jurídico reconhecido como protegido por esse direito, como a esfera privada — a exemplo da divulgação de uma entrevista fictícia que diga respeito à vida privada da pessoa atingida (BGH, NJW 1965, p. 685 – caso Soraya; cf. também BVerfGE 34, 269 [282 e ss.]).
>
> Mesmo quando tal bem jurídico não está diretamente afetado, ainda assim se configura uma violação ao direito geral da personalidade se forem atribuídas a alguém declarações que ele não fez e que prejudiquem sua reputação social conforme ele próprio a define. **Isso decorre do princípio da autodeterminação que fundamenta o direito geral da personalidade: o indivíduo deve poder decidir, sem restrição à sua esfera privada, como deseja ser representado perante terceiros ou perante o público em geral, inclusive no que diz respeito a se, como e em que termos deseja manifestar-se por meio de suas próprias declarações**. (tradução livre e sem destaques no original).

Assim, o enunciado aberto do direito geral da personalidade, aliado a uma intepretação constitucional progressiva, concediam-lhe amplitude suficiente a alcançar os possíveis desafios impostos pelas transformações tecnológicas e sociais, nos casos de risco às esferas de privacidade do indivíduo. Ao ser alçado a estatura constitucional, sua aplicação deixa de ser a de um direito de objeção adstrito aos julgamentos infraconstitucionais do direito privado e passa a ser um direito fundamental autônomo. Nesse sentido, arremata Laura Schertel Ferreira Mendes[140]:

> Com esse ponto de partida, o direito geral de personalidade passa ser formulado em um nível abstrato, de modo que ele possa oferecer proteção abrangente, tendo como ponto fulcral o conceito de autodeterminação. Dessa forma, na jurisprudência de direitos fundamentais, esse direito é apresentado como direito de liberdade indistinto, que complementa os direitos de liberdade específicos.
>
> Em relação a essa abstração, seu conteúdo não pode ser definido de forma conclusiva; existe somente uma definição específica na análise do caso concreto. Com isso, a função mais importante do direito da personalidade geral consiste em proteger o indivíduo contra futuras ameaças, que sempre podem voltar a surgir no cotidiano contemporâneo.

[140] MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. **Revista de Ciências Jurídicas Pensar**, v. 25, n. 14, 2020, p. 9.

3.2. DIREITO DA PERSONALIDADE NO BRASIL

No ordenamento jurídico brasileiro, o direito da personalidade encontra densidade normativa tanto na Constituição Federal de 1988 quanto no Código Civil de 2002. A dignidade da pessoa humana, um dos radicais dos fundamentos do Estado Democrático de Direito (art. 1º, inc. III, da CF), constitui o eixo axiológico em torno do qual gravitam os direitos fundamentais relacionados à individualidade. Entre eles, destaca-se a proteção à intimidade, à vida privada, à honra e à imagem (art. 5º, inc. X), que conforma o núcleo essencial da tutela jurídica da identidade pessoal e da integridade moral dos indivíduos. Esses dispositivos revelam um compromisso normativo com a preservação da autonomia individual dos direitos da personalidade.

Na esfera infraconstitucional, inspirado pelos códigos italiano e português, o Código Civil Brasileiro inaugurou um capítulo dedicado aos direitos da personalidade, estatuído nos artigos 11 ao 21, elencando, inclusive atributos desse direito como a intransmissibilidade, irrenunciabilidade e o fato de serem natos e vinculados à própria existência e desenvolvimento da pessoa humana, como leciona Gustavo Tepedino:

> Os direitos da personalidade devem ser entendidos como especificação analítica da cláusula geral de tutela da personalidade prevista no Texto Constitucional contida nos arts. 1º, III (dignidade humana como valor fundamental da República), 3º, III (igualdade substancial) e 5º, § 2º (mecanismo de expansão do rol dos direitos fundamentais).33 Com base nessa cláusula geral, deverá o intérprete romper com a ótica tipificadora seguida pelo Código Civil, ampliando a tutela da pessoa humana para além do rol de direitos subjetivos previstos pelo legislador[141].

Desta forma, disse-se que os direitos da personalidade têm como fundamento a dignidade da pessoa humana e são responsáveis por assegurar a preservação da identidade, a autonomia e o desenvolvimento individual do ser humano[142]. Logo, os direitos da personalidade não se limitariam apenas à integridade física e psíquica, mas também abarcam aspectos intangíveis, como a imagem, a honra, a privacidade e, no contexto contemporâneo, os dados pessoais.

No âmbito do Código Civil, os direitos da personalidade projetam-se além da perspectiva patrimonialista e passam a refletir a influência de valores existencialistas. Deixam, assim, de ser compreendidos apenas como expressão da capacidade de ser sujeito de relações

---

[141] TEPEDINO, Gustavo; OLIVIA, Milena Donato, **Fundamentos de Direito Civil - Vol. 1 - Teoria Geral do Direito Civil**, 5. ed. Rio de Janeiro: Forense, 2024, p. 145.
[142] BIONI, Bruno, **Proteção de dados pessoais**, 1. ed. Rio de Janeiro: Forense, 2019.

jurídicas, para abarcar atributos essenciais e inalienáveis da natureza da pessoa humana, físico e moral, além de suas respectivas interações sociais. À luz dessas premissas, a tutela desses direitos irradia-se a uma visão de proteção extrapatrimonial do direito.

Uma distinção importante entre direitos da personalidade e direitos patrimoniais é que enquanto os últimos estão voltados para a proteção de bens materiais e interesses econômicos, os direitos da personalidade têm como objeto atributos inatos e intrínsecos da pessoa. Eles não podem ser mensurados em termos de valor econômico, ainda que certas manifestações, como o direito à imagem, possam ter reflexos patrimoniais[143].

Mesmo nesses casos, argumenta-se que o potencial econômico de certos aspectos da personalidade, como o nome ou a imagem, não descaracteriza o caráter extrapatrimonial do direito em si, mas apenas o coloca em uma posição de negociação limitada e sujeita a consentimento expresso e revogável do titular. Em outras palavras, o direito da personalidade não se converte em um bem patrimonial, mas permite que o titular autorize o uso de determinados atributos, desde que observados os limites legais e éticos pautados pela dignidade da pessoa humana.

A natureza dos direitos da personalidade também é tema de debate, especialmente quanto à sua caracterização como direitos subjetivos. Alguns autores como Savigny e Iellinek, adeptos às teorias negativistas, sustentavam que seria impossível conceber um direito que tivesse como objeto o próprio sujeito, uma vez que isso criaria uma relação paradoxal de propriedade sobre si mesmo.

Tepedino[144] e Beltrão[145] discordam dessa perspectiva, defendendo que os direitos da personalidade são, sim, direitos subjetivos, mas de uma natureza especial. Eles não configuram uma relação de propriedade do sujeito sobre si próprio, mas sim um conjunto de prerrogativas que garantem a inviolabilidade de sua dignidade e identidade. Dessa forma, o direito à vida, à integridade física, à honra e à privacidade são considerados irradiações do próprio ser e não objetos exteriores que possam ser adquiridos, transferidos ou negociados como bens patrimoniais.

---

[143] BELTRÃO, Silvio Romero, **Direito Da Personalidade – Natureza Juridica, Delimitação do Objeto e Relações com o Direito Constitucional**. Dimensões Jurídicas da Personalidade na Ordem Constitucional Brasileira. n. 1, p. 203–228, 2013.

[144] TEPEDINO, Gustavo; OLIVIA, Milena Donato. **Fundamentos de Direito Civil - Vol. 1 - Teoria Geral do Direito Civil**. 5. ed. Rio de Janeiro: Forense, 2024. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788530994471>. Acesso em: 18 jun. 2025.

[145] BELTRÃO, Silvio Romero, **Direito Da Personalidade – Natureza Juridica, Delimitação do Objeto e Relações com o Direito Constitucional**. Dimensões Jurídicas da Personalidade na Ordem Constitucional Brasileira. n. 1, p. 203–228, 2013.

Por oportuno, ressalta-se que tais direitos são componentes dos direitos da personalidade e da existência e dignidade da pessoa humana, como pontuaram Siqueira, Rocha e Silva:

> Correntemente, os direitos da personalidade são tidos como prerrogativas, de conteúdo extrapatrimonial, dotadas de certas características fundamentais, como inalienabilidade, perpetuidade e oponibilidade a todos. Atinentes, portanto, a todas as pessoas, por sua própria existência e reconhecimento, não poderão ser afastados, sob pena de vilipendio da sua própria condição ou configuração como pessoa. Em suma, são direitos que amparam a existência, integridade e dignidade, assimilando a própria essencialidade do ser. Nesta direção, é também a partir destes que se projeta a tônica do mínimo existencial[146].

Nesse sentido, os direitos da personalidade não estão circunscritos ao direito privado meramente amparado nos artigos 11 a 21 do Código Civil, mas, sim, trata-se de direito fundamental positivado na Constituição Federal de 1988, o qual extrai sua própria ontologia dos direitos humanos intrínsecos a existência do próprio ser, desvinculados de uma determinada ordem jurídica e de validade universal[147].

Outro ponto relevante é a questão das limitações dos direitos da personalidade. Embora sejam considerados direitos absolutos, no sentido de que devem ser respeitados por todos (*erga omnes*), isso não significa que eles sejam ilimitados. Em situações de conflito com outros direitos fundamentais, como a liberdade de imprensa ou o direito à informação, os direitos da personalidade podem ser relativizados por meio de um juízo de ponderação. Nesses casos, é necessário avaliar qual direito prevalece, considerando o contexto específico e o princípio da proporcionalidade. Por exemplo, o direito à privacidade pode ser limitado quando confrontado com o interesse público na divulgação de informações relevantes, desde que respeitados os limites do respeito à dignidade humana. Essas limitações não implicam na renúncia ou na alienação dos direitos da personalidade, mas sim em uma harmonização necessária para garantir o equilíbrio entre direitos igualmente protegidos pelo ordenamento jurídico[148].

3.3. DIREITO À PRIVACIDADE

---

[146] SIQUEIRA, Dirceu Pereira; ROCHA, Maria Luiza de Souza; SILVA, Rodrigo Ichikawa Claro. **Atividades notariais e registrais, judicialização e acesso à justiça: o impacto da desjudicialização para a concretização dos direitos da personalidade.** Revista Jurídica Cesumar – Mestrado, v. 18, p. 305–355, p. 312.

[147] SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional**. 10. ed. Porto Alegre: Livraria do Advogado, 2009.

[148] BELTRÃO, Silvio Romero, **Direito Da Personalidade – Natureza Juridica, Delimitação do Objeto e Relações com o Direito Constitucional**. Dimensões Jurídicas da Personalidade na Ordem Constitucional Brasileira. n. 1, p. 203–228, 2013.

O direito à privacidade, debatido a partir do célebre artigo *The Right to Privacy* de Warren e Brandeis[149] (1890), também evoluiu desde a concepção de seus contornos, afastando-se da ideia estritamente patrimonialista da defesa dos direitos fundamentais, especialmente o da propriedade privada, avançando-se para o estabelecimento de um paradigma antropocêntrico dos direitos da personalidade.

Assim, o direito à privacidade, atualmente, é interpretado num contexto mais amplo. Considera-se que a representação de suas ações e à autodeterminação do indivíduo não estão circunscritas ao seu espaço habitual, uma vez que os dados a ele relacionados projetam-se além deste âmbito subjetivo. Esses dados transcendem a mera discussão acerca de titularidade, podendo, inclusive, serem tratados de forma destacada de seu titular, transmudando-se em bens passíveis de valoração econômica.

A essa nominada despersonalização da personalidade é o novo desafio afeto à proteção de dados, no qual se discute inclusive a própria dimensão existencial destas informações[150]. Assim, crê-se que, diante da elevada mutabilidade das ferramentas tecnológicas, aliada a baixa percepção social da relevância e sensibilidade do compartilhamento de dados, bem como ausência de referência de seu valor econômico, a letargia no avanço normativo provoca um descompasso entre as garantias necessárias e a positivação das medidas assecuratórias de proteção de dados.

Rodotà[151] complementa esse panorama ao argumentar que a privacidade não pode mais ser reduzida ao conceito clássico de "direito de ser deixado só". Com o surgimento da sociedade da informação e das tecnologias de monitoramento, a privacidade se transformou em um direito de controle sobre o uso das informações pessoais. Isso implica uma redefinição do conceito de privacidade para abranger aspectos coletivos e institucionais, buscando estabelecer mecanismos de controle social e garantir um equilíbrio no exercício do poder de grandes corporações e entidades governamentais. Rodotà enfatiza que a proteção da privacidade deve ir além da defesa individualista, sendo fundamental para assegurar a democracia e a equidade social em um cenário de crescente coleta e tratamento de dados.

---

[149] WARREN, Samuel; BRANDEIS, Louis. **The Right to Privacy**. Civilistica.com, v. 2, n. 3, p. 1–22, 2013. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/127>. Acesso em: 18 jun. 2025.

[150] ROSENVALD, Nelson; MONTEIRO FILHO, Carlos Edison do Rêgo. **Danos causados a dados pessoais: novos contornos**. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/332618/danos-causados-a-dados-pessoais--novos-contornos>. Acesso em: 29 abr. 2024.

[151] RODOTÀ, Stefano, **A vida na sociedade da vigilância – a privacidade hoje**, Rio de Janeiro: Renovar, 2008.

Estabelecida a relevância e importância deste direito, consagrado no artigo 11 do Pacto de São Jose da Costa Rica[152], a sua excepcionalidade deveria ser qualificada e judicialmente fundamentada. Todavia, este não é o cenário apresentado no ordenamento jurídico brasileiro. A banalização da obtenção e disponibilização destas informações estão espraiadas em legislações esparsas, cujo enfrentamento quanto à sua constitucionalidade tem se dado de forma pontual e tem considerado os aspectos fáticos e sociais contemporâneos às manifestações judiciais, a despeito da relevância e magnitude do princípio afrontado, pilar do Estado Democrático de Direito.

A título enumerativo poder-se-ia citar algumas leis que, mesmo de forma reflexa, afetam esse direito: (a) a Lei n.º 9.296/96; (b) o artigo 17-B da Lei n.º 9.613/98; (c) artigo 15 da Lei n.º 12.850/13; (d) artigos 13-A e 13-B do Código de Processo Penal, incluídos pela Lei n.º 13.344/2016; (e) Lei n.º 12.965/2014 – Marco Civil da Internet; e, por fim, (f) Lei n.º 13.709/2018 – Lei Geral de Proteção de Dados Pessoais. Diante do quantitativo de leis ordinárias que tratam a matéria, não são raros os conflitos normativos e as colisões de princípios jurídicos.

Em seu turno, cada normativo mencionado enfrenta seu próprio crivo de constitucionalidade, em julgamentos apartados e lastreados com suas peculiaridades que lhe são exclusivas. Destaca-se a ADI 6.387/DF, cujo objeto versava sobre a Medida Provisória n.º 954/22020 que estabelecia o fornecimento de dados ao IBGE para fins de enfrentamento da Covid-19. A ADPF 695/DF, na qual se abordou o teor do Decreto n.º 10.046/2019, que dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. A ADI 6.529/DF que estabeleceu que os órgãos componentes do Sistema Brasileiro de Inteligência somente podem fornecer dados e conhecimentos específicos à ABIN quando comprovado o interesse público da medida. Outras ADI's também versam acerca do tema: ADI 4.906, ADI 5.059, ADI 5.043 e ADI 5.063, todas, ao fim e ao cabo, destinadas a avaliar a utilização de dados cadastrais, sensíveis ou os estáticos à luz de uma possível afronta à proteção constitucional à privacidade.

3.4. FUNDAMENTOS DA PROTEÇÃO DE DADOS E DA AUTODETERMINAÇÃO INFORMATIVA

[152] Convenção Americana sobre Direitos Humanos (Pacto de San José da Costa Rica), adotada em 22 de novembro de 1969 e promulgada pelo Decreto n. 678, de 6 de novembro de 1992. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/dº0678.htm. Acesso em: 27 mai. 2025.

Até a promulgação da Emenda Constitucional nº 115/2022, a proteção de dados pessoais era compreendida como um direito fundamental implícito, extraído de uma interpretação sistemática e teológica de outros direitos fundamentais positivados na Constituição Federal, especialmente a partir dos princípios da dignidade da pessoa humana (art. 1º, III) e da inviolabilidade da intimidade, vida privada, honra imagem, (art. 5º, X), além do sigilo e inviolabilidade das comunicações (art. 5º, XII). O percurso argumentativo traçado neste capítulo até o presente momento teve como objetivo demonstrar a evolução das necessidades individuais e sociais, cuja proteção jurídica impulsionou uma releitura ampliada desses princípios, agora fortemente marcada pela noção de autodeterminação informativa.

O avanço das tecnologias da informação e a crescente digitalização das interações humanas, inclusive nas relações com o Estado, impuseram novos desafios à tutela dos interesses dos indivíduos. No Brasil, esse fenômeno se intensificou com a consolidação das plataformas de governo digital, em especial por meio do ecossistema de serviços integrados do portal GOV.BR[153], que passou a concentrar dados sensíveis e dados pessoais dos cidadãos. Diante desse cenário, tornou-se inadiável reconhecer o tratamento de dados pessoais como um direito fundamental autônomo, exigindo garantias normativas e institucionais próprias, capazes de assegurar não apenas a proteção contra abusos, mas também a afirmação da liberdade individual e a projeção de seus atributos no ambiente digital.

Nesse mesmo sentido, Ingo Wolfgang Sarlet[154] destaca a incorporação da tecnologia na vida cotidiana das pessoas, referindo-se a esse fenômeno como *Ubiquitous Computing*. Trata-se de uma forma de progresso computacional caracterizada pela integração da tecnologia de maneira tão profunda e constante no cotidiano que ela se torna, ao mesmo tempo, inseparável e invisível aos usuários, operando de modo natural e fluida. Os sistemas computacionais com essa finalidade são concebidos para interagir dinamicamente com o ambiente ao seu redor, seja por meio do compartilhamento de dados com outros dispositivos móveis, seja por conexões com servidores e bancos de dados, a fim de aprender o contexto em que estão inseridos e enriquecer a experiência do usuário com informações e funcionalidades personalizadas[155]. É

[153] BRASIL. Governo lança o Portal Gov.br. Disponível em: https://www.gov.br/sri/pt-br/backup-secretaria-de-governo/assuntos/noticias/noticias-em-acervo/2019/agosto/governo-lanca-portal-gov.br. Acesso em 17 de abril de 2025.

[154] SARLET, Ingo Wolfgang. **Proteção de dados pessoais como direito fundamental na Constituição Federal brasileira de 1988: contributo para a construção de uma dogmática constitucionalmente adequada**. Direitos Fundamentais e Justiça, v. 14, 2020. Disponível em: <https://dfj.emnuvens.com.br/dfj/article/view/875>. Acesso em: 22 abr. 2025.

[155] LYYTINEN, Kalle; YOO, Youngjin, Ubiquitous computing, **Communications of the ACM**, v. 45, n. 12, p. 63–96, 2002.

justamente essa invisibilidade e aparente neutralidade da tecnologia que contribui para que os indivíduos percam, progressivamente, a percepção crítica sobre sua autonomia frente aos sistemas informacionais, enfraquecendo, muitas vezes, a consciência sobre o valor de sua autodeterminação no ambiente digital.

Com essa integração silenciosa da tecnologia ao cotidiano, torna-se essencial a conscientização sobre o valor intrínseco dos dados pessoais e os riscos associados ao seu tratamento. É justamente nesse cenário que se insere o desenvolvimento do direito fundamental à proteção dos dados pessoais, em articulação com o princípio da autodeterminação informativa. Esse direito não nasce dissociado de um histórico de controle estatal da informação, mas como resposta a um processo de transformação no qual os dados deixaram de ser apenas instrumentos administrativos e passaram a constituir ativos estratégicos para o setor público e, mais recentemente, para o setor privado.

Não é irrelevante recordar que o Estado foi, historicamente, o pioneiro na coleta sistemática e na formação de banco de dados sobre seus cidadãos. Como evidenciado na decisão do Tribunal Constitucional Federal Alemão, no caso do microsenso (BVerfGE 27, 1 (6)), já se delineava, desde meados do século XX, o interesse crescente do Poder Público pela obtenção massiva de dados, sob o argumento de subsidiar a formulação de políticas públicas mais eficazes. A época, os custos operacionais para coleta, armazenamento e processamento dessas informações tornavam inviável a participação do setor privado nesse processo[156].

Com o avanço exponencial da tecnologia e redução dos custos computacionais, esse cenário foi radicalmente transformado. O surgimento das hoje denominadas *Bigtechs* tornou possível a iniciativa privada não apenas participar desse ecossistema, mas assumir papel central na coleta, análise e exploração de grandes volumes de dados pessoais. Essa mudança de paradigma revela um novo arranjo de poder informacional, no qual a vigilância e a manipulação de dados não são mais exclusividade do Estado, exigindo, portanto, a reafirmação da autodeterminação informativa como limite e referência na regulação do uso dos dados.

Essa nova dinâmica de forças, provocada pelo impacto disruptivo das tecnologias digitais, tem influenciado diretamente a configuração do ecossistema constitucional, cuja base repousa na harmonia entre normas constitucionais voltadas à proteção dos direitos fundamentais e no equilíbrio entre os Poderes constitucionalmente constituídos. A inserção e atuação das empresas multinacionais de tecnologia têm contribuído para uma reconfiguração

[156] DONEDA, Danilo, **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**, 3. ed. São Paulo: Thomson Reuters Brasil, 2021.

das relações clássicas fundadas no Estado Democrático de Direito, desafiando seus pressupostos estruturais.

Conforme expõe Tamanaha[157], o Estado de Direito (*Rule of Law*) se sustenta em quatro pilares fundamentais: (i) a liberdade individual, que garante aos indivíduos autonomia para agir dentro dos limites da ordem normativa a qual consentiram: (*ii*) a liberdade legal, que impõe ao Estado a observância das leis pré-existentes assegurando previsibilidade e segurança jurídica; (*iii*) a liberdade política, que pressupõe a participação dos cidadãos no processo democrático de criação das leis que os vinculam; e (*iv*) a preservação institucional, que compreende a estrutura organizacional, vertical e horizontal, e procedimental do Estado, concebida para fortalecer o exercício das liberdades individuais.

Entretanto, a atuação dessas multinacionais tecnológicas se dá à margem dessa arquitetura jurídica tradicional. Suas condutas são, em grande medida, orientadas por políticas internas e diretrizes empresariais próprias, propositalmente complexas e não submetidas a processos democráticos ou jurisdicionais típicos dos Estados constitucionais. Diante disso, os Estados enfrentam crescente dificuldade em formular contramedidas constitucionais eficazes que, de um lado, reconheçam e promovam a expansão do exercício dos direitos fundamentais na esfera digital e, de outro, assegurem densidade normativa suficiente para regular o uso de dados pessoais e prevenir violações a esses direitos. Trata-se, como observa a Celeste[158], da urgência de um processo de constitucionalização do ambiente digital, capaz de inserir os agentes privados globais no campo de incidência dos limites constitucionais e dos princípios democráticos.

Assim, o exercício das liberdades no mundo digital e, por conseguinte, os dados pessoais tornam-se o cerne da tutela constitucional contemporânea. Diante disso, revela-se imprescindível a compreensão da conceituação de dados pessoais, na medida em que a sua definição e escopo influenciam a caracterização dos limites e efetividade de sua garantia fundamental. Esse deve ser o ponto de partida para a análise da autodeterminação informativa enquanto projeção da dignidade da pessoa humana na sociedade digital.

Francisco Pereira Coutinho[159] apresenta os metadados, no contexto das comunicações eletrônicas na União Europeia, como informações auxiliares associadas à realização de

---

[157] TAMANAHA, Brian Z., **On the rule of law: History, politics and theory**, Reino Unido: Cambridge University Press, 2011.
[158] CELESTE, Edoardo, Constitucionalismo digital: mapeando a resposta constitucional aos desafios da tecnologia digital, **Direitos Fundamentais & Justiça**, v. 15, n. 45, p. 63–91, 2021.
[159] COUTINHO, Francisco Pereira. **Data Retention in Portugal: Big Brother is (No Longer) Watching**. 2023. Disponível em: <https://papers.ssrn.com/abstract=4216870>. Acesso em: 16 jun. 2025.

comunicações, que não dizem respeito ao conteúdo propriamente dito das mensagens, mas sim às circunstâncias em que a comunicação ocorre. Esses dados se originam do mero uso dos meios e ferramentas como telefonia e internet, bem como compreende elementos como números de telefone utilizados, endereços IP, URL's acessados e informações sobre o posicionamento geográfico dos dispositivos conectados. Em linhas gerais, os metadados traduzem as condições técnicas e operacionais do tráfego das comunicações e do seu faturamento, permitindo a reconstrução do percurso da comunicação e das interações do usuário com sistemas eletrônicos.

Do ponto de vista jurídico, o autor assinala que os metadados devem ser tratados como dados pessoais sempre que possam viabilizar a identificação, direta ou indireta, dos indivíduos relacionados às comunicações. Isso implica que a sua coleta e utilização devem observar os princípios fundamentais do Regulamento Geral sobre a Proteção de Dados, assim como a vinculação a propósitos específicos e legítimos, além da preservação das informações pelo período estritamente necessário ao atendimento dessas finalidades[160].

Em seu turno, Danilo Doneda[161] traz interessantes reflexões acerca da distinção conceitual entre dado e informação, ainda que reconheça que os termos sejam frequentemente utilizados como sinônimos. Para o autor, o "*dado*" corresponde ao conteúdo informacional em estado bruto, isto é, um insumo com potencial de significado, cuja utilidade se revela após sua transmissão, organização ou tratamento. Trata-se, portanto, de uma espécie de "pré-informação". A "*informação*", por sua vez, resulta da extração desse potencial. É o conteúdo interpretado, estruturado, contextualizado ou vinculado apto a gerar sentido e, em determinados casos, conhecimento.

A própria Lei Geral de Proteção de Dados[162], em seu art. 5º, ao definir dados pessoais e dados pessoais sensíveis, adota uma perspectiva prática na qual dado e informação aparecem como termos sinônimos, sempre vinculados à pessoa natural identificada ou identificável:

> Art. 5º Para os fins desta Lei, considera-se:
> I - dado pessoal: **informação** relacionada a pessoa natural identificada ou identificável;
> II - dado pessoal sensível: **dado** pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
> III - dado anonimizado: **dado** relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

---

[160] *Ibid*.

[161] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. 3. ed. São Paulo: Thomson Reuters Brasil, 2021.

[162] BRASIL. Lei n.º 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Diário Oficial da União: seção 1, Brasília, DF, 15 agosto de 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 22 abr 2025.

> IV - banco de dados: conjunto estruturado de **dados** pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

Embora controversa, essa distinção merece acolhida, uma vez que a construção de uma teoria jurídica da informação deve considerar o vínculo objetivo entre o conteúdo informacional e o indivíduo a que ele se refere, de modo que essa conexão configura uma expressão direta de sua personalidade. Nessa perspectiva, esse vínculo entre o dado e o sujeito ultrapassa qualquer consideração sobre a origem ou autoria da informação. Nesse entendimento, Danilo Doneda[163] destaca sobre a lógica dessa argumentação que "*é importante estabelecer este vínculo, pois ele afasta outras categorias de informações que, embora também façam referência a uma pessoa, não seriam consideradas propriamente informações pessoais*".

Esse ponto de vista se harmoniza com a análise desenvolvida por Sandra Wachter e Brent Mittelstadt[164]. Os autores destacam que a vinculação entre o dado e a pessoa não se limita às informações fornecidas diretamente observadas em suas interações. Ela também abrange os dados produzidos por meio de inferências e análises, como os perfis gerados por sistema de inteligência artificial ou ferramentas de big data. Esses dados inferidos, ainda que resultem de operações internas dos agentes de tratamento, são igualmente dados pessoais na medida em que se destinam a descrever, avaliar ou prever atributos do indivíduo, com o impacto potencial sobre a privacidade, autonomia e reputação.

Além das distinções tradicionais entre dado e informação, há uma categorização relevante proposta no contexto europeu, particularmente pelo *Article 29 Working Party*, que aprofunda o debate sobre a natureza dos dados pessoais e reforça a sua aplicação também às inferências. Essa abordagem distingue os dados pessoais quanto a sua origem: de um lado, encontram-se os *dados fornecidos* pelo próprio titular, como nome ou endereço, e os *dados observados*, que são coletados a partir do comportamento do indivíduo durante a interação com serviços, de forma passiva, por exemplo, dados de localização, cliques em páginas ou padrões comportamentais como a escrita ou a forma de caminhar. De outro lado, figuram os dados derivados e inferidos, ou seja, aqueles que não são entregues e nem passivamente percebidos durante o uso de aplicações, mas resultam de operações realizadas pelo controlador ou terceiros com base em informações previamente coletadas[165].

---

[163] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. 3. ed. São Paulo: Thomson Reuters Brasil, 2021, p. 143.
[164] WACHTER, Sandra; MITTELSTADT, Brent, A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI, **Columbia Business Law Review**, v. 2019, p. 494, 2019.
[165] *Ibid*.

Essa distinção é relevante porque evidencia que o titular nem sempre tem ciência da geração desses novos dados pessoais, ainda que eles possam ser igualmente utilizados para tomar decisões ou afetar sua esfera jurídica. O *Article 29 Working Party*, órgão consultivo independente da União Europeia criado com base no artigo 29 da Diretiva 95/46/CE[166], postulou um modelo composto de uma análise de um dado em três dimensões com o intuito de classifica-lo como pessoal, quais sejam, *conteúdo, finalidade e resultado*. Assim, seriam dados pessoais aqueles que: (i) se referem ao conteúdo de uma pessoa identificável, (ii) são usados com propósito de avaliar, tratar ou influenciar o titular; ou (iii) produzem um resultado capaz de afetar seus direitos e interesses. É em relação a este último elemento que a análise das inferências ganha em perspectiva. Mesmo quando não exista uma ligação direta entre o conteúdo do dado e a pessoa, o impacto potencial sobre a esfera jurídica do titular é o requisito necessário para que se imponha a proteção legal típica dos dados pessoais[167].

Portanto, a importância da conceituação precisa dos dados e da identificação do elemento de vinculação reside justamente no fato de que a anonimização ou indeterminação de um dado pressupõe a ruptura desse nexo entre o conteúdo informacional e o sujeito a quem ele se refere. É essa desconexão que impede o dado de ser atribuído a uma pessoa identificada ou identificável, afastando-o do campo de proteção jurídico-personalista. Ademais, ao se tratar de dados desprovidos de correlação específica com o indivíduo, faz-se referência a conteúdos informacionais genéricos, cuja superficialidade impede sua inserção na esfera mais sensível da personalidade, a denominada esfera do segredo (*Geheimsphäre*), a qual deveria ser protegida de forma mais intensa pelo direito geral da personalidade. Assim, a ausência dessa vinculação de alguns dados pode ser um fator determinante na análise da constitucionalidade do uso de geolocalização em procedimentos criminais.

Bruno Bioni[168], ao mencionar a definição linguística de Antonio Houaiss e Mauro de Salles Villar[169], segundo a qual a "*personalidade é a característica ou conjunto de características que distingue uma pessoa*", reforça a compreensão de que o vínculo

---

[166] Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX:31995L0046. Acesso em: 17 jun. 2025.

[167] WACHTER, Sandra; MITTELSTADT, Brent. **A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI**. Columbia Business Law Review, v. 2019, p. 494, 2019. Disponível em: <https://heinonline.org/HOL/Page?handle=hein.journals/colb2019&id=506&div=&collection=>.

[168] BIONI, Bruno. **Proteção de dados pessoais**. 1. ed. Rio de Janeiro: Forense, 2019. Disponível em: <https://www.lexml.gov.br/urn/urn:lex:br:rede.virtual.bibliotecas:livro:2019;001142886>. Acesso em: 12 jun. 2025.

[169] HOUAISS, Antônio; VILLAR, Mauro de Salles. **Dicionário Houaiss da língua portuguesa**. Rio de Janeiro: Objetiva, 2009 *apud* BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro : Forense, 2019. p. 63.

indissociável da informação entre os dados e o sujeito a que se referem faz com que tais dados se constituam em projeções de sua personalidade. Isso porque, ao fim e ao cabo, esses dados permitem a individualização da pessoa, como sua própria expressão, em meio à coletividade, servindo como elemento de identificação no espaço social. Em razão desse aspecto distintivo, a tutela jurídica conferida aos dados pessoais ultrapassa a lógica da privacidade, direcionando-se à tutela da personalidade em sua ostentação pública.

Pela mesma linha de raciocínio, Danilo Doneda[170] rejeita a concepção dos dados pessoais como uma categoria de bem jurídico que atraia, por si só, uma tutela estritamente patrimonialista. O autor alerta para os riscos de uma abordagem que reduza os dados a meros objetos de apropriação, destacando, inclusive, a necessidade de se adotar um tratamento multifacetado, semelhante à lógica aplicada aos direitos autorais, que concilia dimensões patrimoniais e morais. Nesse sentido, embora se reconheça uma certa objetivação dos dados, especialmente no contexto de sua veiculação e tratamento, essa objetivação deve ser compreendida como instrumental e não como característica essencial, servindo apenas para viabilizar sua regulamentação sem que se perca de vista os elementos personalíssimos que lhe são inerentes. Trata-se, portanto, de uma proteção jurídica que, mesmo admitindo traços formais próximos aos direitos reais, devem preservar um vínculo existencial entre o dado e o titular, sem restringi-lo a sua expressão puramente econômica. Bruno Bioni arremata o tema ao afirmar:

> Nesse sentido, os dados pessoais não só se caracterizam como um prolongamento da pessoa (subjetividade), mas, também, influenciam essa perspectiva relacional da pessoa (intersubjetividade). A proteção dos dados pessoais é instrumental para que a pessoa possa livremente desenvolver a sua personalidade[171].

Ingo Sarlet[172] sustenta que o direito à autodeterminação informativa apresenta uma dupla dimensão: (a) individual e (b) coletiva. A dimensão individual relaciona-se a concepção clássica e compreende a visão de direito subjetivo, segundo a qual cada pessoa detém o poder de estabelecer acerca do uso, do acesso, da veiculação e do tratamento de seus dados pessoais. Por sua vez, a dimensão coletiva associa-se à identidade do indivíduo no contexto comunitário,

---

[170] DONEDA, **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**, p. 150–152.

[171] BIONI, Bruno. **Proteção de dados pessoais**. 1. ed. Rio de Janeiro: Forense, 2019. Disponível em: <https://www.lexml.gov.br/urn/urn:lex:br:rede.virtual.bibliotecas:livro:2019;001142886>. Acesso em: 12 jun. 2025, p. 84.

[172] SARLET, Ingo Wolfgang. **Proteção de dados pessoais como direito fundamental na Constituição Federal brasileira de 1988: contributo para a construção de uma dogmática constitucionalmente adequada**. Direitos Fundamentais e Justiça, v. 14, 2020. Disponível em: <https://dfj.emnuvens.com.br/dfj/article/view/875>. Acesso em: 22 abr. 2025.

ressaltando a liberdade desenvolvimento da personalidade em ambiente social para além da concepção estritamente individualista e privada, próprias dos direitos da personalidade.

Considerando esta dimensão coletiva, a necessidade de proteção dos dados relacionada à integração das pessoas em uma sociedade digital, visto que são projeções da personalidade, é expressamente reconhecida por Ingo Sarlet:

> É por tal razão, aliás, que a própria opção terminológica pela proteção de dados pessoais assume uma importância que vai muito além da mera novidade representada pela terminologia em si, porquanto, radica numa viragem concepcional, visto que parte do pressuposto de que dados, para efeitos de sua proteção jurídico-constitucional, devem ser compreendidos em sentido amplo, no sentido da inexistência de dados pessoais irrelevantes ante o processamento eletrônico na sociedade de informação, notadamente pelo fato de que, sendo os dados projeções da personalidade, o seu tratamento, seja qual for, potencialmente pode violar direitos fundamentais[173].

A concepção do livre desenvolvimento da personalidade, tanto no resguardo de sua esfera privada quanto na sua projeção no espaço público, constitui o fundamento a partir do qual se origina a noção do direito à autodeterminação informativa. Esse direito pode ser delineado como a prerrogativa conferida ao indivíduo de controlar o tratamento dos dados que lhe dizem respeito, assegurando não apenas a sua utilização adequada e consentida, mas também a finalidade legítima e a correção no processamento dessas informações.

É inegável que as grandes empresas de tecnologia compreendem a extensão das responsabilidades atribuídas à suas plataformas, assim como o relevante valor econômico que extraem da utilização de dados pessoais e informações associadas ao comportamento de seus usuários[174]. Assim, considerando que o constitucionalismo ainda carece de uma estrutura consolidada que defina contramedidas eficazes[175] e que ofereça um arcabouço normativo capaz de orientar de forma consistente a relação dos Estados juntamente com as *Bigtechs,* o direito à proteção de dados precisa ser compreendido não como uma simples extensão do direito à privacidade, mas assumir particular importância na defesa contra afrontas à intimidade e ao tratamento inadequado de informações pessoais.

Aliado a esse entendimento, deve-se tratar a salvaguarda dos dados também em uma concepção autônoma, especialmente sob a perspectiva da autodeterminação informativa. Esta abordagem autônoma reconhece que, na era digital, o controle sobre os dados pessoais

---

[173] *Ibid*., p. 188–189.

[174] ZUBOFF, Shoshana. **Big Other: Surveillance Capitalism and the Prospects of an Information Civilization**. Journal of Information Technology, v. 30, p. 75–89, 2015.

[175] CELESTE, Edoardo. **Constitucionalismo digital: mapeando a resposta constitucional aos desafios da tecnologia digital**. Direitos Fundamentais & Justiça, Trad. Paulo Renã da Silva Santarém. v. 15, n. 45, p. 63–91, 2021.

transcende a análise puramente restrita à privacidade, ou o direito de ser deixado a sós, abarcando uma série de direitos relacionados ao tratamento justo e transparente das informações dos indivíduos[176].

3.5 PRIVACIDADE DIGITAL E A EVOLUÇÃO DA PROTEÇÃO DE DADOS NO BRASIL

A consolidação da era digital exige uma releitura dos direitos da personalidade, em especial da intimidade e da vida privada, diante das novas formas de exposição do indivíduo no espaço informacional. Como analisa Ilton Norberto Robl Filho, em sua obra "*Direito à intimidade e à vida privada na era digital*"[177], a proteção jurídica da intimidade não deve ser compreendida apenas como objeção à visibilidade e privacidade, mas, sim, como o reconhecimento de um espaço necessário à expressão da intimidade, representando uma relevante missão ao *privacy.* Emerge a noção da extimidade, compreendida como uma forma de tornar público certos aspectos da vida íntima sem que isso represente a perda de sua natureza privada ou mesmo uma autorização para sua reprodução sem a devida cautela e finalidade. Esse é um fenômeno intrínseco à própria contemporaneidade, na qual o sujeito reivindica para si o direito de poder escolher quais experiências deseja compartilhar e, por consequência, reafirma sua autonomia existencial no ambiente digital, podendo auferir proveito individual.

Essa perspectiva promovida pelo autor concede novas possibilidades de valores relacionados à intimidade, a qual passa a não residir apenas no completo sigilo, mas, sim, na possibilidade de autodeterminação sobre os limites entre o público e privado. Isso revela a importância de se assegurar mecanismos jurídicos que sejam revisitados e afastem-se da sua concepção analógica, bem como respeitem a pluralidade de formas de exposição da subjetividade, reconhecendo que a proteção da vida privada, na sociedade digital, deve se articular com a liberdade do indivíduo de construir e projetar sua intimidade. Nesse aspecto, revela-se pertinente, inclusive, a reavaliação das conclusões firmadas pelo Supremo Tribunal Federal no julgamento do tema 876, notadamente no que se refere à rejeição generalizada da tutela jurídica ao direito do esquecimento, em face da complexidade e da multiplicidade de dimensões envolvidas nesse direito, especialmente aquelas relacionadas ao livre

---

[176] BIONI, Bruno. **Proteção de dados pessoais**. 1. ed. Rio de Janeiro: Forense, 2019. Disponível em: <https://www.lexml.gov.br/urn/urn:lex:br:rede.virtual.bibliotecas:livro:2019;001142886>. Acesso em: 12 jun. 2025.

[177] ROBL FILHO, Ilton Norberto, Direito à intimidade e à vida privada na era digital, *in*: **Democracia, direitos humanos e desenvolvimento sustentável: quais os desafios da Itália e do Brasil?**, Napoli: Editoriale Scientifica, 2024, p. 239–248.

desenvolvimento da personalidade, presentes, inclusive, em ordenamentos jurídicos estrangeiros.

Não obstante, o desafio relacionado ao direito a intimidade a vida privada adquiriu novos contornos com advento das tecnologias digitais e consequente intensificação das zonas de contato entre as projeções digitais dos indivíduos e os seus respectivos dados pessoais. No ordenamento jurídico brasileiro, a consolidação desse direito como categoria jurídica autônoma, o direito fundamental à proteção de dados, é consequência de uma construção normativa paulatina e gradual, as quais acompanharam as transformações sociais e tecnológicas da sociedade brasileira.

3.5.1 Lei n.º 9.296/96 – Interceptação telefônica

Diante do contexto retratado, cita-se uma das primeiras normativas brasileiras a tratar diretamente de limitações à atuação estatal em face da privacidade, qual seja, a Lei n.º 9.296/1996, que regulamentou o inciso XII do artigo 5º da Constituição Federal, quanto à interceptação de comunicações telefônicas e de dados. Insta salientar que é uma norma voltada à concretização da cláusula de reserva legal, consubstanciada na exigência de lei formal para restringir ou disciplinar direitos fundamentais, conforme delineado no marco teórico deste trabalho, com base nas contribuições de autores como Robert Alexy, que defendem que toda restrição a direitos fundamentais deve passar por um processo legislativo, cujo objetivo respeite os princípios da legalidade, da proporcionalidade e da reserva de jurisdição.

Assim, tem-se que a interceptação telefônica é a captação de comunicações entre indivíduos, por um terceiro, sem o conhecimento de interlocutores. Consiste em um meio de obtenção de prova, de natureza cautelar, mais invasivos à esfera da privacidade das pessoas à disposição do Estado para fins de concretização do *jus puniendi*[178].

Como dito alhures, a Lei n.º 9.296/1996 estabelece os contornos da medida, fixando como requisitos a prévia e expressa decisão judicial que aponte, de forma inequívoca, a sua imprescindibilidade, além da inexistência de outros meios investigativos eficazes a alcançar a colheita de fontes ou elementos de prova. Isto é, em face da gravidade da medida para o direito fundamental da privacidade, a interceptação só poderá ser admitida como última *ratio*, quando

[178] TOFFOLI, José Antonio Dias, Gravações ambientais, interceptações telefônicas e escutas no processo penal, *in*: MENDES, Gilmar Ferreira; FREITAS, Matheus Pimenta de (Orgs.), **Constituição, Direito Penal e Novas Tecnologias**, São Paulo: Almedina, 2024, p. 127.

não houver alternativa menos invasiva. Esse juízo, reitera-se, deve ser aferido à luz do teste de necessidade, inerente à lógica de solução de colisões entre direitos fundamentais (v. item 2.5).

Contudo, no que se refere à amplitude do objeto da interceptação, merece destaque a contribuição de Luiz Flávio Gomes[179], ao se perfilhar a teoria interna dos direitos fundamentais, segundo a qual cada direito fundamental possui um conteúdo normativo próprio e determinado, sendo suas limitações decorrentes do próprio núcleo essencial que o constitui (v. item 2.4). Com base nessa perspectiva, o autor defende uma interpretação extensiva do termo "comunicação" contido na Lei n.º 9.296/1996, de modo a compreender não apenas o conteúdo literal das conversações, mas também outros elementos correlatos, como dados de identificação da chamada, registros temporais e até mesmo dados de conexão, os quais, embora não integrem o conteúdo da mensagem em sentido estrito, compõem o processo comunicativo e revelam informações sensíveis associados à privacidade do indivíduo:

> Em suma, quando a norma constitucional não possui autorização expressa de limites, a doutrina sustenta a existência de 'limites imanentes'". E a convivência dos direitos fundamentais leva mesmo ao reconhecimento desses limites implícitos ou imanentes. Não vale, em suma, o argumento de que a CF só permitiu a restrição da comunicação telefônica. Quanto a ela, na verdade, existe autorização restritiva expressa. Quanto às comunicações telemáticas (independentes da telefonia), essa permissão é implícita ou imanente. Logo, podia o legislador discipliná-las. A rigor, devia mesmo discipliná-las.
>
> Comunicações telefônicas, hoje, não podem significar só "conversação" ou comunicação de voz. Isso valia para o tempo em que Graham Bell inventou o telefone (1876) ou para o tempo em que foi elaborado o Código Brasileiro de Telecomunicações (art. 4º), em 1962. Não tem sentido nos dias atuais (v. supra itens 8 e 13).
>
> O sigilo de dados, de outro lado, não é absoluto (v. supra item 9, especialmente no que toca ao sigilo de dados telefônicos). Urge reiterar: conforme o constitucionalismo moderno, não existe direito absoluto e o fundamental não é saber se o legislador pode ou não restringir um direito, senão se o faz de maneira excepcional e proporcional, para resolver problemas concretos difíceis e ocorrentes na colisão de direitos fundamentais[180].

A abordagem proposta por Luiz Flávio Gomes, ainda que relevante em seu contexto, exige temperamentos à luz da evolução legislativa e jurisprudencial ocorrida após a publicação de sua obra, datada de 1997. Ressalta-se que o referido autor desenvolveu suas reflexões em um cenário normativo anterior à edição do Marco Civil da Internet, da Lei Geral de Proteção de Dados - LGPD e da Emenda Constitucional n.º 115/2022. Por esse arcabouço normativo, os chamados dados telemáticos, cadastrais e geolocalização passaram a demandar disciplina

---

[179] GOMES, Luiz Flávio; CERNICCHIARO, Raúl, **Interceptação telefônica: lei 9.296, de 24.07.96**, São Paulo: Revista dos Tribunais, 1997.
[180] *Ibid*., p. 173–174.

própria, distinta daquela prevista na Lei n.º 9.296/1996, voltada especificamente à interceptação de comunicações. A propósito, os mandados judiciais de acesso a dados de geolocalização não são, na prática, fundamentados com base nessa legislação, mas, sim, em princípios constitucionais, normativos mais amplos e os artigos 13-B do CPP e 22 do Marco Civil da Internet, evidenciando a ausência de um marco legal específico. Essa lacuna normativa reforça a necessidade de um esforço hermenêutico voltado à construção de critérios compatíveis com a proteção à intimidade à vida privada e à autodeterminação informativa, de forma a evitar decisões arbitrárias e assegurar o respeito às garantias fundamentais de caráter processual.

3.5.2 Código de Defesa do Consumidor

O Código de Defesa do Consumidor (CDC), instituído pela Lei n.º 8.078/1990, representa um marco normativo na consolidação de direitos fundamentais nas relações de consumo no Brasil, antecipando, sob certa perspectiva, a tutela de dados pessoais. Considerando o teor do seu artigo 43, o CDC pode ser interpretado como um dos percursores da legislação brasileira de proteção de dados, ao estabelecer garantias específicas quanto à coleta, armazenamento e divulgação de informações dos consumidores constantes em cadastros e bancos de dados. O dispositivo assegura, por exemplo, o direito de acesso as informações arquivadas, inclusive quanto à sua origem, bem como impõe obrigatoriedade de comunicação prévia ao consumidor em caso de registro negativo, como condição de validade.

Essas previsões antecipam princípios posteriormente consolidados na Lei Geral de Proteção de Dados Pessoais, como a transparência, a finalidade e a necessidade, além de consagrar o direito à retificação de dados. Desta forma, o CDC não apenas coíbe práticas lesivas à dignidade do consumidor no contexto da informação assimétrica, como também inaugurou uma disciplina de controle individual sobre dados pessoais em um período em que proteção de dados ainda não figurava como categoria jurídica autônoma no ordenamento pátrio[181].

Não obstante o inegável avanço, a eficácia do CDC como instrumento de tutela de dados pessoais encontra limitações materiais, dada a sua vocação específica para reequilíbrio das relações consumeristas. Embora a interpretação ampliada de suas disposições tenha contribuído significativamente para os fundamentos de um regime protetivo da informação pessoal, é preciso reconhecer que o Código foi originalmente concebido para equilibrar as assimetrias típicas das relações de consumo e não para disciplinar de forma abrangente o tratamento de

[181] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. 3. ed. São Paulo: Thomson Reuters Brasil, 2021.

dados em múltiplos contextos sociais. Assim, o CDC pode ser compreendido como integrante de um arcabouço normativo mais amplo vinculado ao Sistema Nacional de Defesa do Consumidor que ofereceu suporte inicial à proteção de dados pessoais no Brasil. Essa perspectiva, amplamente discutida por Danilo Doneda[182], evidencia o papel histórico interpretativo do CDC na conformação de princípios que viriam estruturar o atual regime de proteção de dados, ainda que sua aplicação direta permaneça restrita ao campo das relações de consumo.

3.5.3 Marco Civil da Internet

Consoante o desenvolvimento da presente pesquisa, afigura-se que a consolidação da sociedade da informação no Brasil impôs novos contornos ao debate jurídico sobre a privacidade, exigindo respostas legislativas capazes de compatibilizar o desenvolvimento tecnológico à proteção de dados fundamentais. Embora não configure uma lei específica de proteção de dados, a edição da Lei n.º 12.9265/2014, conhecida como Marco Civil da Internet, representa um normativo estruturante da governança digital, vez que disciplina detalhadamente o uso da internet no Brasil, ao introduzir diretrizes principiológicas e garantias mínimas para o tratamento de informações pessoais em ambientes virtuais. Constitui-se, portanto, como instrumento inaugural para a construção de um sistema nacional de proteção de dados, posteriormente consolidado com a LGPD.

Durante a tramitação do projeto de lei que deu origem ao Marco Civil da Internet na Câmara dos Deputados, destacou-se o compromisso institucional com a preservação da integridade do texto, especialmente no que tange à garantia da neutralidade da rede. O processo legislativo foi marcado por intensos debates, tanto técnicos quanto políticos, bem como pela resistência a alterações que comprometessem os princípios fundamentais estabelecidos na proposta inicial, destacado pelo testemunho do Deputado Alexandre Molon[183], relator da matéria na Câmara dos Deputados. Inicialmente concebido como resposta legislativa às vulnerabilidades de espionagem digitais evidenciadas no Brasil em meados de 2010, a condução do trâmite legislativo buscou resguardar o conteúdo normativo frente às pressões de setores econômicos contrários a determinados dispositivos, resultando em um diploma jurídico considerado vanguardista no cenário internacional. Ademais, a ampla participação social,

[182] *Ibid*.
[183] MOLON, Alessandro, Marco Civil da Internet, uma construção da sociedade, *in*: LEITE, George S.; LEMOS, Ronaldo (Orgs.), **Marco Civil da Internet**, Rio de Janeiro: Atlas, 2014, p. xxvii–xxx.

viabilizada por ferramentas institucionais de consulta pública e contribuições abertas à sociedade civil, conferiu ao Marco Civil uma grande legitimidade democrática, rara em legislações dessa natureza[184].

Os princípios estruturantes do Marco Civil, com destaque para a neutralidade da rede, a proteção da privacidade, a inviabilidade das comunicações e a responsabilização não apenas orientam a atividade estatal e o setor privado no ambiente digital, mas também representam vetores interpretativos para o exercício da autodeterminação informativa especialmente diante da relação informacional desproporcional entre usuários e provedores. A neutralidade da rede, ao impedir discriminações no tráfego de dados, assegura o pluralismo e liberdade de acesso à informação. A discussão dessa neutralidade configura-se como um dos pontos mais sensíveis e controversos da regulação jurídica da internet, dada a sua natureza multifacetada que envolve dimensões técnicas, políticas e econômicas. Ainda que o princípio da neutralidade seja amplamente aceito como um ideal normativo em diversas esferas de interação social, sua definição e aplicação no ambiente digital revelam-se especialmente complexas. Essa característica se deve, em grande monta, a estrutura descentralizada heterogênea da internet, que congrega atores com funções sobrepostas, como operadoras de telecomunicações, provedores de acesso, plataformas de conteúdo e redes sociais, cujos interesses frequentemente se contrapõem. Diante desse cenário, torna-se complexa o estabelecimento de uma concepção singular de neutralidade capaz de atender de forma equânime as diferentes esferas de atuação desses agentes[185].

Uma via interpretativa razoável para compreender o conteúdo normativo da neutralidade consiste na recuperação do princípio técnico que orientou a concepção original da internet: arquitetura de rede fim a fim. Com base nesse modelo, os dados transmitidos entre a rede devem ser encaminhados sem qualquer interferência, priorização ou bloqueio indevido por intermediários. Essa lógica guarda semelhança com paradigmas consolidados no direito das comunicações tradicionais, como o sigilo postal e o da correspondência telefônica, nos quais presume-se que o conteúdo circula entre remetente e destinatário sem intervenção ou manipulação. No contexto da internet, a aplicação desse princípio implica a vedação de práticas discriminatórias por parte das operadoras de infraestrutura assegurando que todos os pacotes de dados sejam tratados de forma equânime, independente do conteúdo da origem ou destino. A neutralidade é, portanto, um instrumento normativo essencial para a manutenção da

[184] LEITE, George S.; LEMOS, Ronaldo, **Marco Civil da Internet**, 1. ed. Rio de Janeiro: Atlas, 2014.
[185] GETSCHKO, Demi, As origens do Marco Civil da Internet, *in*: LEITE, George S.; LEMOS, Ronaldo (Orgs.), **Marco Civil da Internet**, 1. ed. Rio de Janeiro: Atlas, 2014, p. 13.

privacidade, a promoção da liberdade de expressão, a concorrência leal entre aplicações e o acesso igualitário de informação[186].

Por sua vez, a proteção da privacidade e a garantia do sigilo das comunicações reafirmam a centralidade da dignidade da pessoa humana em meio à crescente capacidade de rastreamento e de processamento de dados por tecnologias de geolocalização e inteligência algorítmica. A sistemática de proteção à privacidade e a inviolabilidade das comunicações, estabelecida no Marco Civil da Internet, estrutura-se a partir de dispositivos que reconhecem esses direitos como pressupostos essenciais ao exercício do pleno acesso à internet no Brasil. O artigo 8º da Lei n.º 12.965/2014 sedimenta a proteção à privacidade é à liberdade de expressão como fundamentos inarredáveis para o uso legítimo da rede, vinculando sua observância à própria efetividade do direito de acesso à internet. Essa normatividade evidencia que o ambiente digital deve ser estruturado sobre garantias que assegurem a dignidade da pessoa humana e preservação de sua esfera privada e comunicacional. Em reforço a essa lógica protetiva, o artigo 10, parágrafo 2º, do mesmo diploma, estabelece que o conteúdo das comunicações privadas somente pode ser disponibilizado mediante ordem judicial, nos termos e limites legais, assegurando o respeito ao sigilo e à inviolabilidade[187].

É inserido nesse contexto que o artigo 22 do Marco Civil assume especial relevo ao prever a possibilidade de acesso a registros de conexão e de acesso a aplicações mediante ordem judicial para fins investigativos ou instrutórios. A imposição de prazos de retenção, de seis meses para provedores de conexão e de um ano para provedores de aplicações, articula-se com finalidades legítimas de segurança pública, mas suscita importantes questões de compatibilidade com os princípios da finalidade da necessidade e da minimização de dados como delineados na LGPD. A sistemática da retenção compulsória de metadados incluindo informações como endereços IP, data e horário de acesso, torna-se objeto de escrutínio jurídico especialmente quando considerada a sua aptidão para permitir a reconstrução de estatísticas pessoais e padrões comportamentais com elevado grau de intrusão. A questão especificamente acerca da guarda de registros de conexão e de acesso, bem como o artigo 22 da Lei n.º 12.965/2014 serão retomados no capítulo 4 (v. item 4.4.2), vez que são fundamentos utilizados para a expedição dos mandados de geolocalização no Brasil.

---

[186] *Ibid*.

[187] KUJAWSKI, Fabio Ferreira; THOMAZ, Alan Campos Elias, Da proteção aos registros, dados pessoais e comunicações privadas – um enfoque sobre o Marco Civil da Internet, *in*: LEITE, George S.; LEMOS, Ronaldo (Orgs.), **Marco Civil da Internet**, 1. ed. Rio de Janeiro: Atlas, 2014, p. 27–30.

3.5.4 Lei Geral de Proteção de Dados

Como se depreende da evolução normativa histórica anteriormente delineada, a edição da Lei Geral de Proteção de Dados Pessoais, em 2018, constitui o desfecho de um processo marcado pela fragmentação regulatória e pela ausência de um debate interno robusto e sistematizado acerca da tutela da informação pessoal no Brasil. Até então, o tratamento jurídico dos dados pessoais no ordenamento brasileiro era espraiado, apoiando-se em dispositivos constitucionais, como o direito à intimidade, em normas esparsas e em instrumentos como o Código de Defesa do Consumidor e Marco Civil da Internet[188].

Como observa Danilo Doneda[189], o sistema brasileiro de proteção de dados formou-se a partir da adaptação de institutos existentes, como o direito à privacidade, o *habeas data* e normas de proteção ao consumidor, sendo que os conflitos envolvendo dados pessoais foram encaminhados pela via judicial ou por regulamentação setoriais, muitas vezes desvinculados de um eixo conceitual comum, sem, contudo, formar um sistema coeso e compatível com a crescente complexidade das interações digitais na sociedade contemporânea.

A ausência de um marco legal unificado tornou evidente a necessidade de reorganizar o tratamento jurídico dos dados pessoais, assim, a LGPD, inspirada notadamente no Regulamento Geral de Proteção de Dados da União Europeia (GDPR), foi concebida como resposta a esse cenário, estruturando um regime normativo pautado pela autodeterminação informativa, pelo consentimento, pela responsabilização dos agentes de tratamento e pela preservação dos direitos fundamentais. A forte influência europeia na formulação da LGPD é inegável, sobretudo no tocante a conceitos como "*privacy by design*", "*accountability*" e o tratamento diferenciado de dados sensíveis. Essa incorporação normativa externa, embora tenha impulsionado o processo legislativo, não foi acompanhada por uma adaptação criteriosa aos contornos institucionais e culturais do direito brasileiro, o que resultou em lacunas interpretativas e desafios operacionais na aplicação da lei[190].

---

[188] OLIVEIRA, Marco Aurélio Bellizze; LOPES, Isabela Maria Pereira. **Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018**, *in*: FEIGELSON, Bruno; SIQUEIRA, Antonio Henrique Albani (Orgs.), **Comentários à Lei Geral de Proteção de Dados: Lei 13.709/201**, São Paulo: Thomson Reuters Brasil, 2019.

[189] DONEDA, Danilo. **A LGPD como elemento estruturante do modelo brasileiro de proteção de dados**, *in*: CUEVA, Ricardo Villas Bôas; DONEDA, Danilo; MENDES, Laura Schertel (Orgs.), **Lei Geral de Proteção de Dados (Lei nº 13.709/2018) [livro eletrônico]: a caminho da efetividade – contribuições para a implementação da LGPD**, 1. ed. São Paulo: Thomson Reuters Brasil, 2020.

[190] OLIVEIRA, Marco Aurélio Bellizze; LOPES, Isabela Maria Pereira. O**s princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018**. *In*: FEIGELSON, Bruno; SIQUEIRA, Antonio Henrique Albani (Orgs.). Comentários à Lei Geral de Proteção de Dados: Lei 13.709/201. São Paulo: Thomson Reuters Brasil, 2019.

O consentimento do titular para o tratamento de seus dados pessoais emerge como elemento central na arquitetura normativa da Lei Geral de Proteção de Dados, possuindo uma função estruturante, seja pela densidade dos requisitos que o qualificam, seja pela centralidade dos direitos do titular no regime da LGPD. A legislação impõe que o aceite do titular seja expresso com clareza, fruto de uma deliberação consciente e suficientemente informada, de forma a assegurar que ele compreenda a finalidade específica que seus dados serão submetidos. A lei rejeita permissões genéricas ou vagas, exigindo que o escopo do tratamento seja determinado previamente e, caso venha ser alterado de modo substancial, que o titular seja informado, podendo, inclusive, revogar sua anuência[191].

Esse desenho busca atenuar a assimetria informacional existente entre o indivíduo e os agentes de tratamento, criando garantias que protejam a autonomia do cidadão mesmo em contextos de vulnerabilidade contratual ou tecnológica. Isto posto, a LGPD estabelece regras que coíbem práticas enganoso abusivas por parte dos controladores, impedindo a obtenção do consentimento por meios obscuros, contraditórios ou que dificultem o exercício do controle pelo titular.

Ao reconhecer que o consentimento não pode ser uma formalidade vazia, mas sim um instrumento legítimo de autodeterminação informativa, a LGPD reforça a exigência da boa-fé e transparência por parte dos responsáveis pelo tratamento de dados. A própria possibilidade de revogação do consentimento, bem como a vinculação do tratamento a propósitos bem definidos e compatíveis com a expectativa legítima do titular, revela uma tentativa de concretizar um ambiente regulatório pautado pelo respeito à liberdade individual e ao controle sobre as informações pessoais[192].

Contudo, essa interpretação restritiva não esgota a relevância normativa da LGPD no ordenamento jurídico brasileiro. Como sustentado por Danilo Doneda[193], a sistemática de proteção de dados emergiu de maneira fragmentada e reativa, mais influenciada por modelos estrangeiros do que por um amadurecimento interno consistente. Assim, a LGPD representa não apenas o marco regulatório setorial, mas também uma síntese axiológica da trajetória de consolidação do direito fundamental à proteção de dados no Brasil. Seus princípios, como

---

[191] ALIMONTI, Veridiana, Autodeterminação informacional na LGPD: antecedentes, influências e desafios, *in*: CUEVA, Ricardo Villas Bôas; DONEDA, Danilo; MENDES, Laura Schertel (Orgs.), **Lei geral de proteção de dados (Lei nº 13.709/2018): a caminho da efetividade: contribuições para a implementação da LGPD [livro eletrônico]**, ePUB. São Paulo: Thomson Reuters Brasil, 2020.

[192] *Ibid*.

[193] DONEDA, Danilo. A LGPD como elemento estruturante do modelo brasileiro de proteção de dados. *In*: CUEVA, Ricardo Villas Bôas; DONEDA, Danilo; MENDES, Laura Schertel (Orgs.). **Lei Geral de Proteção de Dados (Lei nº 13.709/2018) [livro eletrônico]: a caminho da efetividade – contribuições para a implementação da LGPD**. 1. ed. São Paulo: Thomson Reuters Brasil, 2020.

finalidade, necessidade, transparência, segurança e responsabilização, não podem ser compreendidos como disposições estanques, mas sim como vetores interpretativos com vocação expansiva para outras esferas do direito, inclusive a penal.

Essa compreensão principiológica foi expressamente acolhida na IX Jornada de Direito Civil, promovida pelo Conselho da Justiça Federal, cujo Enunciado n.º 678[194] reconhece que, mesmos nos casos excepcionados pela Lei n.º 13.709/2018, aplicam-se o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos na lei, ainda que se aguarde a edição de legislação específica. Esse posicionamento reforça a ideia de que os princípios informadores da LGPD constituem um mínimo ético jurídico a ser observado em qualquer tratamento de dados pessoais, mesmos nas hipóteses relacionadas à persecução penal.

Assim, embora LGPD, em sua literalidade, exclua do seu escopo as atividades de investigação criminal, não se pode ignorar que os valores fundamentais que a informam devem orientar o desenvolvimento de normas específicas no âmbito penal e, até mesmo, servir de parâmetro de interpretação das normas já existentes. Essa aplicação principiológica revela-se indispensável para o equilíbrio entre as necessidades da segurança pública e a proteção dos direitos fundamentais especialmente em um contexto de crescente complexidade tecnológica e ampliação das possibilidades de vigilância estatal.

Cumpre destacar, ainda que sem a pretensão de esgotar o tema, dada a multiplicidade de iniciativas legislativas sobre a matéria, que há distintos esforços voltados à regulamentação do tratamento de dados pessoais no âmbito penal. Dentre eles, merece atenção anteprojeto de lei elaborado por uma comissão de juristas, cujo resultado do trabalho foi entregue à Presidência da Câmara dos Deputados, em novembro de 2020, e de conteúdo fortemente inspirado na Diretiva (EU) 2016/680, do Parlamento Europeu e do Conselho, que versa sobre o tratamento de dados para fins de investigação e repressão infrações penais[195]. Esse anteprojeto limitava-se a disciplinar as hipóteses previstas nas alíneas "a" e "d" da Lei 13.709/2018, isto é, exclusivamente os contextos de segurança pública e atividades de investigação e repressão penal.

---

[194] IX JORNADA DE DIREITO CIVIL. Enunciado nº 678. Ao tratamento de dados realizado para os fins exclusivos elencados no inciso III do art. 4º da Lei Geral de Proteção de Dados (segurança pública, defesa nacional; segurança do Estado e atividades de investigação e repressão de infrações penais), aplicam-se o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos na LGPD, sem prejuízo de edição de legislação específica futura. Comissão de Trabalho: Direito Digital e Novos Direitos. Coordenador: Ministro Villas Bôas Cueva. Coordenador-Geral: Ministro Jorge Mussi. Brasília: Centro de Estudos Judiciários do Conselho da Justiça Federal, 2023. Disponível em: https://www.cjf.jus.br/enunciados/enunciado/1817. Acesso em: 10 jun. 2025.

[195] AZEVEDO, Cynthia Picolo Gonzaga de *et al*, **Nota técnica: análise comparativa entre o anteprojeto de LGPD penal e o PL 1515/2022**, [s.l.]: Instituto de Referência em Internet e Sociedade (IRIS); Laboratório de Políticas Públicas e Internet (LAPIN), 2022.

Independente deste trabalho técnico, também tramita atualmente na Câmara o Projeto de Lei n.º 1515/2022, que apresenta a proposta semelhante em relação a sua inspiração europeia, contudo há uma disciplina distinta e mais abrangente. O referido PL amplia o escopo normativo para regular todas as hipóteses do inciso III do art. 4º da LGPD, incluindo, além da segurança pública e investigação criminal, também a defesa nacional e segurança do Estado. Há ainda referências a serviços de inteligência e outras atividades correlatas. Não obstante, tanto o Projeto de Lei n.º 1515/2022 quanto o anteprojeto citado adotam uma estrutura normativa de caráter principiológico similar à da LGPD, mas fazendo, também, remissões à legislação processual penal e à futura regulamentação específica para disciplina de alguns aspectos, como o monitoramento de indivíduos. Em todo o caso, o resultado dessas propostas visa suprimir a lacuna existente no ordenamento jurídico brasileiro no que tange ao tratamento de dados pessoais para fins penais, estabelecendo diretrizes conciliam a proteção dos direitos fundamentais dos titulares com a efetividade das atividades estatais de segurança persecução penal.

CAPÍTULO 4: A INVESTIGAÇÃO CRIMINAL E OS LIMITES IMPOSTOS PELA CONSTITUIÇÃO

Como desenvolvido ao longo deste trabalho, os direitos fundamentais possuem uma dimensão negativa, os quais impõem ao Estado o dever de abstenção em relação a condutas que possam comprometer a esfera jurídica individual. Esse equilíbrio normativo é próprio do Estado de Direito e, de forma indissociável, dele decorre a exigência de que toda atuação estatal se submeta aos limites legais, em estrita observância ao princípio da legalidade. Por sua vez, essa legalidade confere previsibilidade e segurança jurídica ao sistema processual penal, atribuindo densidade material ao princípio do devido processo legal penal.

Mendes e Branco[196] fazem referência à expressão alemã *Justizgrundrechte* para designar o rol de proteção dos *direitos fundamentais de caráter judicial*, consagrados na Lei Fundamental da Alemanha, notadamente nos artigos 19, 101 e 103[197]. Esses dispositivos compõem um núcleo protetivo voltado a essa objeção da atuação estatal, assegurando garantias mínimas ao devido processo legal em sentido amplo, não restrito apenas à esfera penal, mas estendido a todas as relações processuais. Esse conjunto normativo essencial representaria a expressão instrumental de defesa dos indivíduos, não apenas no âmbito processual penal.

Partindo dessas premissas, temos que o inquérito preliminar não está imune à incidência desses princípios fundamentais. Como adverte Guilherme de Souza Nucci[198], a atividade

---

[196] MENDES, Gilmar Ferreira; COELHO, Inocêncio Mártires; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional**. 2. ed. São Paulo: Saraiva, 2008, p. 490.

[197] ALEMANHA. *Lei Fundamental da República Federal da Alemanha* (Grundgesetz). Artigos 101 a 104. Disponível em: https://www.gesetze-im-internet.de/englisch_gg/englisch_gg.html#p0571. Acesso em: 8 mai. 2025:

"Article 19 [Restriction of basic rights – Legal remedies]
(1) Insofar as, under this Basic Law, a basic right may be restricted by or pursuant to a law, such law must apply generally and not merely to a single case. In addition, the law must specify the basic right affected and the Article in which it appears.
(2) In no case may the essence of a basic right be affected.
(3) The basic rights shall also apply to domestic legal persons to the extent that the nature of such rights permits.
(4) Should any person's rights be violated by public authority, he may have recourse to the courts. If no other jurisdiction has been established, recourse shall be to the ordinary courts. The second sentence of paragraph (2) of Article 10 shall not be affected by this paragraph.
(…)
Article 101 [Ban on extraordinary courts]
(l) Extraordinary courts shall not be allowed. No one may be removed from the jurisdiction of his lawful judge.
(2) Courts for particular fields of law may be established only by a law.
(..)
Article 103 [Fair trial]
(1) In the courts every person shall be entitled to a hearing in accordance with law.
(2) An act may be punished only if it was defined by a law as a criminal offence before the act was committed.
(3) No person may be punished for the same act more than once under the general criminal laws".

[198] NUCCI, Guilherme de S., **Curso de Direito Processual Penal**, 21. ed. Rio de Janeiro: Forense, 2024.

investigativa deve observar com rigor o princípio da legalidade, a vedação das provas ilícitas e os demais enunciados constitucionais que orientam o devido processo legal desde os momentos iniciais da persecução penal:

> O princípio regente do devido processo legal, como já mencionado, abrange a coletânea de princípios penais e processuais penais, devendo ser integralmente seguido, para que se possa obter uma punição justa.
> Aponta-se, em grande parte, a sua incidência sobre o processo-crime, mas olvida-se a sua relevância para a fase da investigação policial. Há que se ponderar a medida do acerto e do equívoco dessa visão.
> O acerto cinge-se à inexigência de seguimento direto a certos princípios, como a ampla defesa, o contraditório, a publicidade, a presunção de inocência, dentre outros, que são aplicáveis ao processo.
> O equívoco é imaginar que todos os princípios penais e processuais penais somente se aplicam ao processo criminal, pois a persecução estatal pode oprimir o indivíduo desde o início, que ocorre na fase do inquérito. Diante disso, mantêm-se ativos durante a devida investigação penal os princípios da legalidade, da retroatividade benéfica, da culpabilidade, da imunidade à autoacusação, da vedação das provas ilícitas, dentre outros, perfeitamente compatíveis com a atividade do Estado na busca do crime e de seu autor[199].

De acordo com esse berço teórico, a investigação criminal é tradicionalmente compreendida como uma fase pré-processual, de natureza administrativa, voltada à preparação da futura ação penal. Ainda que não seja regida pelo princípio do contraditório, típico da fase processual, não se encontra isenta de controle jurídico, sendo caracterizada por um contraditório diferido, cujos efeitos se projetam para etapa processual. Trata-se de um momento destinado à apuração de um fato determinado, à verificação da materialidade e à identificação de autoria, na lição de Aury Lopes Jr. [200]: "*elemento subjetivo acidental da notícia-crime*. *Não é necessário que seja previamente atribuída a uma pessoa determinada.* ***A atividade de identificação e individualização da participação será realizada no curso da investigação preliminar".*** (Destacou-se).

A investigação criminal, à luz da lógica do sistema processual penal de estrutura mista adotado no ordenamento jurídico brasileiro, configura-se como uma fase pré-processual destinada à apuração da materialidade do fato e à identificação de eventuais indícios de autoria. Sua finalidade precípua é formar um juízo de probabilidade suficientemente consistente para justificar a instauração da ação penal, sem o qual não se legitima o exercício da pretensão punitiva estatal. Nessa etapa, a autoridade responsável atua com base em uma hipótese investigativa fundada em elementos que lastreiam um juízo de possibilidade sobre a ocorrência

---

[199] *Ibid*., p. 59.
[200] LOPES JR., Aury. **Direito Processual Penal**. 22. ed. Rio de Janeiro: SRV, 2025, p. 136. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788553625673/>. Acesso em: 12 maio 2025.

de uma infração penal (*fumus commissi delicti*), promovendo diligências voltadas à obtenção de dados concretos capazes de fortalecer, ou não, essa hipótese.

Importa destacar que, embora antecedente à formação da relação processual penal, a fase investigativa não está excluída do âmbito de incidência dos direitos fundamentais de matriz processual. A sua condução deve observar rigorosamente o princípio da legalidade, cuja força normativa projeta-se sobre todas as esferas da atuação estatal. Guilherme Nucci[201], inclusive, pontua que "*o princípio da legalidade é absoluto, em qualquer plano"*, e "*deve ser fielmente respeitado"*. Assim, a atividade investigatória não pode ser conduzida de forma arbitrária ou desvinculada de controle jurídico, exigindo sempre a observância dos critérios normativos que asseguram a racionalidade, a necessidade e a proporcionalidade dos meios empregados.

A investigação criminal deve partir de um juízo inicial de possibilidade e, no decorrer da apuração, evoluir para um juízo de probabilidade capaz de fundamentar, de modo consistente, a decisão do Ministério Público quanto ao oferecimento da denúncia. Na ausência de elementos de convicção suficientes para caracterizar a justa causa, o encaminhamento legítimo, nesse caso, será o arquivamento dos autos, como forma de resguardar o princípio da não culpabilidade e evitar a instauração indevida do processo penal.

Ressalta-se que, não obstante o juízo de possibilidade que fundamenta a instauração de uma investigação criminal se volte à proteção dos interesses da sociedade, não se pode ignorar que a mera deflagração da atividade investigativa já representa, em alguma medida, uma incursão na esfera de direitos fundamentais dos indivíduos nela envolvidos. E esse tensionamento torna-se ainda mais evidente quando são empregadas técnicas intrusivas, como acesso a dados de geolocalização, que não apenas comprometem a privacidade dos investigados, mas também podem alcançar terceiros alheios à prática delituosa, submetendo-os, ainda que indiretamente, ao controle investigativo do Estado.

É justamente nesse ponto que se impõe uma distinção qualitativa no grau de fundamentação exigido para medidas dessa natureza. Se a abertura do inquérito policial pode se apoiar em indícios mínimos, um juízo de possibilidade, o mesmo não se pode admitir para a requisição de dados de natureza íntima, como os de localização geográfica. O acesso a esse tipo de informação, por sua natureza dotada de elevada carga de intimidade e relacionada à rotina dos indivíduos, exige a demonstração de uma *probable cause*, isto é, um juízo de probabilidade qualificado e baseado em elementos objetivos e concretos que justifiquem a medida. A adoção

[201] NUCCI, Guilherme de S. **Curso de Direito Processual Penal**. 21. ed. Rio de Janeiro: Forense, 2024, p. 59. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9786559649280/>. Acesso em: 12 maio 2025.

desse parâmetro mais elevado de fundamentação não apenas protege contra arbitrariedades, mas resguarda o núcleo essencial dos direitos fundamentais frente ao avanço das tecnologias de vigilância e ao poder investigativo do Estado.

4.1. IMPACTOS DAS TECNOLOGIAS DIGITAIS NAS GARANTIAS DO PROCESSO PENAL

Como anteriormente apontado, a crescente inserção das *Bigtechs* no ecossistema constitucional tem desestabilizado essa equação tradicional, introduzindo novos desequilíbrios de poder e desafios à conformação do processo penal, ainda amplamente estruturado sob paradigmas "analógicos". Trata-se, portanto, de um cenário em que a própria essência do processo penal, com seus princípios do contraditório, ampla defesa, imparcialidade e legalidade estrita, encontra-se tensionada pelas ferramentas digitais contemporâneas, que, se não devidamente regulamentadas, podem representar risco efetivo à preservação das garantias processuais fundamentais.

A exemplo dessas medidas que afetam a coletividade indistintamente e fogem ao escopo das garantias previstas no processo penal tradicional, poder-se-ia mencionar a utilização de algoritmos que analisam e processam dados em massa para prever ou monitorar atividades criminais. Isso ocorre porque o processo penal, em sua forma clássica, foi estruturado para tratar de relações diretas entre o indivíduo e o Estado, onde o exercício do poder punitivo é previsível, legalmente pautado e regulamentado. Todavia, com o avanço de novas tecnologias de vigilância e controle, como a inteligência artificial e a mineração de dados, o *ius puniendi* do Estado passa a ser exercido de maneira menos transparente e mais indireta, dificultando o controle jurídico sobre essas práticas[202].

O Direito Civil oferece uma proteção mais robusta aos direitos da personalidade, em especial à privacidade, em relação ao Direito Penal. Isso se deve, em grande monta, à própria natureza dos seus normativos, voltadas à garantia dos direitos individuais e à regulação das relações entre particulares que estão em mesma hierarquia nos polos dos conflitos. Em contrapartida, com premissa ontológica distinta e partes da relação processual específicas, o Direito Penal tem como finalidade precípua a persecução de ilícitos penais e a aplicação de sanções estatais, a partir da atuação do titular da ação penal.

---

[202] GARCIA, Rafael de Deus, **Processo penal e algoritmos: o Direito à privacidade aplicável ao uso de algoritmos no policiamento**, Tese (Doutorado em Direito), Universidade de Brasília, Brasília, 2022.

Com efeito, as tutelas civis dos direitos da personalidade, em especial aquelas que se relacionam à proteção da privacidade, não encontram correspondência, tampouco a mesma densidade protetiva, na esfera penal[203]. Essa assimetria torna-se ainda mais evidente diante de transformações provocadas pelas novas tecnologias empregadas no policiamento, como sistemas de vigilância em massa, algoritmos de predição criminal e outras ferramentas digitais voltadas ao controle social, como a geolocalização.

Essas tecnologias, a operarem com base em lógica estatística e automatizada, tendem a desconsiderar as nuances subjetivas, reduzindo o indivíduo a categorias abstratas e, por vezes, reforçando estigmas sociais[204]. Isso não apenas acentua a seletividade e desigualdade estrutural já presentes no sistema penal, mas revela fragilidades profundas quanto à efetivação das garantias processuais. A naturalização desse *bias*, estrutural e algorítmico, demanda a necessidade de restruturação do processo penal, na medida em que se torna necessária a consideração, de forma crítica, os novos modos de relações sociais e os impactos que as tecnologias produzem sobre os direitos da personalidade.

Embora o presente trabalho não se aprofunde especificamente sobre o uso de algoritmos, é inegável que essas tecnologias se inserem no mesmo contexto do desafio tecnológico central aqui abordado, pois também se valem da coleta e do processamento massivo de dados para produzir, entre outros efeitos, previsões. Como toda ferramenta tecnológica, os algoritmos não são neutros: refletem escolhas humanas e estão impregnados dos princípios, valores e concepções dos seus programadores.

Os algoritmos são frequentemente percebidos como uma "entidade" de natureza complexa, sobretudo por estudiosos das ciências humanas. Embora, à primeira vista, possam parecer desafiar a lógica do raciocínio, sua definição objetiva revela justamente o oposto. Consiste no uso organizado e estruturado da lógica para desenvolver instruções e etapas previamente definidas com o objetivo de solucionar problemas. A partir de um ponto de partida, essas etapas são seguidas de forma clara e ordenada, permitindo alcançar um resultado ou realizar uma tarefa de modo facilitado ou automatizado[205].

Além disso, o uso de algoritmos remonta a discussões éticas acerca da imparcialidade, discriminação e a precisão das decisões automatizadas. Não obstante essas codificações sejam capazes de processar logicamente grandes quantidades de dados, elas também podem reproduzir e perpetuar preconceitos ou erros sistêmicos, especialmente se forem baseados em

[203] *Ibid*.
[204] *Ibid*.
[205] *Ibid*.

dados enviesados em sua origem[206]. Em um contexto de policiamento, isso pode resultar na criminalização desproporcional de certos grupos sociais ou regiões, sem que essas práticas estejam adequadamente protegidas ou reguladas pelas garantias processuais tradicionais.

De forma objetiva, o conjunto codificado de instruções faz do algoritmo um reflexo das escolhas e intenções de quem o desenvolve. Os interesses e comandos humanos são embutidos em sua arquitetura e direcionam sua operação rumo a um resultado previamente delineado. Mantida essas premissas e adotando-se uma perspectiva ampliada, é possível afirmar que a utilização de dados pessoais em fluxos informacionais processados por sistemas automatizados visa estruturar o convencimento do destinatário da informação. No entanto, esse processo persuasivo pode ser artificialmente manipulado. Consiste, assim, em uma dinâmica que ultrapassa a mera apresentação neutra de dados. Configura-se uma forma de manipulação da percepção e, no último estágio, de ressignificação da realidade[207].

A transposição dessa lógica para o âmbito investigativo evidencia uma preocupação central deste trabalho: a possibilidade de que os mandados de geolocalização e uso massivo de dados, muitas vezes mediados por sistemas automatizados ou algoritmos, conduzam à produção de inferências imprecisas, enviesadas ou desproporcionais. Esse quadro amplia o risco de decisões judiciais ou investigativas baseadas em dados fora de contexto, comprometendo a proteção dos direitos fundamentais. A relevância do tema reside justamente na necessidade de que esses instrumentos sejam acompanhados de rigorosos filtros normativos e procedimentais, aptos a evitar abusos e distorções.

O tratamento de dados de forma randômica e impessoal, desvinculado da lógica individualizada do processo penal, pode conduzir a investigações enviesadas. Em vez de refletirem a busca pela verdade real, as apurações passam a ser orientadas por padrões estatísticos, generalizações e inferências automatizadas. O seu desfecho é a distorção da finalidade investigativa, com a substituição da suspeita fundada por inferências probabilísticas que podem servir mais à confirmação de narrativas do que a apuração imparcial dos fatos[208].

São justamente esses efeitos impessoalizantes ou objetificantes, decorrentes da aplicação de determinadas ferramentas tecnológicas no âmbito da persecução penal que os direitos fundamentais de caráter processual buscam coibir. Esses mecanismos, ao reduzir o

---

[206] NUNES, D.; MARQUES, A. L. P. C., Inteligência artificial e direito processual: vieses algorítmicos e os riscos de atribuição de função decisória às máquinas, **Revista dos Tribunais Online, Revista de Processo**, v. 285, p. 421–447, 2018.

[207] CARDONA, Tamires Diniz, **Sentidos de cuidado por educadores/cuidadores de crianças acolhidas institucionalmente**, Dissertação de Mestrado, Universidade Federal de Pernambuco, Recife, .

[208] GARCIA, Rafael de Deus. **Processo penal e algoritmos: o Direito à privacidade aplicável ao uso de algoritmos no policiamento**. Tese (Doutorado em Direito), Universidade de Brasília, Brasília, 2022.

indivíduo a padrões estatísticos ou aglomerado de dados, podem comprometer a legitimidade e a regularidade das funções investigativas do Estado. Por isso, a necessidade de reiterar que a atuação estatal deve ser pautada estritamente pelo princípio da legalidade.

Ao fixarem essa relação normativa no âmbito do Estado Democrático de Direito, os direitos fundamentais de caráter processual, ainda que demandem revisitação de suas interpretações frente às realidades tecnológicas, não podem ser relativizadas ou mitigadas. Sua preservação é expressão da maximização do princípio da dignidade da pessoa humana, visando que o processo penal continue a desempenhar sua função constitucional de limitar o poder punitivo do Estado e proteger o indivíduo contra abusos[209].

Embora ventile discussões pertinentes ao tema em questão, o Supremo Tribunal Federal teve a oportunidade de avaliar a relação entre os direitos constitucionais à privacidade e à proteção de dados em cotejo com as atividades de inteligência estatais, no julgamento conjunto das ADIs nº 6649 e 695. Do acórdão, extrai-se que o compartilhamento de informações pessoais no âmbito das atividades de inteligência deve observar tanto a legislação específica quanto os parâmetros fixados no julgamento da ADI 6.529, Rel. Min. Cármen Lúcia[210], quais sejam:

> (i) adoção de medidas proporcionais e estritamente necessárias ao atendimento do interesse público; (ii) instauração de procedimento administrativo formal, acompanhado de prévia e exaustiva motivação, para permitir o controle de legalidade pelo Poder Judiciário; (iii) utilização de sistemas eletrônicos de segurança e de registro de acesso, inclusive para efeito de responsabilização em caso de abuso; e (iv) observância dos princípios gerais de proteção e dos direitos do titular previstos na LGPD, no que for compatível com o exercício dessa função estatal.

Há que se ressalvar, todavia, que não há uma exata delimitação do conceito de serviços de inteligência, nem se esses serviços abrangeriam ou estariam correlacionados às investigações criminais. Naquela oportunidade, o STF debruçou-se sobre a requisição de informações pela ABIN e supostas "ações de espionagem", sem enfrentar diretamente a tese da obtenção de dados de geolocalização. Dessa forma, permanece a necessidade de observância ao disposto em legislação específica, a qual, até o momento, não existe de forma clara e específica quanto ao tratamento de dados que possibilitam a geolocalização.

---

[209] MENDES, Gilmar Ferreira; COELHO, Inocêncio Mártires; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional**. 2. ed. São Paulo: Saraiva, 2008.

[210] BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade n. 6.529. Rel. Min. Cármen Lúcia. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=757870910. Acesso em 16 dez. 2024.

Este elevado controle social, atrai as reflexões de Michel Foucault ao mencionar o edifício utópico "Panóticon" idealizado por Bentham, cuja arquitetura propiciava a vigilância e controle social:

> No Panópticon vai se produzir algo totalmente diferente; não há mais inquérito, mas vigilância, exame. Não se trata de reconstituir um acontecimento, mas de algo, ou antes, de alguém que se deve vigiar sem interrupção e totalmente. Vigilância permanente sobre os indivíduos por alguém que exerce sobre eles um poder - mestre-escola, chefe de oficina, médico, psiquiatra, diretor de prisão - e que, enquanto exerce esse poder, tem a possibilidade tanto de vigiar quanto de constituir, sobre aqueles que vigia, a respeito deles, um saber[211].

4.2. PRINCÍPIOS CONSTITUCIONAIS APLICÁVEIS À INVESTIGAÇÃO CRIMINAL

Norberto Bobbio, ao prefaciar a obra Direito e Razão – Teoria do Garantismo Penal de Luigi Ferrajoli[212], ressalta que a visão garantista tem o intuito de descrever premissas de um sistema cujo objetivo é obstar o exercício arbitrário do Estado em prejuízo das liberdades e direitos individuais, principalmente instrumentalizado no Direito Penal. Esse catálogo normativo da teoria garantista fixaria a regra do jogo e determinaria que haveria o governo das leis, "*sub lege* e *per leges*, culminando na diferenciação entre o meramente legal e o estritamente legal.

De fato, como reiteradamente afirmado, o papel do princípio da legalidade torna-se, então, elemento essencial para a contenção do arbítrio estatal e para a proteção dos direitos fundamentais dos indivíduos submetidos à persecução penal. Para tanto, o processo penal, compreendendo a sua fase anterior da investigação criminal, desenvolve-se no sentido de ser um instrumento de proteção para adequação do método de pesquisa em busca da verdade e não apenas objetivando a concretude da persecução penal[213].

No entanto, a necessidade de se conceder amplitude material à segurança jurídica, promovida pela aplicação estrita do princípio da legalidade no processo penal, não deve comprometer a eficácia do procedimento investigativo. Por outro lado, é preciso reconhecer que o processo penal hoje se insere em uma realidade marcada pela interação constante com novas tecnologias e métodos de investigação, que se apoiam no rastreamento de registros

---

[211] FOUCAULT, Michel. **A verdade e as formas jurídicas**. Tradução de Roberto Cabral de Melo Machado e Eduardo Jardim Morais, **Rio de Janeiro: NAU Editora**, 2002.
[212] FERRAJOLI, Luigi. **Direito e razão: teoria do garantismo penal**, [s.l.]: editora revista dos tribunais São Paulo, 2010.
[213] PEREIRA, Eliomar da Silva. **Teoria da investigação criminal**, 1. ed. São Paulo: Editora Almedina Brasil, 2010.

gerados pela massiva produção de dados pessoais. Esse novo cenário impõe o desafio de compatibilizar uso legítimo desses recursos com a preservação das garantias fundamentais que estruturam o devido processo legal.

Considerando essa lógica garantista, Ferrajoli[214] explicita que o princípio da legalidade no sentido lato vincula-se à *reserva relativa de lei*, esta, na sua acepção formal, oriunda de um processo legislativo regular, a qual determina e subjuga a atuação dos magistrados ao seu teor normativo. E esse entendimento se coaduna com a teoria externa das restrições aos direitos fundamentais, que não seriam absolutos e cuja delimitação ocorreria mediante a "*compatibilização concreta dos diferentes interesses, princípios e valores igualmente protegidos pela Constituição*"[215].

Com base nessa premissa firmada e revisitando lição de Virgílio Afonso da Silva[216], embora reconhecidamente controversa na doutrina, o autor sustenta que a afirmação de não haver um direito fundamental de caráter absoluto constitui, a seu ver, uma "ideia absolutamente equivocada". Para ilustrar esse posicionamento, aponta como exemplo a garantia da reserva legal e da anterioridade da lei penal, previstas no artigo 5º, inciso XXXIX, da Constituição, cujo conteúdo não admite mitigação.

Ademais, resgatam-se as premissas teóricas delineadas no Capítulo 2 deste trabalho, especialmente no que tange a teoria dos limites dos direitos fundamentais, com o objetivo de estruturar o raciocínio que relaciona os direitos fundamentais de natureza processual à utilização da geolocalização como meio de obtenção de prova no curso de investigações criminais.

Não obstante os requisitos e possibilidades de restrição aos direitos fundamentais não estejam expressamente disciplinados de forma sistematizada na Constituição Federal de 1988, a aplicação do princípio da legalidade encontra-se claramente prevista no artigo 5°, inciso II[217], segundo o qual "*ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei*".

A partir desse enunciado normativo fundamental, extrai-se, de forma implícita, que quaisquer limitações ao exercício de direitos fundamentais devem necessariamente ter como

---

[214] FERRAJOLI, Luigi. **Direito e razão: teoria do garantismo penal**. [s.l.]: editora revista dos tribunais São Paulo, 2010.

[215] CORDEIRO, Karine da Silva; SCHAFER, Jairo Gilberto. **Restrições a direitos fundamentais**, *in*: ASENSI, Felipe Dutra; PAULA, Daniel Giotti de (Orgs.), Tratado de Direito Constitucional: Constituição, política e sociedade, 1. ed. Rio de Janeiro: Elsevier, 2014, v. 1.

[216] SILVA, Virgílio Afonso da. **Direito constitucional brasileiro**. São Paulo: Edusp. 2021.

[217] BRASIL. **Constituição Federal 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 15 mai. 2025.

fundamento legal uma lei, em sentido formal e material, emanada do Poder Legislativo, aprovada mediante o devido processo legislativo e compatível com os parâmetros constitucionais.

A doutrina constitucional alemã avança neste tema ao prever critérios estritos expressos para a restrição de direitos fundamentais. O artigo 19 da *Grundgesetz*, anteriormente citado, estabelece que a lei restritiva deve ter aplicação geral e abstrata, vedada sua utilização para casos específicos, bem como deve ainda mencionar expressamente qual o direito fundamental está sendo limitado, com a respectiva indicação de sua previsão normativa. Essa conceituação encontra correspondência no que a doutrina denomina teoria dos limites dos direitos fundamentais, a partir da qual se desenvolve a chamada teoria dos limites dos limites (*Schranken-Schranken*). Segundo essa teoria, toda intervenção estatal que implique restrição a um direito fundamental somente será legítima se observar cumulativamente os seguintes requisitos: (i) esteja prevista em lei formal; (ii) a restrição deve possuir uma finalidade específica; (iii) atenda ao princípio da proporcionalidade; e, por fim, (iv) não deve violar o núcleo essencial do direito fundamental afetado[218].

Articulado com esses parâmetros acima alinhavados, há que se ressaltar, ainda, a necessidade de observar a reserva de jurisdição. A denominada cláusula de reserva de jurisdição deve ser compreendida na exigência de que determinadas medidas, diante de sua natureza excepcional, estejam sujeitas exclusivamente à autorização judicial prévia. Nos termos consignados no acórdão do STF, no MS n.º 23.452/RJ, de relatoria do Ministro Celso de Mello, essa cláusula impõe a submissão "*à esfera única de decisão dos magistrados, a prática de determinados atos cuja realização, por efeito de explícita determinação constante do próprio texto da Carta Política, somente pode emanar do juiz e não de terceiros*"[219].

Por conseguinte, o uso da geolocalização como técnica de investigação criminal ainda carece de regulamentação legal específica no ordenamento jurídico brasileiro. Essa lacuna normativa levanta sérias dúvidas quanto à legitimidade de medidas que, embora úteis a persecução penal, impactam diretamente a privacidade e a liberdade de locomoção dos indivíduos. Diante dessa ausência de regulação, a admissibilidade da geolocalização como meio de prova só poderia ser justificada a partir de um juízo de ponderação entre princípios

[218] PEREIRA, Eliomar da Silva. **Teoria da investigação criminal**. 1. ed. São Paulo: Editora Almedina Brasil, 2010.
[219] BRASIL. Supremo Tribunal Federal. MS 23.452/RJ, Rel. Min. Celso de Mello, Tribunal Pleno, julgado em 16 set. 1999, publicado no Diário de Justiça em 12 mai. 2000. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=85966. Acesso: 25 mai. 2025.

fundamentais, nos moldes propostos por Robert Alexy[220], efetuados perante um Juízo competente.

Implica, desta forma, reconhecer que apenas o princípio fundamental colidente, dotado de peso argumentativo superior no caso concreto, como por exemplo o dever de o Estado proteger a vida ou a segurança pública, poderia fundamentar o cotejo de uma restrição aos direitos fundamentais de caráter processual. Ainda assim, nessa hipótese, deveriam ser respeitados os critérios de adequação, necessidade e proporcionalidade em sentido estrito. Fora dessa moldura teórica, qualquer medida restritiva que se pretenda legítima não passaria de instrumento de erosão indevido das garantias fundamentais do processo penal.

4.2.1 Teoria da Prova

Há que se ressaltar que uso de ferramentas que proporcionam a geolocalização situa-se no campo dos meios de obtenção de prova no processo penal. Desta feita, são necessárias algumas observações sobre a teoria da prova, apenas com o fito de melhor ilustrar ou posicionar o debate no âmbito do direito processual penal.

Para evitar a tautologia ou mesmo a redundância no anseio de melhor conceituação de "prova" dentro de sua teoria geral, traz-se definição sedimentada por Aury Lope Jr.[221], segundo o qual prova consiste nos "*meios através dos quais se fará essa reconstrução do fato passado (crime)*". Essa concepção deriva da ideia de que o processo penal tem como uma de suas finalidades a reconstituição de um evento pretérito, o possível fato delituoso, e suas circunstâncias, permitindo a formação de um juízo racional e fundamentado. É um instrumento voltado à construção de conhecimento sobre um fato juridicamente relevante, cuja finalidade é a demonstração ou procedimento voltado a um saber orientado à busca da verdade material, submetida ao crivo da autoridade judicial[222].

Fixada a conceituação de prova e sua finalidade, para a obtenção desses elementos voltados ao conhecimento do juiz, há que se considerar que existem procedimentos que devem ser observados com o intuito de garantir que os resultados obtidos sejam provas válidas, lícitas e idôneas a serem utilizadas no processo penal. Por esta razão, a Teoria Geral da Prova abarca a análise dos meios de prova, os quais seriam, nas palavras de Eliomar da Silva Pereira[223], "*as*

---

[220] ALEXY, Robert. **Teoria dos direitos fundamentais**. Trad. Virgílio Afonso da Silva. 5ª ed. São Paulo : Editora Malheiros, 2008.
[221] LOPES JR., Aury. **Direito Processual Penal**. 22. ed. Rio de Janeiro: SRV, 2025, p. 399. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788553625673/>. Acesso em: 12 maio 2025.
[222] PEREIRA, Eliomar da Silva. **Teoria da investigação criminal**. 1. ed. São Paulo: Editora Almedina Brasil, 2010.
[223] *Ibid*.

formas legalmente estabelecidas pelo Código de Processo Penal, formas como as provas se revelam no processo". Por sua vez, Aury Lopes Jr. destaca a necessidade de distinguir com evidência o que seriam os "meios de prova" e os "meios de obtenção de provas":

> a) Meio de prova: é o meio através do qual se oferece ao juiz meios de conhecimento, de formação da história do crime, cujos resultados probatórios podem ser utilizados diretamente na decisão. São exemplos de meios de prova: a prova testemunhal, os documentos, as perícias etc.
>
> b) Meio de obtenção de prova: ou mezzi di ricerca della prova como denominam os italianos, são instrumentos que permitem obter-se, chegar-se à prova. Não é propriamente "a prova", senão meios de obtenção. Explica MAGALHÃES GOMES FILHO[64] que os meios de obtenção de provas não são por si fontes de conhecimento, mas servem para adquirir coisas materiais, traços ou declarações dotadas de força probatória, e que também podem ter como destinatários a polícia judiciária. Exemplos: delação premiada, buscas e apreensões, interceptações telefônicas etc. Não são propriamente provas, mas caminhos para chegar-se à prova[224].

Com essa definição do autor, poder-se-ia afirmar que os meios de obtenção de prova possuem natureza instrumental, isto é, são as ferramentas ou medidas processuais que, desde que conduzidas conforme as prescrições legais, destinam-se à obtenção de fontes ou elementos de prova, os quais poderão ser incorporados ao acervo probatório e considerados no juízo de convencimento do magistrado. A questão central que se impõe é que, justamente por constituírem procedimentos destinados à produção de prova e, por conseguinte, potencialmente invasivo aos direitos fundamentais, sua adoção e hipóteses devem encontrar respaldo expresso em lei. Essa exigência normativa é devidamente ressaltada por Gustavo Henrique Badaró, ao observar que:

> Em regra, os meios de obtenção de prova implicam restrição a direitos fundamentais do investigado, em geral liberdades públicas ligadas à sua privacidade ou intimidade ou à liberdade de manifestação do pensamento. É o que ocorre na quebra de sigilo bancário ou fiscal, em que há restrição à intimidade (CR, art. 5.º, caput, X), na busca domiciliar, que implica restrição à inviolabilidade do domicílio (CR, art. 5.º, caput, XI) ou, ainda, à interceptação telefônica, realizada como exceção constitucionalmente prevista à liberdade de comunicação telefônica (CR, art. 5.º, caput, XII) [225].

Há que se destacar, ainda, que o artigo 155 e seu parágrafo único do Código de Processo Penal estabelecem os limites para os meios de prova, remetendo à legislação civil os casos em que a prova disser respeito ao estado das pessoas. A sistemática adotada pelo CPP indica que os meios de prova previstos naquele diploma, como a prova testemunhal, pericial, documental, confissão, reconhecimento de pessoas, acareação etc., são considerados provas típicas, por

---

[224] LOPES JR., Aury. **Direito Processual Penal**. 22. ed. Rio de Janeiro: SRV, 2025, p. 430. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788553625673/>. Acesso em: 12 maio 2025.
[225] BADARÓ, Gustavo Henrique. **Processo penal**, 10. ed. São Paulo: Thomson Reuters Brasil, 2024.

possuírem procedimento próprio e disciplina legal. No entanto, com o avanço das tecnologias e novas formas de obtenção de conhecimento, outros meios tornaram-se cientificamente lastreados a comporem o conjunto probatório da ação penal, as denominadas provas atípicas. Ou seja, seriam atípicas aquelas provas cujos meios não estão expressamente previstos no rol do Código de Processo Penal, mas sua validade e admissibilidade decorrem da confiabilidade científica e da observância aos princípios constitucionais do processo penal.

Em seu turno, insta salientar que o artigo 157 do CPP veda a utilização de provas produzidas por meios ilícitos, entendidas como aquelas que foram "*obtidas em violação a normas constitucionais ou legais*". Logo, as provas típicas possuem rito e procedimento a serem observados para sua produção. Por sua vez, embora não taxativamente previstas, mas considerando sua consistência metodológica, as provas atípicas seriam igualmente admitidas, porém, em todos os casos, seriam inadmissíveis aquelas angariadas com afronta ao princípio da legalidade, em prejuízo das normas constitucionais ou legais estatuídas. Aury Lopes Jr. (2025, p. 454) ressalta as cautelas imprescindíveis à admissibilidade das provas atípicas, pontuando que sua utilização somente se legitima quando respeitados os direitos fundamentais e as balizas normativas constitucionais:

> Não se trate de uma prova "típica", mas sim feita em desconformidade com o padrão legal estabelecido, pois, nesse caso, a atipicidade decorre de uma violação da forma, da lei que estabelece seus requisitos, e essa defraudação conduz a ilicitude probatória. Portanto, cuidado: o fato de admitirmos as provas atípicas não significa que permitimos que se burle a sistemática legal. Assim, não pode ser admitida uma prova "disfarçada" de inominada quando na realidade ela decorre de uma variação (ilícita) de outro ato estabelecido na lei processual penal, cujas garantias não foram observadas. Exemplo típico de prova inadmissível é o reconhecimento do imputado por fotografia, utilizado, em muitos casos, quando o réu se recusa a participar do reconhecimento pessoal exercendo seu direito de silêncio (*nemo tenetur se detegere*). O reconhecimento fotográfico, como explicaremos a seu tempo, somente pode ser utilizado como ato preparatório do reconhecimento pessoal, nos termos do art. 226, inciso I, do CPP, nunca como um substitutivo àquele ou como uma prova inominada[226].

Com base no exposto, evidencia-se que o mandado judicial que autoriza o fornecimento de informações capazes de viabilizar a geolocalização de indivíduos deve ser compreendido como meio de obtenção de prova. Por sua natureza, sua adoção exige previsão legal expressa, não apenas em virtude de sua natureza processual, mas, sobretudo, em razão de seu conteúdo intrinsecamente restritivo de direitos fundamentais. Por se tratar de medida que interfere diretamente na esfera da privacidade e da autodeterminação informativa, sua legitimidade e

[226] LOPES JR., Aury. **Direito Processual Penal**. 22. ed. Rio de Janeiro: SRV, 2025, p. 454. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788553625673/>. Acesso em: 12 maio 2025.

legalidade estão condicionadas à observância do princípio da reserva legal e de jurisdição, exigindo-se autorização normativa prévia e específica, nos moldes já discutidos anteriormente quando foram abordadas as condições constitucionais para a restrição de direitos fundamentais, ainda mais aqueles de caráter processual.

4.2.2 Pesca Probatória ou "*fishing expedition*"

Quando se delimitou os contornos da investigação criminal e seus princípios norteadores, afirmou-se que sua finalidade precípua é a apuração de um fato determinado, sobre o qual recaia um juízo de *fumus commissi delicti*. Essa finalidade cinge a atuação das autoridades investigativas, na medida em que os atos praticados durante essa fase de investigação, embora voltados à elucidação da verdade e levantamento de conhecimento, por vezes incidem sobre direitos fundamentais. Por este motivo, essas medidas devem observar, de forma estrita, o princípio da legalidade e os preceitos do devido processo legal, que baliza a atuação estatal num contexto de Estado Democrático de Direito. A superação desses limites, especialmente quando se busca produzir provas de forma indiscriminada ou sem relação específica ou justa causa com um fato delituoso concreto, caracteriza a chamada *fishing expedition*, prática incompatível com as garantias constitucionais de caráter processual que pautam o processo penal[227].

A definição de *fishing expedition* também é concebida por Alexandre Morais da Rosa e Viviani Ghizoni Silva como sendo aquela investigação dotada de caráter genérico, sem causa provável, a qual visa à produção de provas por meio de procedimentos cuja integridade em face dos parâmetros e princípios estabelecidos pela Constituição e pelo processo penal tornam-se questionáveis, obrigando a busca pela legitimação posterior das provas coligidas:

> o fishing expedition ou a 'pescaria probatória' constitui em um meio de 'investigação especulativa indiscriminada, sem objetivo certo ou declarado que, de forma ampla e genérica, 'lança' suas redes com esperança de 'pescar' qualquer prova para subsidiar uma futura acusação ou para tentar justificar uma investigação/ação já iniciada[228].

[227] LOPES JR., Aury. **Direito Processual Penal**. 22. ed. Rio de Janeiro: SRV, 2025. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788553625673/>. Acesso em: 12 maio 2025.
[228] SILVA, Viviani Ghizoni; SILVA, Philipe Benoni Melo e; ROSA, Alexandre Morais da. **Fishing expedition e encontro fortuito na busca e apreensão.** Florianópolis: EMais, 2019.

Não obstante mencionem que o julgamento do HC n.º 137.828/RS[229], de relatoria do Ministro Dias Toffoli, tenha representado a primeira manifestação do Supremo Tribunal Federal acerca do conceito de *fishing expedition*, é importante destacar que, naquele caso, o termo foi empregado no relatório apenas para reproduzir os argumentos dos impetrantes, não integrando a fundamentação da decisão. Por outro lado, no julgamento da Reclamação n.º 43.479/RJ[230], a Corte efetivamente enfrentou o tema de maneira mais aprofundada, inclusive citando expressamente a definição apresentada por Alexandre Morais da Rosa, conforme anteriormente mencionado.

No caso citado, reconheceu-se que o *fishing expedition* caracteriza-se como procedimento investigativo orientado à obtenção indiscriminada de elementos probatórios, ainda que desprovidos de estreita relação com o fato que originou a investigação, com o objetivo de identificar, de forma genérica e prospectiva, eventuais elementos úteis a outros propósitos. Essa prática viola os princípios da legalidade, da proporcionalidade e da especialidade da prova. Avançando-se no debate, inclusive chegou-se a suscitar a discussão sobre o conceito de *lawfare*, entendido como a utilização estratégica do procedimento legitimamente autorizado por autoridades investigativas com fim de legitimar, a posteriori, atos de coleta clandestina de provas, as quais comprometeriam a integridade do conjunto probatório.

Não obstante a evidente ilicitude do *fishing expedition*, salienta-se a sua distinção em relação ao encontro fortuito de provas. A prova colhida de maneira acidental tem sido admitida sob a perspectiva do princípio da serendipidade. Esse princípio consiste na obtenção de elementos probatórios não diretamente buscados, mas que foram encontrados incidentalmente e guardam alguma conexão, mesmo que probatória ou intersubjetiva, com a investigação original. Para essas hipóteses, admitir-se-ia certa flexibilização do princípio da especialidade da prova, contanto que o procedimento inicial tenha observado rigorosamente os limites legais. Essa condição se estabelece em virtude de a autorização judicial para a produção probatória ser, simultaneamente, vinculada, pois exige motivação concreta e o cumprimento de requisitos legais, e vinculante, à medida que os elementos colhidos só podem ser utilizados dentro dos fins e do escopo previamente autorizados. Desta forma, o encontro fortuito de provas apenas

[229] BRASIL. Supremo Tribunal Federal. Habeas Corpus nº 137.828/RS. Rel. Min. Dias Toffoli, julgado em 14 dez. 2016. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=310968214&ext=.pdf. Acesso em 19 mai. 2025.

[230] BRASIL. Supremo Tribunal Federal. Reclamação RCL nº 43.479/RJ. Relator Ministro Gilmar Mendes, julgado em 10 ago. 2021. Disponível em: https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/Rcl43479VotoMGM.pdf. Acesso em: 19 mai. 2025.

será legítimo quando decorrer de um procedimento regular, previamente delimitado, e não de uma devassa genérica incompatível com o devido processo legal[231].

É justamente nessa linha tênue que se inserem os mandados de geolocalização. A depender do momento de sua expedição e da fundamentação apresentada para a sua adoção, essa ferramenta pode se aproximar de uma hipótese de *fishing expedition*, na medida em que a coleta massiva de dados de localização tem o potencial de revelar uma multiplicidade de comportamentos e deslocamentos, gerando vínculos indiretos com outras condutas eventualmente tidas como delituosas, a partir das quais se pode construir artificialmente uma narrativa de conexão com o fato originalmente investigado.

4.3 MANDADOS DE GEOLOCALIZAÇÃO PELO MUNDO

4.3.1 Estados Unidos

Nos Estados Unidos da América, os chamados *geofence warrants* começaram a ser utilizados por autoridades investigativas a partir de 2016, inicialmente com o objetivo de confirmar os deslocamentos de indivíduos já identificados como suspeitos no curso de investigações criminais em andamento. Nesses casos, a medida era autorizada judicialmente com base em um juízo prévio de plausibilidade quanto à autoria e à materialidade delitiva, servindo como técnica auxiliar de reconstrução probatória[232]. O fornecimento dos dados era, em grande monta, realizado pelas *Bigtechs*, como o Google, que já dispunham de infraestrutura tecnológica e expertise jurídica para processar essas solicitações. Esse movimento evidencia que o uso da geolocalização digital, mesmo antes da consolidação da discussão jurídica em torno da sua constitucionalidade, já se inseria como uma prática institucionalidade no relacionamento em matéria de persecução penal entre as entidades públicas responsáveis por investigação e o setor privado.

A análise relevante da constitucionalidade da obtenção de dados geolocalização no sistema jurídico norte-americano ocorreu no julgamento da Suprema Corte no caso *Carpenter v. United States*, em 2018. Naquela oportunidade, discutia-se a legalidade da obtenção de registros históricos de localização de celular (CSLI), diretamente das operadoras de telefonia, com base em simples "*judicial order*" fundada na Stored Communications Act (SCA), e não

---

[231] LOPES JR., Aury. **Direito Processual Penal**. 22. ed. Rio de Janeiro: SRV, 2025. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788553625673/>. Acesso em: 12 maio 2025.

[232] OWSLEY, Brian L., The best offense is a good defense: Fourth Amendment implications of geofence warrants, **Hofstra Law Review**, v. 50, n. 4, 2022.

em observância à reserva de jurisdição, que compreenderia a análise por um magistrado competente acerca do caso concreto (*warrant)*. A Suprema Corte, por maioria, entendeu que essa prática violava a 4ª Emenda da Constituição dos Estados Unidos, reconhecendo que os dados de localização revelam padrões profundos e contínuos da vida do indivíduo e, diante disso, estão protegidos por uma expectativa razoável de privacidade, exigindo-se a expedição de um mandado judicial formal com base em uma *probable cause.*

Especificamente, *Carpenter* tratava de uma medida individualizada, direcionada ao investigado previamente identificado e fundada em dados fornecidos por operadoras de telefonia (geolocalização derivada de informação compulsória). A questão, embora seja um marco quanto ao reconhecimento da sensibilidade dos dados de localização, ainda não contemplava a complexidade dos chamados *warrants* de geolocalização, posteriormente objeto do julgamento do caso People v. Meza[233], em 13 de abril de 2023, pela Corte de Apelações da Califórnia.

Diferentemente do precedente *Carpenter*, no caso *Meza* a autoridade policial buscou do Google a extração e fornecimento de dados de localização de todos os dispositivos que estiveram presentes em determinadas áreas geográficas, durante faixas horárias específicas, sem qualquer delimitação quanto à identidade dos usuários ou existência de suspeita prévia. Essa modalidade de mandado representa uma forma de investigação por exclusão, em que os dados são primeiramente coletados de modo massivo e, apenas posteriormente, filtrados pela autoridade com base em seus próprios critérios (geolocalização derivada de informação consentida).

A Corte da Califórnia declarou que esses mandados genéricos violam a 4ª Emenda por ferirem os princípios da particularidade e da causa provável, bem como os equiparou aos antigos "mandados gerais" (*general warrants*), historicamente rejeitados no direito norte-americano por permitirem varreduras indiscriminadas. Ainda que fundadas em mandado judicial formal, os *geofence warrants* foram considerados inconstitucionais por sua amplitude desproporcional e pela ausência de restrição objetiva à discricionariedade estatal.

Outro elemento distintivo reside na plataforma de coleta. Enquanto no caso *Carpenter* envolvia operadoras de telefonia, cuja coleta de dados CSLI é passiva e restrita a registros de torres de comunicação, os *geofence warrants* exploram a funcionalidade "*Location History*" do Google, que registra com precisão muito superior dos deslocamentos dos usuários, conforme salientado anteriormente. Desse modo, a diferença essencial entre os dois precedentes reside

[233] ESTADOS UNIDOS. *People v. Meza*. Court of Appeal of the State of California. Disponível em: https://www.eff.org/files/2023/04/21/b318310_opf_people_v._meza_et_al.pdf. Acesso em 17 set. 2023.

não apenas no instrumento legal (*judicial order* em contraposição aos *geofence warrants*), mas também no grau de generalidade da medida, no objeto de coleta (individualizado x massivo), na precisão dos dados e na plataforma utilizada. A jurisprudência norte-americana, portanto, caminhou para reconhecer que, embora o uso do mandado judicial seja requisito necessário, ele não é suficiente quando a medida violar valores constitucionais da razoabilidade, da proporcionalidade e da especificidade da prova.

Assim, os *warrants* começaram a enfrentar questionamentos judiciais mais incisivos em meados de 2020, justamente em razão dos protestos relacionados aos movimentos *Black Lives Matter*. As impugnações judiciais concentraram-se na alegada violação à 4ª Emenda Constitucional Americana, que protege os cidadãos contra buscas e apreensões arbitrárias e estabelece a necessidade de demonstração de *probable cause* para a emissão de ordens judiciais invasivas.

Além disso, argumentou-se *que Geofence Warrants* permitiam a identificação massiva de indivíduos presentes em determinada área geográfica, o que, na prática, possibilitaria a elaboração de perfis ideológicos e políticos de cidadãos em pleno exercício do direito à manifestação. Essa prática seria incompatível com os princípios democráticos e representaria um preocupante instrumento de vigilância estatal generalizada, com impacto significativo sobre os direitos à privacidade, à liberdade de expressão e à liberdade de reunião.

Mais recentemente, a inconstitucionalidade do *geofence warrant* foi reafirmada pela Corte de Apelações do Quinto Circuito, no caso *United States v. Smith* (2024)[234], no qual foi enfatizado que os mandados configuram verdadeiros instrumentos de varredura digital, dissociados da exigência de individualização da suspeita e de delimitação específica da coleta probatória. A Corte entendeu que esses mandados, ainda que formalmente autorizados por autorização judicial, são incompatíveis com a proteção constitucional contra buscas não razoáveis, por meio da emissão de acesso indiscriminado a dados de localização de milhões de indivíduos.

Por outro lado, o quarto circuito ao apreciar o caso *United States v. Chatrie*[235], manteve a validade de um *geofence warrant*, ainda que com voto dividido entre os magistrados quanto aos fundamentos. A divergência revelou uma tensão não resolvida acerca da aplicabilidade da doutrina da expectativa razoável de privacidade aos dados de localização armazenados por

[234] UNITED STATES v. Smith, 110 F.4th 817 (5th Cir. 2024). Disponível em: https://law.justia.com/cases/federal/appellate-courts/ca5/23-60321/23-60321-2024-08-09.html. Acesso em: 26 maio 2025.

[235] UNITED STATES v. Chatrie, 107 F.4th 319 (4th Cir. 2024). Disponível em: https://www.ca4.uscourts.gov/opinions/224489.p.pdf. Acesso em: 26 maio 2025.

terceiros, especialmente em situações nas quais o usuário teria previamente consentido, ainda que de forma genérica, com a coleta dos dados. Enquanto parte da Corte entendeu que o consentimento contratual afasta a proteção da 4ª Emenda, outra parte sustentou que a simples aceitação de termos de uso não equivale a autorização irrestrita de acesso estatal.

Diante dessas decisões conflitantes, configura-se um *circuit split*, a qual é uma divergência interpretativa entre cortes de apelação federal, que reforça a possibilidade de futura revisão pela Suprema Corte dos Estados Unidos, com o objetivo de uniformizar a compreensão constitucional sobre a legitimidade dos *geofence warrants*[236]. Esse cenário revela que, no sistema jurídico norte-americano, ainda que tenha havido avanços no reconhecimento da proteção à privacidade em face da tecnologia, a efetividade dessa proteção depende da clareza normativa, da adequação dos instrumentos judiciais utilizados e do controle proporcional das medidas intrusivas.

Por óbvio, os casos americanos citados servem para o estudo dos fundamentos e inteligência daquele país sobre os mandados de geolocalização, haja vista ser o *judicial review* o seu sistema de controle difuso de constitucionalidade e o direito comparado não ser objeto específico do presente estudo.

4.3.2 Portugal

A legislação portuguesa que regula o acesso a metadados de comunicações eletrônicas para fins de investigação criminal, originalmente estabelecida pela Lei n.º 32/2008, de 17 de julho, foi substancialmente reformulada com a promulgação da Lei n.º 18, de 5 de fevereiro de 2024. Essa alteração normativa teve como principal objetivo assegurar a conformidade do ordenamento jurídico nacional com os parâmetros estabelecidos pelo Tribunal de Justiça da União Europeia e pelo Tribunal Constitucional Português. O novo regime buscou estabelecer um equilíbrio entre essas exigências de eficácia na persecução penal e observância dos limites constitucionais à retenção e utilização de metadados, impondo garantias legais reforçadas para sua coleta, conservação e acesso, sob estrito controle judicial.

Nesse sentido, cabe destacar que a Lei n.º 32/2008 havia sido elaborada para incorporar ao ordenamento jurídico português a Diretiva n.º 2006/24/CE, do Parlamento Europeu, que impunha aos provedores de serviços e as operadoras de telecomunicações a obrigação de reter dados de tráfego de internet e de chamadas telefônicas, ainda que limitados a registros

[236] O'ROURKE, Mollye, Fourth and Fifth Circuits Split Over Geofencing in Fourth Amendment Interpretation, **Lincoln Memorial University Law Review Archive**, v. 12, n. 2, 2025.

considerados “estáticos”, como informações cadastrais, datas, horários e duração das comunicações[237].

Embora não houvesse acesso ao conteúdo das mensagens, entendeu-se que tais elementos eram suficientes para permitir a reconstrução da rotina e dos hábitos dos usuários, por meio da chamada engenharia reversa. Essa técnica, ao combinar dados isolados, possibilita traçar com precisão o perfil comportamental dos cidadãos, inferindo padrões de deslocamento, frequência de contatos e tendências de consumo.

Esse potencial invasivo foi reconhecido pelo Tribunal de Justiça da União Europeia, que invalidou a referida Diretiva em 2014, em resposta a pedidos do Tribunal Supremo Irlandês e do Tribunal Constitucional Austríaco (casos apensados C-293/12 e C- 594/12)[238]. A Corte considerou que a exigência ampla e generalizada de retenção de dados, sem critérios objetivos e salvaguardas eficazes, violava os direitos fundamentais da privacidade e a proteção de dados pessoais, consagrados nos artigos 7º e 8º da Carta de Direitos Fundamentais da União Europeia[239]:

> A Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Diretiva 2002/58/CE, é inválida.

Esse julgamento representou um marco na proteção dos dados pessoais na Europa, ao reconhecer que metadados, mesmo sem revelar diretamente o conteúdo das comunicações, podem impactar gravemente a esfera privada ao permitir um mapeamento das redes sociais padrões de comportamento e aspectos sensíveis da vida cotidiana. Pode-se afirmar que esta Diretiva permitia um dos primeiros *data exhaust*, que compreenderia o procedimento de obtenção de informações da vida cotidiana dos indivíduos (*small data)*, sua análise e

---

[237] COUTINHO, Francisco Pereira. **Data Retention in Portugal: Big Brother is (No Longer) Watching**. 2023. Disponível em: <https://papers.ssrn.com/abstract=4216870>. Acesso em: 16 jun. 2025.

[238] UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia. Acórdão de 8 de abril de 2014, nos processos apensados C-293/12 e C-594/12. Digital Rights Ireland Ltd v. Minister for Communications e outros. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A62012CJ0293. Acesso em 05 de abril de 2025.

[239] “***Artigo 7****. Respeito pela vida privada e familiar*

> Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações.

Artigo 8*. Protecção de dados pessoais*

> Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito.

> Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação.

> O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente”.

Disponível em European Commission and European Parliament, Carta dos direitos fundamentais da União Europeia, Publications Office, 2001. Acesso em 05 de abril de 2025.

descaracterização, tornando-os abstratos e passíveis de tratamento, com valor comercial agregado, porém sem chamar atenção de autoridades reguladoras[240].

Posteriormente, em Portugal, o seu respectivo Tribunal Constitucional, ao apreciar a compatibilidade da legislação nacional com os direitos fundamentais consagrados na Constituição, declarou, com eficácia geral, a inconstitucionalidade de dois dispositivos da Lei n.º 32/2008. O primeiro refere-se à norma que impunha a obrigação genérica de conservação de dados de tráfego e localização por parte dos prestadores de serviços de comunicações eletrônicas, entendida como incompatível com as garantias constitucionais da proteção de dados pessoais, à reserva da vida privada e ao princípio da proporcionalidade. O segundo ponto de inconstitucionalidade identificou a omissão legislativa quanto à obrigação de notificar o titular dos dados quando as autoridades de investigação criminal acessarem essas informações, desde que a notificação não represente risco efetivo à investigação ou à segurança de terceiros. A ausência de notificação foi considerada violadora dos direitos de informação e tutela jurisdicional efetiva ao indivíduo, exigindo reforma normativa que assegure maior transparência e controle sobre o uso de dados pessoais no âmbito penal. A redação do Acórdão n.º 268/2022 foi assim formulada:

> Pelos fundamentos expostos, o Tribunal Constitucional decide:
>
> a) Declarar a inconstitucionalidade, com força obrigatória geral, da norma constante do artigo 4.º da Lei n.º 32/2008, de 17 de julho, conjugada com o artigo 6.º da mesma lei, por violação do disposto nos números 1 e 4 do artigo 35.º e do n.º 1 do artigo 26.º, em conjugação com o n.º 2 do artigo n.º 18.º, todos da Constituição;
>
> b) Declarar a inconstitucionalidade, com força obrigatória geral, da norma do artigo 9.º da Lei n.º 32/2008, de 17 de julho, relativa à transmissão de dados armazenados às autoridades competentes para investigação, deteção e repressão de crimes graves, na parte em que não prevê uma notificação ao visado de que os dados conservados foram acedidos pelas autoridades de investigação criminal, a partir do momento em que tal comunicação não seja suscetível de comprometer as investigações nem a vida ou integridade física de terceiros, por violação do disposto no n.º 1 do artigo 35.º e do n.º 1 do artigo 20.º, em conjugação com o n.º 2 do artigo 18.º, todos da Constituição..

Em outro caso igualmente relevante, o Tribunal Constitucional, por meio do Acórdão n.º 800/2023, que analisava o Decreto n.º 91/XV que já propunha alterações à Lei n.º 32/2008, pronunciou-se pela inconstitucionalidade da norma constante no artigo 2º do Decreto n.º 91/XV, na parte que alterava o artigo 4º da Lei n.º 32/2008, conjugado com o artigo 6º da mesma lei, quanto aos dados de tráfego e de localização. A Corte entendeu que a conservação

[240] ZUBOFF, Shoshana**. Big Other: Surveillance Capitalism and the Prospects of an Information Civilization**. Journal of Information Technology, v. 30, p. 75–89, 2015.

generalizada e diferenciada desses dados, mesmo por períodos reduzidos, violava os direitos fundamentais à autodeterminação informativa e à reserva da vida privada.

Como decorrência dessa decisão, foi promulgada a Lei n.º 18/2024, de 5 de fevereiro, que reformulou o regime de conservação e acesso a metadados da Lei n.º 32/2008[241], estabelecendo, entre outras medidas, que a conservação de dados de tráfego e localização só pode ocorrer mediante autorização judicial prévia, a ser exarada no prazo de 72 horas, fundamentada na necessidade exclusiva de investigação, deteção e repressão de crimes graves, bem como que essa autorização deve ser concedida por uma formação das secções criminais do Supremo Tribunal de Justiça.

A nova disciplina introduzida pela Lei n.º 18/2024 harmoniza o ordenamento português com os parâmetros definidos no Direito da União Europeia, em especial o Regime Geral de Proteção de Dados (Regulamento (EU) 2016/679), que estabelece normas gerais sobre o tratamento de dados pessoais, bem como com a Diretiva (EU) 2016/680, a qual trata especificamente da proteção de dados no contexto da investigação e repressão criminal. Essa última diretiva foi incorporada ao ordenamento jurídico português por meio da Lei n.º 59/2019,

[241] "Artigo 6.º Período e regras de conservação
1 - Para efeitos da finalidade prevista no n.º 1 do artigo 3.º, as entidades referidas no n.º 1 do artigo 4.º devem conservar, pelo período de um ano a contar da data da conclusão da comunicação, os seguintes dados:
a) Os dados relativos à identificação civil dos assinantes ou utilizadores de serviços de comunicações publicamente disponíveis ou de uma rede pública de comunicações;
b) Os demais dados de base;
c) Os endereços de protocolo IP atribuídos à fonte de uma ligação.
2 - Os dados de tráfego e de localização apenas podem ser objeto de conservação mediante autorização judicial fundada na sua necessidade para a finalidade prevista no n.º 1 do artigo 3.º, sem prejuízo daqueles conservados pelas entidades referidas no n.º 1 do artigo 4.º nos termos definidos contratualmente com o cliente para efeitos emergentes das respetivas relações jurídicas comerciais ou por força de disposição legal especial.
3 - O pedido de autorização judicial para conservação de dados de tráfego e de localização tem caráter urgente e deve ser decidido no prazo máximo de 72 horas.
4 - De forma a salvaguardar a utilidade do pedido de autorização judicial para conservação de dados de tráfego e de localização, o Ministério Público comunica de imediato às entidades referidas no n.º 1 do artigo 4.º a submissão do pedido, não podendo os dados ser objeto de eliminação até à decisão final sobre a respetiva conservação.
5 - A fixação e a prorrogação do prazo de conservação de dados de tráfego e de localização referida nos números anteriores devem limitar-se ao estritamente necessário para a prossecução da finalidade prevista no n.º 1 do artigo 3.º, devendo cessar logo que se confirme a desnecessidade da sua conservação.
6 - As entidades referidas no n.º 1 do artigo 4.º não podem aceder aos dados aí elencados salvo nos casos previstos na lei ou definidos contratualmente com o cliente para efeitos emergentes das respetivas relações jurídicas comerciais.
7 - A autorização judicial a que se referem os n.os 2 e 3 compete a uma formação das secções criminais do Supremo Tribunal de Justiça, constituída pelos presidentes das secções e por um juiz designado pelo Conselho Superior da Magistratura, de entre os mais antigos destas secções. PORTUGAL. Lei n.º 32/2008, de 17 de julho. Regula a conservação e a transmissão dos dados de tráfego e de localização relativos a pessoas singulares e coletivas, bem como os dados relacionados com os assinantes ou utilizadores processados e armazenados por prestadores de serviços de comunicações eletrónicas acessíveis ao público ou de uma rede pública de comunicações." Diário da República, 1.ª série, n.º 136, 17 jul. 2008. Disponível em: https://diariodarepublica.pt/dr/detalhe/lei/32-2008-456812. Acesso em: 31 mai. 2025

a qual regulamenta o tratamento de dados por autoridades policiais, judiciais e de investigação criminal.

Não obstante o aparente conflito de normas, a Lei n.º 59/2019 permanece como marco normativo geral, tendo as disposições da Lei n.º 18/2024 como norma especial, no que tange ao tratamento de metadados oriundos de comunicações eletrônicas. Ao modificar a redação da Lei n.º 32/2008, a Lei n.º 18/2024 conferiu densidade normativa ao princípio da legalidade no âmbito da produção probatória, ao alinhar-se às exigências do artigo 125º do Código de Processo Penal português, que consagra a legalidade da prova como condição de validade no processo penal, como alerta Maria Beatriz Seabra de Brito[242] (2017, p. 11). Essa conformidade traduz a observância do princípio da reserva legal, especialmente quando se trata da limitação de direitos fundamentais, cuja exigência, de modo análogo, também se impõe no ordenamento jurídico brasileiro.

Em termos práticos, a obtenção de dados de geolocalização em Portugal está amparada por um conjunto normativo que assegura a compatibilização entre as necessidades da investigação criminal e a proteção dos direitos fundamentais. A Lei n.º 59/2019, que incorpora a Diretiva (EU) 2016/680, disciplina o tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais, destacando-se nesse contexto o seu artigo 19, que regula os direitos do titular de dados no âmbito de processos penais.

Complementarmente, a Lei n.º 18/2024, que alterou a Lei n.º 32/2008, estabelece o regime aplicável à conservação e ao acesso a metadados relacionados a comunicações eletrônicas, incluindo dados de tráfego e de localização, bem como endereços IP atribuídos a dispositivos de origem. Esse regime aplica-se aos dados gerados no âmbito das redes públicas de comunicações ou que sejam publicamente acessíveis. Ademais, nos casos em que a medida investigativa envolva o acesso aos sistemas informativos ou telemáticos, deve-se observar o procedimento compatível previsto na Lei n.º 109/2009 (Lei do Cibercrime), a qual regula os meios de obtenção e preservação de prova digital[243].

Nos termos da Lei n.º 18/2024, o pedido de acesso a esses dados deve ser formulado pelo Ministério Público e submetido à apreciação de um juízo competente, que deverá avaliar

---

[242] MARIA BEATRIZ SEABRA DE BRITO. **Novas tecnologias e legalidade da prova em processo penal: natureza e enquadramento do GPS como método de obtenção de prova.**, Mestre, Universiadade Nova de Lisboa, Lisboa, 2017, p. 11.

[243] ROCHA, Maria João de Almeida. **A interseção entre a proteção de dados pessoais e a investigação criminal: contributo para uma análise jurídica crítica do regime aplicável ao tratamento de dados pessoais para fins de aplicação da lei**, Dissertação de Mestrado, Faculdade de Direito, Universidade de Lisboa, Lisboa, 2023.

sua pertinência no contexto da investigação de crimes graves. A autorização judicial dependerá da existência de indícios concretos, da demonstração da necessidade da medida, bem como a inexistência de meios intrusivos para obtenção da prova, em consonância com os princípios da legalidade, proporcionalidade e subsidiariedade.

4.3.3 Itália

Em substituição ao Código de Processo Penal Italiano de 1930, o C*odice di Procedura Penale*, conhecido como Código Vassalli, foi aprovado por meio do Decreto n.º 447, de setembro de 1988, do Presidente da República[244]. A promulgação desse novo diploma normativo refletiu o progressivo reconhecimento da importância de disciplinar o processo penal a partir da proteção e afirmação dos direitos fundamentais do indivíduo. Sua adoção marcou uma guinada significativa na tradição processual italiana, promovendo a transição de um sistema de matriz inquisitorial para um modelo acusatório. Em seus fundamentos, destacam-se na atribuição das funções investigativas do Ministério Público, bem como a atuação de um juiz imparcial competente para autorizar, mediante requisitos legais, medidas que afetem direitos individuais[245].

Contudo, a transição do sistema inquisitivo para o modelo acusatório, promovida pela reforma processual penal italiana de 1988, enfrentou resistências especialmente no âmbito da magistratura, cuja atuação passou a ser delimitada pela separação de funções e pelo fortalecimento das garantias do contraditório. Essa resistência decorreu em parte da percepção de perda do protagonismo no controle da instrução penal, uma verdadeira abstinência de poder. Em consequência, decisões de inconstitucionalidade incidentes sobre os dispositivos centrais do novo código enfraqueceram a coerência sistêmica da reforma, por introduzirem, sob o pretexto de controle de constitucionalidade, elementos de política criminal que destoavam das premissas estruturantes do modelo acusatório[246].

Em resposta a essas tensões institucionais e à necessidade de harmonização com reformas também em curso no processo civil italiano, promoveu-se a alteração do artigo 111[247]

---

[244] ITÁLIA. *Codice di Procedura Penale*. Gazzetta Ufficiale. Disponível em: https://www.gazzettaufficiale.it/sommario/codici/codiceProceduraPenale. Acesso em: 02 jun. 2025

[245] SPANGHER, Giorgio. **Il processo penale dopo trent'anni. Sovrastrutture retrospettive**. Archivio Penale, 2020. Disponível em: <https://archiviopenale.it/File/DownloadArticolo?codice=9153b659-2351-4337-92ed-72f65aa42fa4&idarticolo=21714>. Acesso em: 2 jun. 2025.

[246] *Ibid*.

[247] "Art. 111 - A jurisdição atua-se mediante o justo processo regulado pela lei.
Cada processo desenvolve-se no contraditório entre as partes, em condições de igualdade perante juiz terceiro e imparcial. A lei assegura a razoável duração.

da Constituição da República Italiana, conferindo densidade constitucional ao princípio do devido processo legal e ao contraditório na produção da prova[248]. A partir de então, a proteção dos direitos fundamentais passou a ocupar papel central na reconstrução da dogmática processual penal, favorecendo a abertura interpretativa para novos paradigmas de produção probatória, com reflexos diretos sobre estrutura normativa e axiológicas do processo penal[249].

Assim, o Código Vassalli disciplinava, nos artigos 266 a 271 as interceptações de comunicações, estabelecendo que o conteúdo devassado deveria ser transcrito apenas na parte relevante para a investigação ou para o exercício do direito de defesa do investigado. O referido diploma, de outro modo, não tratava de forma específica a coleta de dados relativos às chamadas telefônicas, como data horário e duração, os quais, embora não se confundissem com o conteúdo da comunicação, também implicavam ingerência na esfera da privacidade. Desta forma, a *Sentenza* n.º 81/1993[250] da Corte Constitucional italiana reconheceu a relevância da proteção dos dados pessoais no contexto penal, ao afirmar que, ainda que os dados não estivessem abrangidos nas garantias procedimentais previstas nos artigos 266 e seguintes do Código, por não se tratar de interceptação *strictu sensu*, configuravam-se como informações sensíveis. Logo, com fundamento no artigo 15 da Constituição italiana[251], que assegura a inviabilidade da liberdade e do sigilo das comunicações, a Corte concluiu que a obtenção desses

---

No processo penal a lei assegura que a pessoa acusada de um crime seja, no mais breve tempo possível, informada reservadamente sobre a natureza e os motivos da acusação dirigida ao seu cargo, disponha de tempo e das condições necessárias para preparar a sua defesa; tenha faculdade, perante o juiz, de interrogar ou de fazer interrogar as pessoas que fazem declarações sobre ele, obter a convocação e o interrogatório de pessoas para sua defesa nas mesmas condições da acusação e adquirir qualquer outro meio de prova a seu favor; seja assistido por um intérprete, se não compreender ou não falar a língua utilizada num processo.
O processo penal é regulado pelo princípio do contraditório na formação da prova. A culpabilidade do arguido não pode ser provada com base em declarações dadas por quem, por livre escolha sempre se subtraiu voluntariamente ao interrogatório por parte do arguido ou do seu defensor.
A lei regula os casos em que a formação da prova não tem lugar em contraditório por consenso do arguido ou por impossibilidade comprovada de natureza objetiva ou por efeito de conduta ilícita provada. (...)".
ITÁLIA. Constituição (1947). **Constituição da República Italiana**. Tradução oficial para o português. Roma: Senado da República. Disponível em: https://www.senato.it/sites/default/files/media-documents/COST_PORTOGHESE.pdf. Acesso em: 2 jun. 2025

[248] SCHENK, Leonardo Faria. **Breve relato histórico das reformas processuais na Itália: um problema constante: a lentidão dos processos cíveis.** Revista Eletrônica de Direito Processual. v. 2, 2008.

[249] SPANGHER, Giorgio. **Il processo penale dopo trent'anni. Sovrastrutture retrospettive**. Archivio Penale, 2020. Disponível em: <https://archiviopenale.it/File/DownloadArticolo?codice=9153b659-2351-4337-92ed-72f65aa42fa4&idarticolo=21714>. Acesso em: 2 jun. 2025.

[250] ITALIA. Corte Costituzionale Italiana. Sentenza n. 81/1993, pronunciada em 26 de fevereiro de 1993 e publicada em 11 de março de 1993. Disponível em: https://www.cortecostituzionale.it/actionSchedaPronuncia.do?param_ecli=ECLI%3AIT%3ACOST%3A1993%3A81. Acesso em: 3 jun. 2025.

[251] "Art. 15 -A liberdade e o segredo da correspondência e de qualquer outra forma de comunicação são invioláveis. A sua limitação pode ocorrer somente por determinação da autoridade judiciária, sendo mantidas as garantias estabelecidas pela lei."
ITÁLIA. Constituição (1947). **Constituição da República Italiana**. Tradução oficial para o português. Roma: Senado da República. Disponível em: https://www.senato.it/sites/default/files/media-documents/COST_PORTOGHESE.pdf. Acesso em: 3 jun. 2025

dados exigiria a observância da reserva de jurisdição, devendo a sua requisição ser submetida à apreciação da autoridade judiciária competente.

Posteriormente, foi instituído o *Codice in materia di protezione dei dati personali,* por meio do Decreto Legislativo n.º 196, de 30 de junho de 2003, o qual representa um marco cerca da tutela dos dados pessoais na Itália. Conhecido como "Código da Privacidade", esse diploma passou por significantes modificações em face do Decreto Legislativo n.º 101, de 10 de agosto de 2018, cujo objeto era a integração da legislação daquele país com as disposições introduzidas pelo Regulamento Geral sobre a Proteção de Dados da União Europeia. Essas alterações introduzidas destinavam-se, além de maiores medidas assecuratórias dos direitos dos titulares de dados, impunha previsões mais exaustivas acerca do tratamento de dados e sua responsabilização (*accountability*)[252].

No tocante especificamente a geolocalização, observa-se que o ordenamento jurídico italiano não dispõe de uma regulamentação autônoma específica para esse meio investigativo no processo penal, mas disciplina sua utilização a partir da interpretação conjugada do artigo 15 da Constituição, do *Codice di Procedura Penale* e do *Codice in matéria de protezione dei dati personali,* especialmente após a reforma promovida pelo Decreto Legislativo n.º 101, de agosto de 2018. Cita-se, em particular, o artigo 132 do Código da Privacidade que estabelece que os dados de tráfego de localização somente podem ser conservados e acessados para fins de investigação criminal ou segurança pública mediante autorização judicial, bem como por período não superior ao estritamente necessário ao alcance das finalidades almejadas.

A jurisprudência italiana tem tradicionalmente reconhecido que a geolocalização, tanto retrospectiva quanto em tempo real, constitui medida altamente intrusiva e, por isso, está sujeito ao princípio da reserva de jurisdição. Contudo, decisões recentes da Corte de Justiça da União Europeia, como o caso HK (C-746/18)[253], têm questionado a adequação do modelo italiano, especialmente quanto ao disposto no artigo 132, 3-*bis* do Código da Privacidade que prevê a autorização de retenção de dados pelo Ministério Público em casos de urgência, na medida em que haveria a necessidade de independência e imparcialidade do *Parquet*. Esse aparente conflito tem levado a um debate acadêmico acerca da necessidade de reforma do sistema de produção

[252] CAIANIELLO, Michele. **Increasing Discretionary Prosecutor's Powers: The Pivotal Role of the Italian Prosecutor in the Pretrial Investigation Phase**, *in*: OXFORD HANDBOOKS EDITORIAL BOARD (Org.), Oxford Handbook Topics in Criminology and Criminal Justice, [s.l.]: Oxford University Press, 2012.
[253] UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia. Processo C-746/18 – H. K. contra Prokuratuur. Acórdão da Grande Secção de 2 mar. 2021. Disponível em: https://curia.europa.eu/juris/document/document.jsf?docid=222421&doclang=PT. Acesso em: 3 jun. 2025.

de prova nesse ponto, inclusive em torno de eventual afastamento da aplicação do artigo 132 do Código da Privacidade à luz dos entendimentos das Cortes da União Europeia[254].

Como procedimento, a sua utilização, em regra geral, demanda requerimento do Ministério Público e autorização judicial devidamente fundamentada, conforme os princípios da necessidade, proporcionalidade e adequação, previstos tanto na Constituição quanto no próprio artigo 5º da GDPR[255]. Não obstante, permanece em aberto a questão sobre a validade dessas autorizações quando emanadas pelo próprio Ministério Público.

No mais, dessa forma, o modelo italiano adota a postura garantista, assegurando que o avanço tecnológico não comprometa os direitos fundamentais à privacidade, a autodeterminação informativa e ao devido processo legal. Apenas com intuito ilustrativo, transcreve se o teor do artigo 132 do Código da Privacidade:

> Arte. 132
> (Retenção de dados de tráfego para outras finalidades).
> 1. Sem prejuízo do disposto no artigo 123.º, n.º 2, os dados relativos ao tráfego telefónico serão conservados pelo fornecedor durante vinte e quatro meses, a contar da data da comunicação, para efeitos de apuramento e repressão de crimes, enquanto, para os mesmos efeitos, os dados relativos ao tráfego telemático, excluindo em qualquer caso o conteúdo das comunicações, serão conservados pelo fornecedor durante doze meses, a contar da data da comunicação.
> 1-bis. Os dados relativos a chamadas não atendidas, tratados temporariamente por prestadores de serviços de comunicações eletrónicas acessíveis ao público ou por uma rede pública de comunicações, são armazenados durante trinta dias. (15) (17) (33)
> 2. PARÁGRAFO REVOGADO PELO DECRETO LEGISLATIVO Nº 109, DE 30 DE MAIO DE 2008.
> 3. Dentro do prazo de conservação imposto por lei, se houver indícios suficientes de crimes para os quais a lei estabeleça pena de prisão perpétua ou prisão não inferior a três anos, determinada nos termos do artigo 4.º do Código de Processo Penal , e de crimes de ameaça e perseguição ou perturbação de pessoas por meio de telefone, quando a ameaça, perseguição e perturbação forem graves, quando relevantes para a apuração dos factos, os dados são adquiridos mediante autorização emitida pelo juiz com despacho fundamentado, a requerimento do Ministério Público ou a requerimento do advogado do arguido, do investigado, do lesado e de outros particulares.
> 3-bis. Quando houver motivos de urgência e houver motivos para crer que o atraso possa causar sérios prejuízos à investigação, o Ministério Público ordena a obtenção dos dados por meio de despacho fundamentado, que é comunicado imediatamente, e em qualquer caso no prazo máximo de quarenta e oito horas, ao juiz competente para emitir a autorização na forma ordinária. O juiz, dentro das quarenta e oito horas seguintes, decide sobre a validação por meio de despacho fundamentado. PERÍODO REVOGADO PELO DECRETO LEGISLATIVO Nº 132, DE 30 DE SETEMBRO DE 2021, CONVERTIDO COM ALTERAÇÕES PELA LEI Nº 178, DE 23 DE NOVEMBRO DE 2021.

---

[254] LEO, Guglielmo. **Le indagini sulle comunicazioni e sugli spostamenti delle persone: prime riflessioni riguardo alla recente giurisprudenza europea su geolocalizzazione e tabulati telefonici.** Sistema Penale, p. 19, 2021.

[255] UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados – GDPR), art. 5.º. Disponível em: https://gdpr-info.eu/art-5-gdpr/. Acesso em: 3 jun. 2025.

> 3-ter. No que diz respeito aos dados armazenados para as finalidades indicadas no parágrafo 1, os direitos previstos nos artigos 12 a 22 do Regulamento podem ser exercidos na forma prevista no artigo 2-undecies, parágrafo 3, terceiro, quarto e quinto períodos.
> 3º trimestre. Os dados obtidos em violação ao disposto nos parágrafos 3 e 3-bis não poderão ser utilizados.
> 4-ter. O Ministro do Interior ou, por sua delegação, os chefes dos escritórios centrais especializados em TI ou telemática da Polícia Estadual, os Carabinieri e a Guardia di Finanza, bem como as outras entidades indicadas no parágrafo 1 do Artigo 226 das disposições de execução, coordenação e transição do Código de Processo Penal , nos termos do Decreto Legislativo n.º 271 de 28 de julho de 1989 , podem determinar, também em relação a quaisquer solicitações feitas por autoridades investigativas estrangeiras, que os fornecedores e operadores de serviços de TI ou telemáticos retenham e protejam, de acordo com os métodos indicados e por um período não superior a noventa dias, os dados relativos ao tráfego telemático, excluindo em qualquer caso o conteúdo das comunicações, para fins de realização das investigações preventivas previstas no supracitado Artigo 226 das disposições nos termos do Decreto Legislativo n.º 271 de 1989 , ou para fins de apuração e repressão de crimes específicos. A disposição, que pode ser prorrogada por motivos justificados por um período total não superior a seis meses, pode prever métodos específicos de armazenamento de dados e a possível indisponibilidade dos próprios dados por fornecedores e operadores de serviços de TI ou telemáticos ou por terceiros.
> 4º. O prestador ou operador de serviços informáticos ou telemáticos a quem for dirigida a ordem referida no parágrafo 4º deve cumprir sem demora, fornecendo imediatamente à autoridade requerente garantias de cumprimento. O prestador ou operador de serviços informáticos ou telemáticos é obrigado a manter sigilo sobre a ordem recebida e as atividades subsequentemente realizadas durante o período indicado pela autoridade. Em caso de violação da obrigação, aplicar-se-á o disposto no artigo 326.º do Código Penal, salvo se o facto constituir crime mais grave.
> 4-quinquies. As medidas adotadas nos termos do parágrafo 4-ter serão comunicadas por escrito, sem demora e, em qualquer caso, no prazo de quarenta e oito horas a contar da notificação ao destinatário, ao Ministério Público do local da execução, que, se as condições estiverem preenchidas, as validará.
> Em caso de não validação, as medidas adotadas perderão a sua eficácia.
> 5. O tratamento de dados para as finalidades referidas no parágrafo 1 é realizado no cumprimento das medidas e precauções de garantia do interessado prescritas pelo Fiador.((com uma disposição geral)), visando garantir que os dados armazenados tenham os mesmos requisitos de qualidade, segurança e proteção dos dados disponibilizados online, bem como indicar as modalidades técnicas de destruição periódica dos dados, após decorridos os prazos referidos no n.º 1.

4.4. DISCIPLINA NORMATIVA PARA O USO DE GEOLOCALIZAÇÃO NO BRASIL

Caso, observados critérios rigorosos da necessidade, adequação e proporcionalidade, a geolocalização poderia ser admitida como meio legítimo de obtenção de prova, sobretudo quando resultar em encontro fortuito de elementos probatórios relacionados ao objeto da investigação. Não obstante, o problema reside no fato de que não há regulamentação legal específica que defina esses requisitos objetivos e subjetivos para a decretação dessa medida. Essa análise por vezes é feita no teste de adequação e necessidade da medida, com base em analogia aos requisitos da Lei de Interceptação Telefônica (Lei n.º 9.296/96), destacando-se a inexistência de outros meios disponíveis para obtenção da prova e gravidade do crime

investigado, o que acaba por inserir sua utilização em um campo indefinido e, por esta razão, com potencial risco para a segurança jurídica e às garantias fundamentais das pessoas abrangidas no perímetro delimitado.

Observa-se, ainda, a existência de decisões judiciais que se fundamentam no artigo 22 do Marco Civil da Internet (Lei n.° 12.965/2014) para autorizar medidas de geolocalização. Todavia, essas decisões carecem de respaldo jurídico adequado, uma vez que o referido dispositivo legal se limita a autorizar, mediante ordem judicial, o fornecimento de dados cadastrais, registros de conexão e de acesso a aplicações de internet, categorias que não abrangem, de forma explícita ou implícita, dados de localização geográfica. Como exposto no Capítulo 2 deste trabalho, o endereço IP tem por finalidade a identificação do terminal utilizado para a conexão à rede, servindo como elemento técnico vinculado à autoria de condutas em ambiente virtual. Sua precisão, no entanto, é limitada e, na prática, pouco difere das informações já constantes dos dados cadastrais, não sendo apto, por si só, a revelar a localização física do usuário. Logo, a utilização do artigo 22 como fundamento para autorizar a obtenção de dados de localização poderia configurar interpretação extensiva prejudicial a direito fundamental, o que contraria o princípio da legalidade estrita.

4.4.1 Artigo 13-B do Código de Processo Penal Brasileiro

Como mencionado na introdução deste trabalho, a previsão normativa atualmente existente quanto ao uso de dados de geolocalização é pontual e deveria possuir alcance bastante restrito, destinada exclusivamente ao auxílio na apuração de crimes relacionados ao tráfico de pessoas. Consiste em exceção inserida no ordenamento por meio do artigo 13-B o Código de Processo Penal, que assim dispõe:

> “13-B Se necessário à prevenção e à repressão dos crimes relacionados ao tráfico de pessoas, o membro do Ministério Público ou o delegado de polícia poderão requisitar, mediante autorização judicial, às empresas prestadoras de serviço de telecomunicações e/ou telemática que disponibilizem imediatamente os meios técnicos adequados – como sinais, informações e outros – que permitam a localização da vítima ou dos suspeitos do delito em curso.

Cabe destacar que essa alteração promovida no Código de Processo Penal por meio da Lei n.º 13.344, de 6 de janeiro de 2016, tem origem no Projeto de Lei do Senado Federal (PLS) n.º 479/2012, de autoria da Comissão Parlamentar de Inquérito do Tráfico Nacional e Internacional de Pessoas no Brasil, cujo objetivo era fortalecer mecanismos de prevenção e repressão ao tráfico de pessoas, tanto no âmbito interno quanto no plano internacional.

A atuação da referida Comissão foi bastante influenciada pelos princípios abraçados pela Convenção das Nações Unidas contra o Crime Organizado Transnacional, conhecida como Convenção de Palermo, especialmente no que se refere à cooperação entre os Estados na repressão a infrações penais transnacionais.

Consoante o dispositivo no artigo 27[256] da Convenção, os Estados signatários assumiriam o compromisso de atuar de forma coordenada para garantir a maior efetividade às ações de repressão às infrações nela previstas. Essa atuação conjunta pressupunha a criação ou aprimoramento de mecanismos de comunicação entre autoridades competentes, de modo a viabilizar o intercâmbio rápido e seguro de informações relevantes. Além disso, a norma estimularia a cooperação interestatal na condução de investigações voltadas à identificação e localização de suspeitos, bem como de outros envolvidos nas condutas ilícitas do crime organizado transnacional.

Não obstante a tramitação regular e a aprovação do PLS n.º 479/2012, no Senado Federal, é importante destacar que a criação e inserção do atual artigo13-B no Código de Processo Penal não estava prevista no texto original do referido projeto. Essa proposta possuía escopo temático ao tráfico nacional e internacional de pessoas e não incluía qualquer previsão específica quanto ao acesso, por autoridades investigativas a dados de geolocalização ou informações similares.

Contudo, uma alteração relevante no conteúdo da proposição ocorreu após o envio à Câmara dos Deputados, que na condição de Casa revisora, apensou ao PLS n.º 479/2012 o Projeto de Lei n.º 6.934, de 2013, de sua iniciativa. A questão dessa junção de matérias está no fato de que o PL n.º 6.934/2013 foi apensado antes mesmo de ser apreciado por qualquer comissão temática da Câmara, o que impediu uma análise aprofundada independente de seu

---

[256] "Artigo 27 - Cooperação entre as autoridades competentes para a aplicação da lei1. Os Estados Partes cooperarão estreitamente, em conformidade com os seus respectivos ordenamentos jurídicos e administrativos, a fim de reforçar a eficácia das medidas de controle do cumprimento da lei destinadas a combater as infrações previstas na presente Convenção. Especificamente, cada Estado Parte adotará medidas eficazes para:
a) Reforçar ou, se necessário, criar canais de comunicação entre as suas autoridades, organismos e serviços competentes, para facilitar a rápida e segura troca de informações relativas a todos os aspectos das infrações previstas na presente Convenção, incluindo, se os Estados Partes envolvidos o considerarem apropriado, ligações com outras atividades criminosas;
b) Cooperar com outros Estados Partes, quando se trate de infrações previstas na presente Convenção, na condução de investigações relativas aos seguintes aspectos:
i) Identidade, localização e atividades de pessoas suspeitas de implicação nas referidas infrações, bem como localização de outras pessoas envolvidas;"
BRASIL. Decreto nº 5.015, de 12 de março de 2004. Promulga a Convenção das Nações Unidas contra o Crime Organizado Transnacional, adotada pela Assembleia-Geral das Nações Unidas em 15 de novembro de 2000. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/decreto/d5015.htm. Acesso: 21 mai. 2025.

mérito. Esse projeto é que introduzia a disciplina normativa hoje consagrada no artigo 13-B do Código de Processo Penal, autorizando, mediante decisão judicial, a requisição de sinais de telecomunicações para a localização de vítimas e suspeitos em casos de tráfico de pessoas. A justificativa apresentada para a inclusão desse dispositivo limitava-se, de forma bastante sucinta, a afirmar:

> Reforçaram-se as cautelas que a adoção internacional de crianças brasileiras deve se cercar; foram dados mais instrumentos aos membros do Ministério Público e às autoridades policiais e judiciárias para prevenir e impedir o cometimento de tais delitos, sem descurar das responsabilidades que devem ter tais agentes públicos quando do uso desses instrumentos legais.

A partir da aglutinação da matéria, originou-se um substitutivo, posteriormente encaminhado à análise de uma Comissão Especial, criada especificamente para apreciar o texto consolidado. O parecer final dessa Comissão, publicado em 11 de dezembro de 2014, não trouxe fundamentação jurídica, constitucional ou técnica que justificasse adequadamente a introdução de uma medida tão sensível invasiva como acesso judicial a dados de geolocalização. O parecer se restringiu ao mencionar que: "*à Polícia e ao Ministério Público é assegurado o acesso a dados da internet necessários às suas investigações, o que agilizará o inquérito e garantirá maior efetividade em suas ações de combate ao tráfico de pessoas*"[257].

Considerando o teor dessa manifestação, com visão eminentemente utilitarista, ignorou-se o necessário debate sobre os limites constitucionais à restrição de direitos fundamentais, como à privacidade e à autodeterminação informativa, e revela a fragilidade do processo legislativo que deu origem à norma, ou debate não se quedou em oportunidade específica ou não foi adequadamente documentado. A ausência de justificativas ancoradas nos princípios da proporcionalidade, legalidade estrita e proteção do núcleo essencial dos direitos fundamentais reflete a carência de fundamentação que acompanha a positivação do artigo 13-B do CPP.

O resultado do aparente raso debate legislativo culminou no ajuizamento da ADI 5.642, cujo objeto era justamente a análise acerca da prescindibilidade de autorização judicial para o fornecimento de informações ao Ministério Público e delegado de polícia de dados compreendidos como informações concernentes à qualificação pessoal, filiação e endereço (dados reputados como cadastrais), além do alcance das autorizações judiciais que envolvam o fornecimento de informações acerca dos meios técnicos adequados – como sinais, informações e outros – que permitam a localização da vítima ou dos suspeitos dos crimes de tráfico de pessoas que estejam em curso.

[257] https://imagem.camara.gov.br/Imagem/d/pdf/DCD00201412120019200000.PDF#page=615

Nesta ação direta de inconstitucionalidade, o Plenário Virtual do Supremo Tribunal Federal se debruçou sobre o tema e caminhou no sentido da prevalência do interesse público da apuração e investigação do delito sobre o direito à privacidade. Fixou-se o entendimento de que o fornecimento de dados cadastrais não seria considerado como hipótese de interceptação de voz ou telemática, não se exigindo, portanto, as mesmas garantias constitucionais. No entanto, o ponto relevante nesta ADI está inserido no teor do voto do Ministro Relator Edson Fachin, que ao final concluiu:

> Continuam sendo passíveis de requisição sem controle judicial prévio, mas sempre sujeito ao controle judicial posterior, a localização de terminal ou IMEI de cidadão em tempo real por meio de ERB por um período determinado e desde que necessário para os fins de reprimir os crimes contra a liberdade pessoal descritos no art. 13-A do Código Penal;

Não se olvida a importância de dotar as investigações criminais de maior quantidade possível de instrumentos constitucionais para seu aperfeiçoamento, principalmente considerando a gravidade dos tipos penais abrangidos pelos artigos 13-A e 13-B do Código de Processo Penal. Contudo, embora formalmente citada nas inúmeras decisões judiciais, a relevância do tratamento de dados do indivíduo e sua aderência ao direito da privacidade, seu conteúdo substancial e seu impacto no exercício da individualidade e participação social tem se colocado inadvertidamente em segundo plano.

A mera cogitação do fornecimento de informações de localização do terminal ou IMEI, isto é, a sua geolocalização, sem sequer a autorização judicial prévia, como se faz crer o Ministro Relator da ADI 5.642, dando efetividade aos artigos do Código de Processo Penal, aparenta-se um tanto quanto a caracterização de um Estado Policial, em seu sentido conotativo negativo que pressupõe um Estado dotado de atividades policiais de cunho arbitrário, em total desrespeito aos direitos, liberdade e dignidade humana[258].

Destaca-se, ainda, a relevante a questão da temporalidade no julgamento da ADI 5.642. Embora a decisão tenha sido proferida em 2024, o julgamento foi iniciado antes da promulgação da Emenda Constitucional n.º 115/2022, que incluiu expressamente a proteção de dados pessoais no rol dos direitos e garantias fundamentais, conferindo lhe natureza autônoma e vinculada à cláusula do artigo 5º da Constituição. Não obstante, o novo enunciado normativo constitucional foi mencionado de forma marginal no debate, prevalecendo, entre a maioria dos Ministros do STF, o fundamento tradicional do artigo 5º, inciso XII, que garante inviolabilidade

[258] CHAPMAN, Brian, **Police State**, London: Macmillan Education UK, 1971.

das comunicações telefônicas e de dados. Com essas premissas, o STF reafirmou a jurisprudência já consolidada segundo a qual a proteção conferida pelo inciso XII incide sobre a comunicação de dados, ou seja, sobre conteúdo comunicacional e não se estende aos chamados dados estáticos, cadastrais ou objetivos, entendidos como informações meramente identificadoras, mesmo que armazenadas digitalmente. Essa distinção foi reforçada com base em precedentes anteriores da Corte, especialmente em remissão ao voto do Ministro Sepúlveda Pertence, no julgamento do RE 418.416, em que já se sustentavam que o alcance da reserva de jurisdição não se aplicaria aos dados formais ou de natureza meramente cadastral.

Embora o debate acerca da expressão "dados cadastrais" não tenha sido travado à luz da LGPD, a Corte estabeleceu que esses dados cadastrais não abrangeriam interceptações de comunicações de voz ou dados (telemática); dados de IP com data, hora e fuso; extratos de chamadas telefônicas e mensagens de texto (SMS/MMS); e serviço de agenda virtual, dados de e-mail ou registros de conexão à internet.

De fato, no acórdão da referida ADI, quanto ao artigo 13-A do CPP, o STF sedimentou o entendimento de que a requisição direta de dados meramente cadastrais, como o nome, endereço e filiação, por autoridades policiais ou membros do Ministério Público não exige prévia autorização judicial, por não estarem submetidos à reserva de jurisdição. Reiterou-se que a medida visa exclusivamente permitir a identificação de vítimas e suspeitos de crimes que atentam contra a liberdade individual e que outros normativos esparsos já previam essa possibilidade, especialmente no que tange ao Ministério Público.

Já quanto ao artigo 13-B do CPP, os debates foram mais percucientes. O ponto central da controvérsia reside na compatibilidade da medida com a cláusula de reserva de jurisdição e com os direitos fundamentais à intimidade e à proteção de dados. A Corte, por maioria, considerou constitucional o dispositivo, desde que submetida a uma interpretação restritiva que respeite os parâmetros do controle judicial e da legalidade estrita.

De forma mais específica, avançou-se na discussão sobre o alcance do §4º do artigo 13-B, que autoriza a requisição direta dos dados pelas autoridades investigativas, no caso de inércia judicial superior a 12 horas, com a exigência de comunicação imediata ao juízo competente. Não obstante manifestação relativamente diversa dos Ministros Gilmar Mendes e Rosa Weber, o fundamento principal que sustentou a admissibilidade dessa exceção foi a natureza dos crimes tratados pelo dispositivo e a situação de flagrância naquele lapso temporal. Essa excepcionalidade foi legitimada com base na premissa de que a finalidade do artigo é assegurar a resposta estatal imediata às situações de privação de liberdade, não se prestando a apuração de delitos de menor gravidade ou sem conexão com o resgate da vítima. Outrossim, os Ministros

do STF identificaram, na controvérsia, uma colisão entre os direitos à privacidade e à intimidade e o dever condicional de proteção à vida. A prevalência deste último, em hipóteses excepcionais de risco iminente, fundamentou a admissibilidade da medida de geolocalização, considerada legítima na medida em que visa resguardar bens jurídicos essenciais e insuscetíveis de renúncia.

Ademais, embora o *caput* do artigo 13-B mencione apenas o tráfico de pessoas, a maioria dos Ministros reconheceu que o dispositivo deve ser interpretado de forma sistemática com o artigo 13-A, abrangendo um rol de delitos que incluem sequestro, cárcere privado, trabalho escravo, extorsão mediante sequestro, entre outros. Essa compreensão ampliada está fulcrada na finalidade comum de ambos os dispositivos, qual seja, permitir a atuação estatal imediata em casos que envolvam restrição da liberdade da vítima.

Muito embora as discussões ocorridas o julgamento da referida ADI tenham abarcado, de certa monta, o cerne da discussão sobre o emprego da ferramenta de geolocalização, constata-se que algumas das premissas adotadas pela Corte demandam revisitação à luz da promulgação da Emenda Constitucional n.º 115/2022, exigindo-se uma compreensão mais robusta da autodeterminação informativa enquanto dimensão do direito da personalidade, em consonância com os princípios norteadores da Lei Geral de Proteção de Dados Pessoais. Há que se rememorar que o Estado Democrático de Direito é fundado na supremacia da lei e na contenção do Poder Estatal mediante normas previamente estabelecidas, isto é, seria incongruente admitir ausência de previsão legal específica que autorize o uso desse instrumento em outras hipóteses investigativas, além daquelas taxativamente previstas no ordenamento jurídico. É um sistema que adota o princípio da legalidade como cláusula estruturante, não sendo admissível a restrição de direitos fundamentais por meio de decisões interpretativas, ainda que elas sejam pertinentes a casos diversos.

A ausência de uma conceituação precisa dos dados pessoais, aliada à indefinição quanto a sua dimensão jurídica e projeção, bem como a insuficiência de resposta legislativa aos desafios decorrentes das inovações tecnológicas, têm levado as Cortes, no intuito de legitimar o uso do instrumento de geolocalização, a utilizar como fundamento legal o artigo 22 da Lei n.º 12.965/2014, aliado, por analogia, a alguns requisitos da Lei n.° 9.296/96, como a inexistência de outros meios disponíveis para obtenção da prova e gravidade do crime investigado. Entretanto, essa última lei é originalmente voltada à regulamentação da interceptação de comunicações, como forma de restrição a direito fundamental consagrado no artigo 5°, inciso XII, da Constituição Federal, o que demonstra uma inadequação teórica e normativa na aplicação por analogia desse regime à tutela de dados de localização, uma vez que o parágrafo

único da referida lei cinge o espectro material de incidência, destinando-a, apenas, "*à interceptação do fluxo de comunicações em sistemas de informática e telemática*".

Outrossim, a Lei n.° 9.296/96 estabelece requisitos rigorosos para sua autorização, conferindo à medida natureza excepcional, devendo ser empregada como última possibilidade instrumental para instrução do conjunto probatório, entendimento rigoroso que deveria ser seguido no emprego do artigo 22 do Marco Civil da Internet. A título exemplificativo, a admissibilidade do meio de obtenção de prova por interceptação telefônica é condicionada à existência de indícios razoáveis de autoria ou participação em infração penal punida com pena de reclusão, à impossibilidade de obtenção da prova por outros meios e à gravidade do delito. Além disso, a reserva de jurisdição é requisito imprescindível para o deferimento da medida.

4.4.2 Marco Civil da Internet e a sua previsão nos artigos 10 e 22

Embora uma análise exaustiva das disposições do Marco Civil da Internet não constitua o objeto central do presente trabalho, no item 3.5.3 do Capítulo 3 foram abordados os princípios que orientam essa legislação, na medida em que fornecem importantes balizas interpretativas para a compreensão das normas que regulam a requisição judicial de registros de conexão e de acesso a aplicações de internet. A referência a esses princípios revela-se particularmente relevante diante das interpretações que buscam conferir a esses registros eficácia jurídica suficientes para fundamentar medidas de geolocalização.

O ordenamento jurídico brasileiro impõe às empresas do setor de telecomunicações a obrigação de reter metadados de seus usuários por períodos determinados estabelecidos tanto em leis quanto em regulamentos infralegais. Essa obrigatoriedade tem origem em um conjunto normativo que inclui a Lei n.º 12.850/2013 (Lei das Organizações Criminosas), a Lei n.º 12.965/2014 (o Marco Civil da Internet) e diversas resoluções da Agência Nacional de Telecomunicações (ANATEL), como as Resoluções n.º 426/2005, 477/2007 e 738/2020[259]. A

[259] "Art. 65-J. A fim de assegurar a permanente fiscalização e o acompanhamento de obrigações legais e regulatórias, as prestadoras devem manter à disposição da Anatel os dados relativos à prestação do serviço, incluindo, conforme o caso e observada a regulamentação pertinente:
I - documentos de natureza fiscal, dados cadastrais dos assinantes e dados de bilhetagem e das ligações efetuadas e recebidas, bem como data, horário, duração e valor da chamada pelo prazo mínimo de 5 (cinco) anos, nos serviços que permitam a realização de tráfego telefônico; e,
II - registros de conexão à Internet pelo prazo mínimo de 1 (um) ano nos serviços que permitam a conexão à Internet.
Parágrafo único. Para fins do disposto neste artigo, considera-se registro de conexão à Internet o conjunto de informações referentes à data e hora de início e término de uma conexão à Internet, sua duração e o endereço IP utilizado pelo terminal, assim como as portas lógicas utilizadas quando do compartilhamento de IP público, para o envio e recebimento de pacotes de dados." AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES (Brasil). Resolução nº 738, de 21 de dezembro de 2020. Altera o Regulamento dos Serviços de Telecomunicações para

motivação principal para essa imposição decorre da pressão exercida, durante os respectivos processos legislativos, por autoridades investigativas e órgãos de segurança pública, os quais buscaram garantir o acesso a dados essenciais para a persecução penal, fortalecendo os mecanismos de investigação e combate ao crime[260].

Para que se possa avançar na análise jurídica acerca da retenção de dados de conexão e dos registros de acesso a aplicações de internet, mostra-se imprescindível recorrer às definições expressamente consignadas no Marco Civil da Internet. Essas definições representam uma forma de interpretação autêntica conferida pelo próprio legislador oferecendo parâmetros normativos objetivos que devem guiar a exegese e aplicação dos dispositivos subsequentes da norma. A precisão conceitual fornecida por esses preceitos legais é fundamental para delimitar a clareza, o alcance e os limites das obrigações de guarda de dados impostos à agentes privados. Justifica-se, portanto, a transcrição dos incisos pertinentes do artigo 5º da Lei n.º 12.965/2014, com vistas a proporcionar maior clareza à discussão e elucidar a abrangência dos contornos jurídicos das obrigações tratadas:

> Art. 5º Para os efeitos desta Lei, considera-se:
> (...)
> VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;
> VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet; e
> VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.

Visando a compreensão da sistemática de guarda e disponibilização dos mencionados registros, impõe-se a observação crítica do artigo 10 do Marco Civil da Internet. Esse dispositivo está inserido na Seção II da norma, dedicada à proteção aos registros, aos dados pessoais e as comunicações privadas, bem como estabelece que tanto à conservação quanto à eventual disponibilização desses registros deve-se observar, de forma estrita, os direitos fundamentais à intimidade, à vida privada, à honra e à imagem das pessoas envolvidas, direta ou indiretamente. A redação legal evidencia a intenção do legislador de submeter o tratamento

incluir disposições sobre sigilo, prevenção à fraude e ações de apoio à segurança pública. Disponível em: https://informacoes.anatel.gov.br/legislacao/resolucoes/2020/1495-resolucao-738. Acesso em: 05 jun. 2025.

[260] ABREU, Jaqueline de Souza. **Guarda obrigatória de registros de telecomunicações no Brasil: sobre as origens da retenção de dados e as perspectivas para direitos fundamentais**, *in*: Anais do IV Simpósio Internacional LAVITS: Vigilância, Tecnopolíticas, Territórios. Salvador: LAVITS, 2016.

de dados digitais a balizas constitucionais evitando usos desproporcionais ou incompatíveis com os valores estruturais do Estado de Direito.

Contudo, o §3º do mesmo artigo introduz uma flexibilização parcial dessa proteção ao dispor que essas garantias não impedem o acesso, por autoridades administrativas legalmente competentes, aos dados cadastrais, compreendidos como aqueles que informam a qualificação pessoal, a filiação e o endereço do usuário, desde que requisitados nos termos da lei. Essa diferenciação entre os dados que possam ser solicitados, ou seja, dados cadastrais de menor impacto e não dados pessoais sensíveis, é fulcral para a delimitação do regime jurídico aplicável a cada tipo de informação, pois se estabelece um rigor procedimental e formal mínimo visando a proteção, conforme o nível de intrusão na esfera privada do indivíduo:

> Seção II
> Da Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas
>
> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
>
> § 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º .
>
> § 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º .
>
> § 3º O disposto no caput não impede o **acesso aos dados cadastrais** que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição. (grifou-se)

Essa lógica é reforçada pelo teor do Decreto n.º 8.771/2016, que regulamenta aspectos essenciais do Marco Civil da Internet e especifica os procedimentos que devem ser observados pelos provedores de conexão e de aplicações. O decreto determina que as requisições de dados cadastrais devem ser feitas de maneira individualizada com a identificação precisa dos titulares cujos dados se busca acessar e com indicação expressa das informações pretendidas. Dessa forma, o ordenamento jurídico veda expressamente pedidos genéricos, coletivos ou inespecíficos, ainda que voltados a dados considerados de menor sensibilidade, reforçando o compromisso com a proteção da privacidade:

> Art. 11. As autoridades administrativas a que se refere o art. 10, § 3º da Lei nº 12.965, de 2014, indicarão o fundamento legal de competência expressa para o acesso e a motivação para o pedido de acesso aos dados cadastrais.

> § 1º O provedor que não coletar dados cadastrais deverá informar tal fato à autoridade solicitante, ficando desobrigado de fornecer tais dados.
> § 2º São considerados dados cadastrais:
> I - a filiação;
> II - o endereço; e
> III - a qualificação pessoal, entendida como nome, prenome, estado civil e profissão do usuário.
> § 3º **Os pedidos de que trata o caput devem especificar os indivíduos cujos dados estão sendo requeridos e as informações desejadas, sendo vedados pedidos coletivos que sejam genéricos ou inespecíficos.** (grifou-se)

Dessa coerência, evidencia-se que o sistema normativo impõe um controle rigoroso exclusivamente para os dados cadastrais, afastando práticas investigativas indiscriminadas. Desse modo, o tratamento de dados mais sensíveis, como os registros de conexão e de acesso, disciplinados no artigo 22 da mesma lei, exige, por consistência sistemática, um grau ainda mais elevado de fundamentação a especificidade e controle jurisdicional. Embora o Decreto n.º 8.771/2016 tenha sido editado para regular o disposto no artigo 10 da Lei n.º 12.965/2014, ao estabelecer parâmetros técnicos e procedimentos para proteção dos dados pessoais e do conteúdo das comunicações privadas, seus efeitos normativos repercutem também na interpretação do artigo 22 da mesma lei. Exigindo elementos objetivos para requisição de dados cadastrais, ainda que sejam de natureza menos sensível, a sistemática leva a crer que o acesso a informações, sobretudo aquelas que podem revelar padrões comportamentais e hábitos de vida, não podem prescindir de controle proporcional mais rígido, específico e se afastar da reserva de jurisdição.

A estrutura normativa referente à retenção de dados na internet distingue duas categorias de agentes, cada qual com obrigações específicas. Os primeiros são os provedores de conexão (como Claro, Vivo, Tim e etc), responsáveis pela infraestrutura de acesso à rede, incumbidos de assegurar a conexão dos terminais dos usuários à internet. A estes é imputada a obrigação de armazenar, pelo prazo de um ano, os registros de conexão, os quais compreendem informações como data, hora, de início e término de conexão, duração e o endereço IP utilizado pelo terminal (v. item 1.1.2.1 – Localização por IP). Aos provedores de conexão é vedada a guarda de registros de acesso a aplicações de internet. Isto é, poder-se-ia afirmar que a empresa de telecomunicações não pode armazenar dados referentes aos aplicativos acessados por seus usuários de conexão. Logo, pela literalidade do artigo 14[261] da Lei n.º 12.965/2014, a Claro,

[261] "Art. 14. Na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de internet." BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 6 jun. 2025.

Vivo, Tim e outras (provedoras de conexão) não podem registrar se os usuários acessaram o e-mail, serviços Google ou e-commerce, quando e por quanto tempo o fez.

Já os provedores de aplicação (como Google, Meta, Amazon, Spotfy e etc) compreendem aqueles que disponibilizam ambientes digitais com funcionalidades diversas, acessíveis mediante conexão, além de voltadas à interação direta com o usuário, como redes sociais, e-commerce e sistemas de compartilhamento de conteúdo. A eles cabem a responsabilidade pela guarda dos registros de acesso às suas próprias aplicações por seis meses[262]. Em seu turno, os provedores de aplicação não podem armazenar dados que não foram informados em suas aplicações, salvo mediante seu expresso consentimento (artigo 16, incisos I e II).

A delimitação normativa prevista no Marco Civil da Internet é essencial para o adequado enquadramento jurídico da técnica de geolocalização a ser empregada (v. itens 2.1.1 e 2.1.2). Nos termos do inciso VI do artigo 5º do referido diploma, os provedores de conexão são obrigados a armazenar, pelo prazo de um ano, apenas os registros de conexão, compreendidos como a data, hora de início e término da conexão, sua duração e o endereço IP utilizado. A literalidade de dispositivo não inclui qualquer menção à Estação Rádio Base (ERB) à qual o terminal esteve vinculado, tampouco autoriza a guarda de registros de acesso a aplicações de internet. Assim, no rigor da norma, a única informação de localização potencialmente acessível pelos provedores de conexão seria aquela inferida de forma indireta e imprecisa a partir do endereço IP (v. tem 2.1.2.1).

É verdade que determinadas resoluções administrativas da Anatel impõem obrigações técnicas a as operadoras de telecomunicações, inclusive exigindo a retenção temporária de dados de ERB por razões operacionais ou de segurança. No entanto, esses normativos possuem natureza infralegal e, portanto, não detém estatura normativa para justificar a mitigação de direitos fundamentais, como da intimidade e da proteção de dados pessoais. A eventual requisição de dados que permitam geolocalização precisa exige base em lei formal e específica, nos termos do artigo 5º, inciso LXXIX, da Constituição Federal e do artigo 10, §2º da Lei n.º 12.965/2014, sob pena de violação ao princípio da reserva legal qualificada.

Em seu turno, os provedores de aplicações de internet, a exemplo de plataformas como Google, Meta ou Amazon, estão sujeitos à obrigação de armazenar, pelo prazo de 6 meses, os

[262] KUJAWSKI, Fabio Ferreira; THOMAZ, Alan Campos Elias. Da proteção aos registros, dados pessoais e comunicações privadas – um enfoque sobre o Marco Civil da Internet. *In*: LEITE, George S.; LEMOS, Ronaldo (Orgs.). **Marco Civil da Internet**. 1. ed. Rio de Janeiro: Atlas, 2014, p. 27–30. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788522493401/>. Acesso em: 5 jun. 2025.

registros de acesso às suas próprias aplicações, ou seja, informações relativas à data, hora e endereço IP utilizados pelo usuário no momento do acesso. Esses registros, contudo, não abrangem o conteúdo da navegação, tão pouco dados como localização geográfica, conexões por Wi-Fi ou Bluetooth, ou compartilhamento de localização. O acesso a essas informações, por se tratar de dados pessoais sensíveis e integrantes da esfera privada do titular, somente pode ocorrer mediante ordem judicial específica e fundamentada respaldada em legislação formal que observe os princípios constitucionais da proporcionalidade necessidade e adequação. Qualquer coleta ou utilização sem essa base legal compromete a validade do ato e implica violação ao direito fundamental à proteção de dados, especialmente após o reconhecimento de sua autonomia normativa com a Emenda Constitucional n.º 115/2022.

Não obstante a lógica normativa delineada pelo Marco Civil da Internet que distingue de forma precisa os tipos de registros passíveis de retenção, registro de conexão e de acesso a aplicações de internet, observa-se, na prática, o emprego do artigo 22 da referida lei como fundamento para admitir a requisição judicial de informações de geolocalização. De fato, esse dispositivo prevê a possibilidade de que a parte interessada requeira judicialmente o fornecimento de registros para fins de investigação penal ou instrução processual desde que observados os requisitos legais dispostos em seu parágrafo único. São eles: (i) fundados indícios da ocorrência do ilícito; (ii) justificativa motivada da utilidade dos registros solicitados para a investigação ou instrução probatória; e (iii) delimitação temporal do período a que os registros se referem.

Entretanto, cumpre reiterar que os tipos de registros definidos no artigo 5º da mesma norma, registros de conexão e de acesso a aplicações de internet, não contemplam, em sua literalidade, dados de localização geográfica, como reiteradamente afirmado acima. Apesar disso, mandados judiciais de localização têm sido frequentemente embasados no artigo 22 Marco Civil como se observa, por exemplo, no emblemático caso da investigação do assassinato da ex-vereadora Marielle Franco, no qual a autoridade judicial determinou a obtenção de dados que permitissem a reconstrução dos deslocamentos de determinados suspeitos. O emprego do artigo 22, embora recorrente, suscita controvérsias quanto à sua adequação jurídica, uma vez que amplia o alcance de dispositivo legal sem haja autorização expressa ou previsão normativa específica que ampare a coleta de dados de localização, os quais, por sua natureza, integram a esfera de proteção dos direitos fundamentais à intimidade e à autodeterminação informativa cuja restrição demanda lei formal específica e respeito ao princípio da reserva de jurisdição.

4.5. CASO MARIELLE FRANCO

Deve-se ressaltar que não há ineditismo no sistema judiciário brasileiro quanto à expedição dos *geofence warrants* para produção de prova em inquéritos e ações criminais. Destacam-se, no Superior Tribunal de Justiça, os **Recursos em Mandado de Segurança n.^{os}** 60.698, 61.302 e 62.143, nos quais, em seus julgamentos, avaliou-se a decisão do juiz **da 1ª instância do Rio de Janeiro** poderia determinar que o Google fornecesse dados técnicos relacionados ao caso do homicídio da vereadora Marielle Franco e seu motorista, Anderson Gomes.

A medida judicial impugnada tinha por objetivo identificar os usuários que, no intervalo temporal de quatro dias, realizaram pesquisas por palavras-chaves, como **"Marielle Franco", "vereadora Marielle", "agenda vereadora Marielle", "casa das pretas", "rua dos inválidos, 122" ou "rua dos inválidos".** Além disso, a decisão judicial fixou um perímetro geográfico específico na cidade do Rio de Janeiro e estendeu a requisição de dados ao uso do aplicativo de mapas *Waze*, com o intuito de obter os respectivos endereços dos IPs ou identificadores de dispositivos (Device Ids) de seus usuários.

A empresa Google, ao impetrar o mandado de segurança, apresentou uma argumentação estruturada com base na proteção dos direitos fundamentais. Defendeu que a ausência de uma individualização dos alvos investigativos tornaria a ordem judicial excessivamente ampla e incompatível com o princípio da legalidade estrita, caracterizando, em sua argumentação, verdadeira medida genérica e indiscriminada de busca *(fishing expedition).* A *Bigtech* também aduziu que a extensão temporal da requisição e a abrangência dos critérios adotados comprometiam desproporcionalmente a privacidade de um número indeterminado de cidadãos, inclusive aqueles que nada se relacionavam com a conduta delituosa ou fatos investigados. Por fim, sustentou que não se havia demonstrado a imprescindibilidade da medida, tão pouco a inviabilidade de obtenção da prova por outros meios menos invasivos.

Os Ministros do STJ, ao analisar o recurso, assentaram que os dados solicitados pelo Ministério Público, por se referirem a registros de conexão e acesso a aplicações de internet, 5 adorariam na categoria dos denominados "dados estáticos" ou cadastrais. A Corte traçou distinção conceitual entre esses dados, que correspondem a informações técnicas armazenadas previamente pelos provedores, e os dados compreendidos no fluxo de comunicação cuja Inter receptação depende de autorização judicial fundada nos moldes da Lei n.º 9.296/1996. O acórdão do recurso fundamentou-se na ideia de que o regime de proteção conferido aos dados estáticos, embora igualmente amparado por garantias condicionais de privacidade e intimidade,

admite mitigação em hipóteses excepcionais, especialmente diante de crimes de Extrema gravidade e complexidade investigativa.

Sob o prisma normativo, a Corte invocou os artigos 10, 22 e 23 do Marco Civil da Internet, interpretando que os dispositivos citados não exigem a prévia individualização dos investigados, desde que a ordem judicial contenha elementos mínimos, como indícios da ocorrência do ilícito, justificativa da utilidade na medida e delimitação temporal dos dados requeridos. Partindo-se dessa perspectiva, o STJ concluiu que, em contextos como o dos autos, a própria finalidade da medida investigativa justifica a ausência de identificação prévia dos titulares dos dados, sendo justamente o fornecimento das informações requeridas o meio para alcançar a identificação posterior dos possíveis envolvidos no crime.

No que concerne à proporcionalidade, o acórdão não adotou a estrutura tripartida da análise, adequação, necessidade e proporcionalidade em sentido estrito, para concluir que a medida era legítima, diante do interesse público na apuração de crimes dolosos contra vida com ampla repercussão. A decisão ainda ressalvou que os dados irrelevantes à investigação deveriam ser descartados de modo a mitigar eventuais impactos indevidos sobre terceiros alheios à investigação.

Não obstante os bem lançados apontamentos, a decisão da Corte Superior diverge de abordagens mais restritivas presentes na jurisprudência de tribunais estrangeiros, como a Corte Europeia de Direitos Humanos, especialmente no julgamento que culminou na invalidade da Diretiva n.º 2006/24/CE, nos casos apensados *Digital Rights Ireland e Seitlinger* (v. item 4.3.2). Ainda que a norma dissesse respeito apenas a dados considerados estáticos, como registro de ligação e duração de chamadas, entendeu-se que essas informações, quando armazenadas de forma generalizada e sem cautelas adequadas, permitem a reconstrução detalhada da vida privada dos indivíduos, representando ingerência grave e desproporcional na esfera da intimidade. A Corte Europeia concluiu que, justamente por seu potencial invasivo, esses dados também exigem tutela normativa específica e estão submetidos a reserva legal e a critérios estritos de necessidade e proporcionalidade. Em contraste, poder-se-ia acreditar que a solução acolhida pelo STJ no caso Marielle revela uma postura mais permissiva quanto ao acesso estatal a informações sensíveis mesmo diante da ausência de disciplina legal específica sobre o tema aplicável ao caso.

Desta forma, percebe-se que os mandados de geolocalização além de enfrentar a análise de sua colisão com os princípios constitucionais da inviolabilidade da intimidade e vida privada de uma pessoa e sigilo das comunicações, ainda enfrentam questionamentos no âmbito do direito processual penal, podendo ser consideradas medidas genéricas e indiscriminadas de

busca (*fishing expedition*), vez que os mandados precisam necessariamente possuir a identificação dos envolvidos e objetivo certo, devendo, inclusive, definir o local e espaço temporal. Assim, tem-se que o procedimento de *geofencing*, se não propriamente empregado, caracteriza-se como uma afronta aos direitos fundamentais da personalidade e da intimidade dos cidadãos. No caso do mandado de geolocalização, há pessoas que não são investigadas ou acusadas da prática de algum ato ilícito e têm sua privacidade e liberdade devassadas em busca de atos de informação/investigação, atrelados a um juízo de probabilidade, na definição trazida por Aury Lopes Jr.[263], e não um juízo de prova que visa firmar o convencimento do juiz, produzidos em observância aos princípios da ampla defesa e do contraditório.

4.6. TEMA 1148 DO SUPREMO TRIBUNAL FEDERAL

Entre as inovações estruturantes promovidas pela Emenda Constitucional n.º 45, de 2004, conhecida como "Reforma do Judiciário", destaca-se, com especial relevo, a criação da repercussão geral, mecanismo processual que condiciona a admissibilidade dos recursos extraordinários à demonstração da relevância jurídica, política, social ou econômica da matéria constitucional discutida, bem como de sua transcendência além dos interesses subjetivos das partes envolvidas. Desde sua previsão no §3º do artigo 102 da Constituição Federal, o instituto tem papel central na redefinição da atuação do Supremo Tribunal Federal, permitindo à Corte exercer controle mais seletivo estratégico de sua pauta jurisdicional.

Essa nova lógica processual reflete não apenas uma tentativa de racionalização do volume de demandas submetidas à Corte Constitucional, mas também a afirmação de sua função como instância de definição normativa orientadora da interpretação constitucional no país. A regulamentação infraconstitucional foi estabelecida pela Lei n.º 11.418/2006, que introduziu os artigos 543-A e 543-B ao CPC/1973, posteriormente substituídos pelos artigos 1.035 a 1.041 do CPC/2015. A doutrina ressalta que a repercussão geral não é apenas técnica processual, mas também ferramenta de política judicial, por meio da qual o STF atua como agente de estabilização constitucional, selecionando causas paradigmáticas com potencial de irradiar efeitos estruturais sobre o ordenamento jurídico[264].

Insere-se nesse contexto a relevância do Tema 1148 da sistemática de repercussão geral, no qual se discute "*limites para decretação judicial da quebra de sigilo de dados telemáticos,*

[263] LOPES JR., Aury. **Direito processual penal**, 16. ed. São Paulo: Saraiva Educação, 2019.
[264] FREITAS JÚNIOR, Horival Marques. **Repercussão geral das questões constitucionais**, Dissertação de Mestrado, Universidade de São Paulo, São Paulo, 2014.

no âmbito de procedimentos penais, em relação a pessoas indeterminadas". A controvérsia originou-se no âmbito do Recurso Extraordinário n.º 1.301.250/RJ, interposto pela Google do Brasil Internet LTDA., em face do acórdão proferido pelo Superior Tribunal de Justiça que negou provimento ao recurso ordinário em mandado de segurança relacionado à investigação do homicídio da vereadora Marielle Franco acima descrito. O julgamento inaugural desse recurso extraordinário concluiu pelo reconhecimento da repercussão geral quanto à discussão acerca da constitucionalidade no *"fornecimento de registros de acesso à internet e de IPs (internet protocol address), circunscritos a um lapso temporal demarcado, sem, contudo, a indicação de qualquer elemento concreto apto a identificar os usuários"*[265].

O referido recurso ingressou no Supremo Tribunal Federal no dia 26 de novembro de 2020, sendo distribuído à relatoria da Ministra Rosa Weber. O processo teve tramitação complexa, marcada pela manifestação diversas entidades admitidas como *amicus curiae*, refletindo o elevado grau de interesse público e a sensibilidade constitucional da matéria. Após essa fase de instrução e admissibilidade, o feito foi incluído na pauta do Plenário Virtual do STF para julgamento, em 22 de setembro de 2023, ocasião em que a Ministra Rosa Weber proferiu seu voto, judicioso e denso em fundamentos, poucos dias antes de sua aposentadoria, efetivada em 30/09/2023.

Em suas razões de decidir, a Ministra atribuiu especial relevo ao princípio da legalidade, considerado valor estruturante da atividade investigatória e da produção de provas no processo penal. Para a Relatora, a atuação tanto dos órgãos de persecução penal quanto do poder judiciário deve observar, de forma estrita, os limites estabelecidos em norma formal e específica, sobretudo quando se trata de medidas potencialmente lesivas a direitos fundamentais, como a quebra de sigilo de dados pessoais.

A Ministra também destacou a centralidade do direito fundamental à proteção de dados pessoais no contexto constitucional contemporâneo, observando que a ausência de legislação específica que discipline, de modo adequado, o tratamento de dados sensíveis no âmbito criminal, como a LGPD penal, fragiliza as garantias do titular dos dados diante de medidas estatais de caráter invasivo. Alertou que a inexistência de balizas legais claras demanda o judiciário a uma postura ainda mais cautelosa, com o intuito de evitar o esvaziamento das garantias relacionadas à privacidade e à autodeterminação informativa.

---

[265] BRASIL. Supremo Tribunal Federal. Recurso Extraordinário n.º 1.301.250/RJ. Relatora: Ministra Rosa Weber. Reconhecimento de repercussão geral em 27 maio 2021. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=756074304. Acesso em: 7 jun. 2025.

Ao interpretar os dispositivos do Marco Civil da Internet, a Ministra Rosa Weber defendeu que o número de IP e o identificador de dispositivo (Device ID) devem ser qualificados como dados pessoais, e não meras informações cadastrais. Esse entendimento decorre do reconhecimento de que a atribuição de endereçamento de IP, dada a sua lógica técnica de sua atribuição, muitas vezes dinâmica e reutilizável, possibilitam, de forma direta ou indireta, a individualização dos seus titulares, o que amplia seu potencial lesivo à intimidade quando tratados de forma indiscriminada.

Por fim, a Relatora, embora reconhecesse a gravidade e repercussão do crime, teceu críticas à generalidade da decisão judicial questionada, que autorizava a requisição de registro de um universo indeterminado de usuários com base em critérios excessivamente genéricos, como a realização de buscas poder terminadas palavras-chave e a delimitação de um intervalo temporal especial. A seu ver, a ausência de individualização mínima dos alvos e de parâmetros objetivos compromete os postulados da proporcionalidade e necessidade, expondo a privacidade de inúmeros cidadãos ao risco de devassa informacional sem justificativa adequada:

> Entendo, na linha da jurisprudência sedimentada desta Suprema Corte, inadmissível, sob o ponto de vista constitucional – seja sob o ângulo do direito fundamental à privacidade, seja sob a óptica do direito fundamental à proteção de dados pessoais –, a quebra generalizada do sigilo de dados de pessoas indeterminadas e indetermináveis previamente.
> Isso porque, na minha compreensão, sendo o sigilo de dados telemáticos a regra constitucional, o seu afastamento somente se torna possível quando indicada especificamente a causa provável, com suporte no acervo já colhido. Somente quando presente tais requisitos se mostra legítima a pontual ruptura da esfera de privacidade de titularidade de todos os cidadãos.
> A legitimidade da quebra de sigilo de dados advém, segundo penso, necessariamente da indicação concreta e fundamentada de que existem indícios de autoria e materialidade em face de pessoa certa e determinada, ou, no mínimo, determinável, pois ilegítimas investigações genéricas, com o escopo de buscar elementos incriminadores aleatórios, sem qualquer espécie de amparo prévio.
> Não se pode esquecer que a quebra do sigilo de dados telemáticos consubstancia restrição a direitos fundamentais. Assim, a meu juízo, referida limitação, no que diz especificamente com o afastamento do sigilo constitucional determinado por meio de decisão judicial, somente deve ser efetivada de forma pontual, episódica, caso estritamente necessária para elucidação de práticas delituosas, com a individualização do investigado e do objeto da investigação (MORAES, Alexandre de. Direitos humanos fundamentais: teoria geral – comentários aos arts. 1º a 5º da Constituição da República Federativa do Brasil – doutrina e jurisprudência. 12. ed. São Paulo: Atlas, 2021, p. 161), em ordem a mitigar o impacto do ato decisório[266].

Cabe destacar que o julgamento do Recurso Extraordinário n.º 1.301.250/RJ permanece suspenso em decorrência de pedido de vista formulado pelo Ministro Gilmar Mendes, na sessão

[266] BRASIL. Supremo Tribunal Federal. Recurso Extraordinário n.º 1.301.250/RJ. Relatora: Ministra Rosa Weber. Voto da Relatora em 22 de setembro de 2025. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=6059876. Acesso em: 7 jun. 2025.

plenária do Supremo Tribunal Federal, realizada em 24 de abril de 2025. Após o voto da Ministra Rosa Weber, o julgamento havia sido retornado em 16 de outubro de 2024, ocasião em que os Ministros Alexandre de Moraes e Cristiano Zanin proferiram seus votos. Em seguida, o Ministro André Mendonça solicitou vista regimental e apresentou o seu voto em 23 de abril de 2025. Contudo, no dia seguinte a esta retomada, o Ministro Gilmar Mendes requereu nova vista, o que resultou na interrupção do julgamento e postergação de sua conclusão. Assim, muito embora os votos proferidos até o momento tenham sido objeto de debate na sessão, a redação final e a formação definitiva do entendimento da Corte permanecem pendentes, aguardando o voto vista e eventual deliberação dos demais Ministros. Até que haja o seu desfecho, a tese de repercussão geral ainda não foi firmada, o que mantém em aberto a definição jurisprudencial sobre os parâmetros constitucionais para acesso judicial a dados digitais sensíveis no âmbito de investigações criminais a pessoas indeterminadas.

Não obstante, considerando o teor da gravação das sessões[267][268], foi possível acompanhar os entendimentos dos Ministros que proferiram seus votos, bem como os debates travados. O Ministro Alexandre de Moraes apresentou seu voto-vista, discordando do voto da relatora. O Ministro manifestou preocupação com os efeitos de interpretação excessivamente restritiva da quebra do sigilo de dados em investigação criminal. Assim, defendeu a constitucionalidade da requisição judicial dirigida ao Google, argumentando que a medida se voltava a um grupo indeterminado, mas determinável de usuários. Para tanto, o Ministro considerou outros elementos probatórios apurados durante a instrução criminal, como no caso concreto, identificados a partir de meios objetivos como buscas por palavras-chave, em local e período delimitados. Essa delimitação objetiva afastaria o risco de uma devassa generalizada e legitimaria a medida, a qual ainda seria submetida à autorização judicial.

O Ministro também enfatizou que o direito ao sigilo de dados, à semelhança de outros direitos fundamentais, não possui caráter absoluto, podendo ser relativizado diante da gravidade do crime e da necessidade de assegurar a eficácia na persecução penal. Em diversos momentos o magistrado apontou que a quebra do sigilo de dados é um meio de obtenção de prova relevantíssimo às autoridades policiais, sem a qual a atividade investigativa poderia ser severamente comprometida. Invocando o artigo 22 do Marco Civil da Internet, sustentou que a

[267] BRASIL. Supremo Tribunal Federal. Sessão de julgamento – Tema 1148 – RE n.º 1.301.250/RJ – 16 out. 2024. Participação dos Ministros Alexandre de Moraes e Cristiano Zanin. YouTube, 16 out. 2024. Disponível em: https://www.youtube.com/watch?v=tkGYtwsnR1c. Acesso em: 7 jun. 2025.
[268] BRASIL. Supremo Tribunal Federal. Sessão de julgamento – Tema 1148 – RE n.º 1.301.250/RJ – 23 abr. 2025. Voto do Ministro André Mendonça. YouTube, 23 abr. 2025. Disponível em: https://www.youtube.com/watch?v=Gr7y0wV7W_A&t=4s. Acesso em: 7 jun. 2025.

legislação brasileira autoriza o compartilhamento desses dados com autoridades públicas, desde que mediante decisão judicial. Procurou, ainda, deslegitimar a resistência da empresa Google, alegando que, embora utilize dados pessoais com finalidades comerciais, opõem-se ao seu uso legítimo e processos investigatórios o que configuraria uma postura contraditória.

Todavia, a manifestação do voto do Ministro Alexandre de Moraes suscita críticas técnicas relevantes que merecem exame aprofundado. Um dos principais pontos de atenção reside na ausência de uma distinção rigorosa entre as diferentes categorias de dados pessoais. Em diversas passagens de sua apresentação, o Ministro parece equiparar dados cadastrais, registros de aplicações e dados de conteúdo, como os históricos de busca, sem observar as definições estabelecidas pelo artigo 5º da Lei n.º 12.965/2014. Essa equiparação ignora que essas categorias possuem natureza jurídica distintas e, por conseguinte, demandam níveis diferenciados de proteção e requisitos específicos para acesso por parte do Poder Público.

Embora a LGPD, no seu artigo 5º, distinga entre dados pessoais sensíveis, aqueles que dizem respeito à origem racial ou étnica, convicção religiosa, opinião política, filiação à sindicato, dados referentes à saúde, à vida sexual, dados genéticos ou biométricos vinculados a uma pessoa natural, e, por exclusão, os dados pessoais não sensíveis, essa separação tradicional se mostra, em parte, insuficiente frente aos desafios impostos pelo uso massivo de tecnologias de big data e inteligência artificial no tratamento das informações. Isso porque, como pontuado no item 3.4 da presente dissertação, ao abordar os metadados e a natureza dos dados de tráfego e localização, no contexto europeu, Coutinho[269] ponderou que, mesmo informações que isoladamente não se revelem sensíveis podem, quando trabalhadas e interconectadas pelas empresas de tecnologia, conduzir a inferências altamente reveladoras acerca da vida privada, das preferências e até mesmo de aspectos íntimos dos indivíduos ou de grupos.

Essa negligência em reconhecer que os dados, quando tratados de forma massiva contextual, podem ensejar inferências altamente reveladoras sobre a vida privada, compromete a eficácia do regime jurídico protetivo dos dados. É justamente essa preocupação destacada por Watcher e Mittelstadt[270], ao analisar as fragilidades do regime de salvaguardas aos dados conferido pela RGPD. O tratamento massivo de dados, sejam eles fornecidos diretamente pelo titular ou coletados por meios indiretos, como registro de localização, padrões de navegação e uso de dispositivos, permite a formulação de inferências e a criação de novos dados pessoais

---

269 **COUTINHO, Francisco Pereira. Data Retention in Portugal: Big Brother is (No Longer) Watching**. 2023. Disponível em: <https://papers.ssrn.com/abstract=4216870>. Acesso em: 16 jun. 2025.

270 WACHTER, Sandra; MITTELSTADT, Brent. **A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI**. Columbia Business Law Review, v. 2019, p. 494, 2019. Disponível em: <https://heinonline.org/HOL/Page?handle=hein.journals/colb2019&id=506&div=&collection=>.

que não existiam na forma original. Esses dados inferidos, ainda que resultantes do processamento de informações não sensíveis, são capazes de gerar impactos relevantes sobre direitos fundamentais, ao influenciar a privacidade, a reputação, a autonomia e a própria identidade dos indivíduos. De fato, essas inferências devem ser encaradas, do ponto de vista jurídico, com o mesmo grau de proteção aos dados sensíveis, especialmente diante do risco que venham a fundamentar decisões automatizadas ou avaliações que afetem diretamente a esfera jurídica e social das pessoas.

Esse panorama evidencia a necessidade de uma postura crítica no momento de emprego das categorias jurídicas, visando o adequado fortalecimento das garantias constitucionais em face do tratamento automatizado e massivo de dados. Conforme já sustentado por Bruno Bioni[271], o foco da proteção de dados deve estar na finalidade e nos riscos gerados pelo tratamento, mais do que apenas na natureza originária dos dados coletados, exigindo do legislador e do intérprete uma atenção redobrada à ação de mecanismos que impeçam o uso discriminatório, injusto ou desproporcional de informações pessoais, especialmente as derivadas e inferidas.

A falta de clareza na distinção dessas espécies de dados compromete a análise jurídica quanto à necessidade de reserva legal, proporcionalidade da medida e observância ao devido processo legal substancial, sobretudo em contexto de requisição de dados em massa. Assim, a interpretação adotada pelo Ministro pode diluir os critérios constitucionais de proteção à intimidade e à autodeterminação informativa. Ademais, essa confusão conceitual pode resultar em erro de enquadramento jurídico das hipóteses de acesso aos dados, especialmente no tocante ao artigo 10 do Marco Civil da Internet, que estabelece diferentes regimes de proteção conforme a natureza das informações envolvidas.

Além disso, a invocação do Marco civil da Internet como base normativa para legitimar a quebra de sigilo no caso concreto revela uma dissonância entre a finalidade da norma e a natureza da conduta investigada. A citada lei é uma legislação orientada à disciplina do comportamento e das relações jurídicas estabelecidas no ambiente digital, voltada à proteção da neutralidade da rede, à privacidade dos usuários e à regulação do tratamento de dados na esfera da internet. No entanto, a manifestação do voto parte do pressuposto de que essa mesma norma pode embasar a requisição de dados pessoais para apuração de um crime ocorrido no

[271] BIONI, Bruno. **Proteção de dados pessoais**. 1. ed. Rio de Janeiro: Forense, 2019. Disponível em: <https://www.lexml.gov.br/urn/urn:lex:br:rede.virtual.bibliotecas:livro:2019;001142886>. Acesso em: 12 jun. 2025.

mundo real desconectado do contexto originário de produção das informações digitais cuja quebra se pretende.

Essa aplicação transversa da norma ignora que os rastros digitais buscados não são o meio pelo qual o crime foi cometido, mas apenas elementos indiciários auxiliares à sua elucidação. Ao transpor os dispositivos do Marco Civil da Internet para autorizar a obtenção de dados relevantes e íntimos em um cenário de coleta massiva e não individualizada sem que haja previsão legal específica para esse tipo de medida, a manifestação do Ministro fragiliza a exigência constitucional da reserva legal estrita para restrições a direitos fundamentais. A menção à investigação de crimes digitais, como a pedofilia, embora relevante em outros contextos, não se mostra pertinente ao caso concreto, pois homicídio investigado foi cometido no espaço físico e a tentativa de obtenção de provas por meio de histórico de buscas revela uma operação inversa: busca-se aplicar o marco regulatório da internet à reconstrução fática de eventos reais, sem que a conexão entre esses universos esteja juridicamente disciplinada.

Por fim, ao longo de sua manifestação o Ministro Alexandre de Moraes faz reiteradas referências a crimes em que há restrição à liberdade da vítima, como forma de justificar a excepcionalidade e a necessidade das medidas de quebra de sigilo de dados. Contudo aparenta desconsiderar que a própria constitucionalidade dos artigos 13-A e 13-B do Código de Processo Penal, que regula as hipóteses legais de localização de investigados por meio de dados telemáticos, já foi analisada e reconhecida pelo Supremo Tribunal Federal no julgamento da ADI n.º 5.642/DF. Naquela ocasião, a Corte assentou que a adoção dessas medidas exige previsão legal específica, controle judicial e observância aos princípios da proporcionalidade da reserva de jurisdição. O risco, que se evidencia, é o de se utilizar exceções legítimas, como os casos de restrição à liberdade das vítimas, para justificar medidas que, no caso concreto, não se enquadram na moldura normativa já delineada e validada pelo próprio STF.

O Ministro Cristiano Zanin também proferiu seu voto, o qual reconheceu a complexidade da matéria e apresentou um voto de conciliação entre as preocupações com a eficácia da investigação criminal levantada pelo Ministro Alexandre de Moraes e a necessária proteção dos direitos fundamentais, especialmente os direitos à privacidade e à autodeterminação informativa.

O Ministro destacou a centralidade do princípio da proporcionalidade como critério orientador da atuação judicial em matéria de quebra de sigilo. Em sua ótica, ordens judiciais que alcancem pessoas inicialmente indeterminadas só se justificam quando houver nos autos elementos prévios que permitam identificar um grupo “determinável”, ou seja, quando houver indicativos concretos que vinculem logicamente os dados buscados ao fato investigado.

Afirmou ser indispensável que a medida seja necessária, adequada e proporcional ao caso concreto. Ao analisar a tese de repercussão geral pretendida, propôs que seja possível distinguir entre usuários suspeitos e usuários não suspeitos, reservando o acesso aos dados apenas aqueles sobre os quais recai algum tipo de vinculação aos fatos sob apuração.

Adicionalmente, o Ministro Cristiano Zanin tratou da interpretação do Marco Civil da Internet, destacando as diferenças entre o artigo 22, que trata de dados de conexão em registros de acesso, em cotejo com o artigo 10, que versa sobre dados pessoais e informações de conteúdo, e advertiu que o dever legal de guarda e posto as plataformas está limitado ao primeiro, bem como que não há imposição expressa quanto a retenção de dados de conteúdo, como histórico de buscas. Com isso, criticou a extensão das ordens judiciais a dados não abrangidos pela obrigação legal de armazenamento.

Em seu turno, o Ministro André Mendonça apresentou um voto técnico e cauteloso, alinhado em parte, ao entendimento da Ministra Rosa Weber, mas com ênfases próprias que o distinguem dentro do Colegiado do Supremo. Seu voto defende uma interpretação restritiva das hipóteses de quebra judicial de sigilo de dados, sobretudo quando se trata de medidas voltadas a pessoas indeterminadas, ainda que determináveis, refutando a tese o Ministro Alexandre de Moraes.

Desde o início da sua manifestação, o Ministro enfatiza a centralidade do princípio da proporcionalidade como filtro para admissibilidade dessas medidas, o que envolve não apenas a adequação e a necessidade, mas, sobretudo, a proporcionalidade em sentido estrito. Defende que a requisição judicial de dados telemáticos só é legítima quando precedida de uma fundada suspeita, um requisito que, segundo ele, já é consolidado em outros precedentes da Corte, como o Tema 280, que trata da revista pessoal.

Segundo Mendonça, para que se autorize o compartilhamento de dados de pessoas, é necessário observar: (i) os atingidos devem ser objetivamente determinados; (ii) a especificação precisa do tipo de dado envolvido no acesso; (iii) a identificação de um fator de correlação claro entre os dados requeridos e as pessoas investigadas; e (iv) a demonstração de que esses dados são imprescindíveis e não podem ser obtidos por meios menos invasivos. Ele alerta que, sem esses requisitos, corre-se o risco de se validar autênticas *fishing expeditions* ou mesmo "arrastões probatórios", incompatíveis com o devido processo legal e com os direitos fundamentais à intimidade à privacidade e à proteção de dados pessoais.

No aspecto normativo, o Ministro André Mendonça propôs que a tese firmada pelo STF faça referência expressa aos artigos 7º; 10, §§1º e 2º; e 22 (*caput* e parágrafo único) da Lei n.º 12.965/2014, ressaltando que não se deve mencionar apenas os incisos II e III do parágrafo

único do artigo 22, mas sim o dispositivo em sua integralidade, a fim de se garantir uma interpretação conforme à Constituição e às demais exigências legais. Ademais, defende que se insira expressamente a necessidade de que a ordem judicial esteja lastreada em fundados indícios de ocorrência de infração penal, acompanhada de justificativa motivada sobre a utilidade dos registros solicitados e de delimitação temporal da medida.

Em seu voto, o Ministro posiciona-se de forma crítica à expressão "pessoas indeterminadas, mas determináveis", presente na redação sugerida inicialmente pelo Ministro Alexandre de Moraes. Para ele, essa expressão é excessivamente vaga e pode gerar interpretações amplas e perigosas. Em substituição, propõe-se que o acesso aos dados só seja admitido quando demonstrada a existência de fundada suspeita objetiva, entendida como identificação de elementos concretos que estabeleçam um vínculo entre os dados buscados e os fatos investigados. Mendonça reafirma que o simples fato de a medida ser autorizada por ordem judicial não basta para validá-la, é necessário que o magistrado fundamente de forma clara específica os critérios de admissibilidade da medida, sob pena de nulidade.

Apesar da consistência argumentativa o voto de Mendonça também foi alvo de críticas por parte de outros membros da Corte. O Ministro Alexandre de Moraes, por exemplo, advertiu para o risco de se inviabilizar instrumentos legítimos e modernos de investigação criminal, especialmente no combate à crimes de pedofilia e sequestro, ao se exigir, de forma demasiadamente rígida, a individualização prévia de suspeitos. Segundo Moraes, a jurisprudência não pode desconsiderar a realidade empírica das investigações criminais contemporâneas, que muitas vezes partem de rastros digitais indeterminados para apenas a posteriori identificar os autores da infração penal.

Nesse ponto a divergência entre os dois Ministros revelou diferentes visões sobre o equilíbrio entre a segurança pública e direitos fundamentais. Enquanto Mendonça privilegia a proteção da esfera privada do cidadão comum e teme os efeitos de uma jurisprudência excessivamente permissiva, Alexandre de Moraes enfatiza a necessidade de ferramentas eficazes de persecução penal, desde que submetidos a controle judicial. Essa tensão revela um dilema jurídico e político mais profundo, qual seja, como compatibilizar o avanço da tecnologia investigativa com respeito às garantias constitucionais evitando tanto a ineficácia estatal quanto a banalização da violação de direitos.

Em síntese, o voto do Ministro André Mendonça contribui significativamente para o debate sobre os limites da atuação estatal na coleta de dados telemáticos investigações criminais, ao introduzir um grau maior de exigência quanto à fundamentação, delimitação e controle judicial das medidas de quebra de sigilo. Sua proposta busca evitar abusos, preservar

a integridade do processo penal e promover segurança em um cenário de crescente intersecção entre tecnologia e investigação. Contudo, o modelo a ser fixado pela Corte exigirá, na prática, aprimoramento técnico das decisões judiciais e maior rigor das autoridades investigativas, para que se alcance o equilíbrio almejado entre liberdade e segurança. A solicitação de visto por parte do Ministro Gilmar Mendes, reconhecido por suas contribuições em matéria de direitos fundamentais e processo penal, reitera a complexidade do debate e a necessidade de amadurecimento do tema antes da fixação da tese com repercussão geral.

4.7. CAMINHOS PARA O DIREITO BRASILEIRO

Ao se examinar as manifestações de voto dos Ministros do Supremo Tribunal Federal, constata-se que o entendimento acerca do sistema de proteção de dados no Brasil ainda se apresenta de forma fragmentada. Para uma análise mais sistemática do tema, toma-se como referência o julgamento da ADI 6.387/DF, ocorrido em 7 de maio de 2020, no qual o STF apreciou a ação direta de inconstitucionalidade ajuizada pelo Conselho Federal da Ordem dos Advogados do Brasil. A ação impugnava a Medida Provisória n.º 954, ato normativo extraordinário editado sob alegação de urgência, que disciplinava o compartilhamento de **dados cadastrais**, como nomes, números de telefone e endereços de pessoas físicas ou jurídicas, entre empresas de telecomunicações e o IBGE. Ressalta-se que esse tratamento de dados tinha como finalidade específica, qual seja, viabilizar a produção de estatísticas oficiais durante a emergência de saúde pública decorrente da pandemia da COVID-19.

Como ressaltado no item 1.2 do Capítulo 1, que abordou o uso das tecnologias de geolocalização durante a pandemia, diversas soluções tecnológicas foram implementadas com êxito, constituindo exemplos notórios de cooperação entre o poder público e a iniciativa privada na tentativa de mitigar a crise sanitária, a exemplo do SIMI-SP e dos sistemas de alerta de proximidade com pessoas em potencial situação de risco. É inegável que essas iniciativas suscitaram relevantes discussões jurídicas acerca da proteção de dados, em especial devido à *vacatio legis* da LGPD naquele momento. Ainda assim, os debates já poderiam ter sido orientados pelos direitos fundamentais, conforme advertido em artigo de Clara Iglesias Keller e Jane Reis Gonçalves Pereira[272].

[272] KELLER, Clara Iglesias; PEREIRA, Jane Reis Gonçalves. **Data protection in times of Covid-19: the risks for surveillance in Brazil**. Internet Policy Review, 2020. Disponível em: <https://policyreview.info/articles/news/data-protection-times-covid-19-risks-surveillance-brazil/1462>. Acesso em: 28 abr. 2025.

Pretende-se evidenciar, contudo, é que as circunstâncias fáticas que compunham o pano de fundo do julgamento da ADI 6387/DF poderiam ser interpretadas como favoráveis ao compartilhamento das informações solicitadas. Isso porque os dados a serem tratados, de natureza meramente cadastral, situam-se em um patamar inferior na escala de intrusão à esfera privada, de modo que, em tese, não configurariam afronta grave aos direitos fundamentais à intimidade e à privacidade. Ressalta-se que a tese de mitigação da proteção de dados cadastrais foi acolhida pelo Superior Tribunal de Justiça no julgamento do RMS 60.698/RJ, em 26 de agosto de 2020, referente ao caso do homicídio da vereadora Marielle Franco, já mencionado.

No entanto, ao apreciar a ADI 6.387/DF, o STF adotou uma compreensão mais rigorosa quanto aos limites constitucionais aplicáveis à proteção de dados. Naquele julgamento, a Corte asseverou a necessidade de observância estrita ao âmbito de proteção assegurado pelas cláusulas constitucionais que resguardam a liberdade individual, a privacidade e o livre desenvolvimento da personalidade. Assim, embora o compartilhamento de dados previstos na Medida Provisória n.º 954/2020 estivesse vinculado a uma finalidade específica, qual seja, a produção de estatísticas oficiais durante a emergência de saúde pública, bem como dissesse respeito a dados de natureza aparentemente meramente cadastral, o STF entendeu que essas circunstâncias não afastavam a necessidade de um controle rigoroso de proporcionalidade. Reconhecendo a existência de uma colisão em sentido estrito entre direitos fundamentais individuais e o bem coletivo associado à proteção de saúde pública, a Corte decidiu pela suspensão da eficácia da medida provisória, em razão dos riscos à preservação da intimidade e da autodeterminação informativa dos cidadãos.

Em sentido oposto, no julgamento da ADI 5.642/DF, ocorrido em 18 de abril de 2024, que tratava da constitucionalidade dos artigos 13-A e 13-B do Código de Processo Penal, conforme examinado no item 4.4.1 deste Capítulo, o Supremo Tribunal Federal adotou um entendimento mais flexível quanto à proteção dos dados pessoais. A Corte reafirmou que o direito à privacidade, embora revestido de caráter fundamental, não ostenta natureza absoluta, sendo passível de mitigação diante da necessidade de preservação da segurança pública. O voto do Ministro Relator afastou a existência de expectativa legítima de privacidade em relação a dados cadastrais, inclusive citando a *third-party doctrine* do direito norte-americano e a disciplina do Marco Civil da Internet. Ainda que tenha reconhecido a possibilidade técnica de localização de dispositivos a partir da comunicação com estações rádio-base, continuou a tratar essas informações como se dados cadastrais fossem. Outrossim, considerou que a requisição de meios técnicos prevista no artigo 13-B do CPP não ofende a reserva de jurisdição, na medida em que tem por finalidade permitir a localização e identificação imediata da vítima em situações

de flagrante delito, contexto no qual a Constituição admite restrições mais severas ao direito à privacidade.

Nessa linha, o STF validou a possibilidade de requisição administrativa desses dados pelas autoridades competentes, sem a necessidade de controle judicial prévio, demonstrando uma mudança significativa de postura em relação ao rigor anteriormente adotado no julgamento da ADI 6.387/DF. De fato, neste caso, na colisão em sentido estrito entre os direitos fundamentais subjetivos à privacidade e à proteção dos dados e, de outro lado, o bem coletivo da segurança pública, prevaleceu a tutela deste último, desde que observados os requisitos legais e a proporcionalidade da medida, evidenciando uma solução que prioriza o interesse coletivo.

Neste mesmo ponto, quando o Supremo Tribunal Federal iniciou os debates no âmbito do Tema 1148 da repercussão geral em Plenário, tornou-se evidente, pelas manifestações dos Ministros, que a gravidade dos crimes em análise poderia justificar a intervenção do Estado na esfera da privacidade do indivíduo. Em diversas ocasiões, os magistrados fizeram referência expressa à aplicação do teste de adequação, necessidade e proporcionalidade em sentido estrito, concluindo pela possibilidade de mitigação desse direito fundamental em face do interesse coletivo representado pela segurança pública. Ressalta-se, contudo, que a decisão não foi acompanhada de fundamentação detalhada sobre o caso concreto, o que limita a apuração dos fundamentos do precedente.

A proposição de encaminhamento da tese pelo Ministro Alexandre de Moraes revela a intenção de ampliar o alcance da definição de dados sujeitos a fornecimento para fins de persecução penal. O magistrado propõe que sejam incluídos, além dos dados cadastrais, os registros de conexão e de aplicação da internet, compreendidos aqueles capazes de indicar a localização do usuário, bem como, em certa medida, os dados fornecidos voluntariamente às empresas de tecnologia. A sugestão, portanto, busca abarcar um espectro mais amplo de informações, não inicialmente previstos no Marco Civil da Internet:

> 1) É constitucional a requisição judicial de registros de conexão ou de registros de acesso a aplicativos de internet para fins de investigação criminal ou instrução processual penal, inclusive o fornecimento de dados pessoais por provedores, em cumprimento de medida de busca reversa por palavra-chave, com fundamento no art. 10 e no art. 22 da Lei 12.965/2014 (Marco Civil da Internet), desde que preenchidos os requisitos de (a) fundados indícios de ocorrência do ilícito; (b) motivação da utilidade dos registros solicitados para fins de investigação ou instrução probatória; (c) período ao qual se referem os registros.
> 2) A ordem judicial poderá se referir a pessoas indeterminadas, mas determináveis a partir de outros elementos de provas, obtidos previamente na investigação e que justifiquem objetivamente a medida, desde que necessária, adequada e proporcional,

> justificando-se, ainda, a inexistência de outros meios menos invasivos para obter tais informações e a conveniência da medida em relação à gravidade do delito investigado. 3) A determinação judicial conterá, com precisão, os indexadores utilizados para a busca pretendida na base de dados do provedor, devendo a suspeita estar suficiente e formalmente fundamentada, de maneira proporcional. Esses indexadores podem envolver tanto as palavras-chave pesquisadas por indivíduos como determinações geográficas e temporais da busca[273].

Analisando detidamente a proposta do Ministro, percebe-se, ainda, certa imprecisão na abrangência dos dados a serem objeto de requisição. Essa incerteza conceitual acarreta incongruências, inclusive quanto ao tratamento jurídico conferido aos mandados de geolocalização. Em diversas oportunidades, as Cortes afastaram aplicação da Lei de Interceptação Telefônica sob o fundamento de que os dados de geolocalização seriam equivalentes a dados meramente cadastrais, contidos nos relatórios das Estações Rádio-Base, dispensando, por decorrência lógica, a observância dos rigorosos requisitos previstos naquela norma. Paradoxalmente, no entanto, ao fundamentar a legitimidade de medidas intrusivas, como sugerido no item 2, os magistrados recorreram justamente aos requisitos e fundamentos próprios da interceptação telefônica, como a indispensabilidade da medida, além do Marco Civil da Internet, o que revela uma inconsistência normativa e argumentativa contida na jurisprudência.

No que se refere ao fundamento dos mandados de geolocalização, reitera-se que o artigo 10 do Marco Civil da Internet estabelece que a guarda e a disponibilização de registro de conexão, de acesso a aplicações de internet, de dados pessoais e do conteúdo de comunicações privadas devem observar, de forma rigorosa, a proteção da intimidade, da vida privada, da honra e da imagem das partes envolvidas. O artigo 22 da mesma lei delimita que apenas ***os registros de conexão e os registros de acesso a aplicações de internet*** podem ser requisitados por ordem judicial para fins de formação de conjunto probatório em processo penal, não abrangendo, portanto, dados pessoais sensíveis, nem o conteúdo das comunicações.

Por sua vez, o Decreto n.º 8.771/2016, ao regulamentar o Marco Civil, impôs cautelas adicionais no tratamento de dados cadastrais quando requeridos por autoridades administrativas, vedando expressamente o atendimento a solicitações genéricas ou coletivas, nos termos do §3º do artigo 11. Esse rigor normativo em relação a dados que, em tese, possuem menor grau de sensibilidade, reforça o entendimento de que, por maior razão, dados pessoais relevantes como aqueles relacionados à geolocalização retrospectiva não podem ser objeto de

[273] BRASIL. Supremo Tribunal Federal. Tema 1148. Proposta de tese apresentada pelo Min. Alexandre de Moraes. Recurso Extraordinário n.º 1.301.250. Brasília, DF, 16 out. 2024. Disponível em: https://portal.stf.jus.br/jurisprudenciaRepercussao/verAndamentoProcesso.asp?incidente=6059876&numeroProcesso=1301250&classeProcesso=RE&numeroTema=1148. Acesso em: 19 de jun. 2025.

requisição generalizada, ainda que por autoridades judiciais. Essa cautela decorre não só da natureza mais invasiva dessas informações, mas da necessidade de preservar o núcleo essencial do direito à privacidade e à proteção de dados pessoais frente à atuação do Estado.

Além disso, os prazos e tipos de dados que podem ser objeto de guarda são definidos de forma taxativa pelo Marco Civil da Internet. O artigo 13 obriga os provedores de conexão a manterem os registros de conexão pelo prazo de um ano, enquanto o artigo 15 impõe aos provedores de aplicações de internet o dever de manter registros de acesso às suas aplicações pelo período de seis meses. Em ambos os casos a guarda se limita aos registros definidos no artigo 5º da Lei. Não há, portanto, previsão legal que obrigue provedor ou prestadores de serviços a manter registros ou outros dados pessoais que permitam a reconstrução de deslocamentos ou a identificação geográfica pretérita dos usuários. Admitir interpretação extensiva da lei nesse ponto significaria criar, por via hermenêutica, um regime de retenção massiva e indiscriminada, dissociado de finalidade específica e ilegítimo. Esse cenário converteria, em última análise, todos os usuários da internet no Brasil em potenciais suspeitos, já que seus dados, ainda que de conexão ou de acesso a aplicações, estariam armazenados, de forma generalizada, por períodos de um ano ou seis meses, independentemente de qualquer vínculo prévio com a investigação criminal ou de necessidade concreta para apuração de ilícitos.

Apenas a título de exercício argumentativo, destinado a estressar as hipóteses possíveis, imagina-se o caso do homicídio da vereadora Marielle Franco. Para se delimitar o perímetro correspondente ao local dos disparos, partiu-se da premissa de uma restrição do universo de pessoas potencialmente relacionadas ao fato, presentes em determinada área geográfica do Rio de Janeiro no momento do crime. Entretanto, essa restrição só se mostrou viável porque, em uma última análise, havia acesso à informação sobre a totalidade dos usuários com aparelhos celulares móveis naquela localidade. Esse fato pressupõe, por decorrência lógica, a prévia retenção e disponibilização de dados abrangendo todos os usuários, independentemente de qualquer suspeita inicial. Esse exemplo ilustra que, na ausência de filtros efetivos e de finalidade específica delimitada, corre-se o risco de considerar todos os cidadãos como potenciais suspeitos até que a delimitação geográfica permita um recorte mais preciso. Isto posto, o Marco Civil da Internet, cuja natureza é assegurar direitos e garantias no ambiente digital, poderia ser indevidamente convertido em um instrumento de vigilância e de retenção massiva de dados, incompatível com os princípios do Estado Democrático de Direito.

A evolução do entendimento no STF remete ao debate havido em Portugal, ainda quando da análise da Diretiva da Retenção de Dados 2006/24/CE e a respectiva Lei de Retenção

de Dados (Lei n.º 32/2008). Como bem salientou Francisco Coutinho[274], os metadados possuem um elevado potencial informativo, sendo capazes de revelar aspectos da vida privada de um indivíduo com riqueza de detalhes, muitas vezes superiores ao próprio conteúdo das comunicações. A identificação de padrões de comportamento, deslocamentos, relações pessoais e hábitos pode ser traçada a partir desses dados, o que torna a retenção indiscriminada de metadados uma grave ameaça ao direito à privacidade e à proteção de dados pessoais.

Como ventilado no presente trabalho, o debate no ordenamento jurídico português, ainda que o autor Coutinho atribua avanços e retrocessos na discussão travada entre o Tribunal Constitucional português e o Tribunal de Justiça da União Europeia, ficou estabelecido que a retenção de dados não pode ocorrer de forma geral e indiscriminada, sem vínculo a uma finalidade específica e legítima. Esse processo traduziu-se em um aperfeiçoamento do sistema de proteção de dados naquele país, pautado por critérios de proporcionalidade e necessidade em sua acepção mais estrita.

Diante desse contexto, Portugal, ao identificar os riscos de uma legislação que impunha a retenção indiscriminada de dados cadastrais, adotou uma postura de contenção, aprimorando os critérios e as finalidades dos mandados que autorizam a quebra de sigilo. Paralelamente, a União Europeia, ao declarar a invalidade da Diretiva 2006/24/CE, consolidou o entendimento que até os metadados[275], por permitirem inferências relevantes[276], podem assumir a natureza de dados pessoais pertinentes a uma esfera íntima, o que impulsionou uma revisão estrutural de normas de proteção de dados, a GPDR, e combinando na edição da Lei n.º 18/2024, em Portugal. No Brasil, de modo oposto, persiste um cenário de fragmentação, em que avanços jurisprudenciais buscam suprir, nem sempre harmonicamente, lacunas não vislumbradas pelo texto legal.

Isso evidencia que, embora haja um reconhecimento formal do valor *prima facie* da proteção de dados pessoais, suas fronteiras e a definição do núcleo essencial desse direito oscilam de forma casuística no âmbito das Cortes, o que fragiliza o juízo axiológico quanto à sua real relevância no exercício da ponderação entre os princípios em colisão.

Propõe-se, portanto, que o ordenamento jurídico brasileiro desenvolva um marco normativo específico e detalhado, capaz de disciplinar de maneira clara os requisitos materiais

---

[274] **COUTINHO, Francisco Pereira. Data Retention in Portugal: Big Brother is (No Longer) Watching**. 2023. Disponível em: <https://papers.ssrn.com/abstract=4216870>. Acesso em: 16 jun. 2025.

[275] *Ibid*.

[276] WACHTER, Sandra; MITTELSTADT, Brent. **A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI**. Columbia Business Law Review, v. 2019, p. 494, 2019. Disponível em: <https://heinonline.org/HOL/Page?handle=hein.journals/colb2019&id=506&div=&collection=>.

e procedimentais para acesso e tratamento de dados pessoais, inclusive os chamados dados meramente cadastrais e metadados, no âmbito das investigações criminais. Esse marco deve, em primeiro plano, consolidar o direito fundamental à proteção de dados como garantia autônoma, cuja restrição só se justifica mediante observância da reserva legal e de jurisdição. A disciplina normativa deve dialogar com os parâmetros da Lei Geral de Proteção de Dados e do Marco Civil da Internet, inspirando-se, também, na sistemática da lei de interceptação telefônica, que consagra o caráter excepcional e restrito de medidas dessa natureza.

Para dados pretéritos, compreendendo dados cadastrais e de localização obtidos a partir de registros de conexão ou de inferências, o acesso poderá ocorrer mediante decisão judicial fundamentada, desde que demonstrada a necessidade da medida para a investigação. Por outro lado, para o compartilhamento e tratamento de dados em tempo real ou futuros, especialmente aqueles que envolvam a dinâmica de localização ou outros dados sensíveis, deverá ser exigida decisão judicial que comprove: (a) fundada suspeita e indícios de ocorrência do ilícito, não relacionados a crimes digitais; (b) motivação da utilidade dos registros solicitados para fins de investigação ou instrução probatória se referir a pessoas indeterminadas, mas determináveis a partir de outros elementos de provas, obtidos previamente na investigação e que justifiquem objetivamente a medida; (c) desde que necessária, adequada e proporcional; (d) a inexistência de outros meios menos invasivos.

Essa proposta visa harmonizar o necessário equilíbrio entre a tutela dos direitos fundamentais dos cidadãos e as demandas legítimas da persecução penal, prevenindo abusos e garantindo maior segurança jurídica às decisões que autorizem o acesso a dados pessoais. Ao conferir maior precisão e densidade normativa ao tema, o marco regulatório pretendido contribuiria para fortalecer a proteção do núcleo essencial do direito fundamental à proteção de dados no Brasil, assegurando que eventuais restrições sejam efetivamente excepcionais, devidamente motivadas e compatíveis com os princípios do Estado Democrático de Direito.

CONCLUSÃO

Guiada pelo objetivo geral delineado, a trajetória percorrida ao longo desta pesquisa proporcionou a identificação de achados relevantes, os quais suscitam debates que exigem elevado critério técnico e metodológico, amparados nos alicerces da teoria dos direitos fundamentais. Esse rigor visa obstar a mera utilização instrumental de conceitos ou exploração seletiva de noções clássicas, impondo ao pesquisador o dever de buscar a compreensão dos fundamentos epistêmicos que informam o direito, a fim de evitar reduções simplificadoras que desaguem em discursos retóricos e carentes de densidade científica.

No percurso inicial da pesquisa, partindo dos eventos ocorridos em 8 de janeiro de 2023, na Praça dos Três Poderes, que motivaram a escolha do tema, projetava-se no projeto que o principal desafio na análise da constitucionalidade do mandado de geolocalização consistiria na inadequada mensuração da importância dos direitos fundamentais vinculados à privacidade, proteção de dados e autodeterminação informativa. Esperava-se identificar falhas na preservação do núcleo essencial dessas garantias constitucionais e, diante disso, reforçar o dever de se resolver a colisão em sentido estrito entre esses direitos e a necessidade de manutenção da segurança pública. Para tanto, aplicaram-se os testes de adequação, necessidade e proporcionalidade em sentido estrito, conforme a teoria de Robert Alexy.

Contudo, à medida que a revisão bibliográfica e o exame crítico das decisões judiciais avançaram, revelou-se que o problema a ser enfrentado não se limitava à harmonização entre direitos fundamentais em colisão. A celeuma emergida perpassava pela correta percepção do direito à proteção de dados e a natureza dessas informações que, por sua vez, determinariam o seu adequado tratamento. E, de fato, uma vez verificada a possibilidade de superação desta etapa, tornava-se evidente a necessidade de investigar os requisitos normativos e procedimentais que deveriam orientar a expedição dos mandados de geolocalização. O resultado final esperado destinava-se assegurar o respeito ao princípio da legalidade estrita, evitando que tais medidas se convertessem em instrumentos de produção indiscriminada de provas ou em expedientes de vigilância incompatíveis com os postulados do Estado de Direito.

Essa compreensão epistêmica permite superar a tentação da argumentação casuística, resguardando o compromisso com a lógica sistemática da unicidade da Constituição Federal, ancorada nos princípios estruturantes dessa ordem constitucional. A ausência de uma base principiológica sólida implicaria o risco de fragmentação da construção teórica diante da complexidade das interações entre os direitos fundamentais e os instrumentos normativos

destinados à sua concretização e restrição, abrindo espaço para soluções circunstanciais e desprovidas de coerência sistemática.

Diante da complexidade inerente à conceituação e delimitação da densidade normativa dos direitos fundamentais, adotou-se como referencial a teoria dos direitos fundamentais de Robert Alexy, a qual dialoga, em certa medida, com as formulações de Ingo Wolfgang Sarlet[277], que reconhecem na dignidade da pessoa humana o pilar axiológico da estrutura constitucional dos direitos fundamentais, assegurando a sua aplicabilidade e plena eficácia. Diante dessa perspectiva, os direitos fundamentais qualificam-se como mandamentos de otimização, cuja realização se dá na máxima medida possível frente as restrições fáticas e jurídicas existentes, entendimento esse acolhido pelo próprio Supremo Tribunal Federal em diversos julgados, como na ADI 4.923/DF[278], no HC 126.292/SP[279] e na ADI 3.937/SP[280]. Partindo desse pressuposto, impõe-se a análise da amplitude normativa do §1º do artigo 5º da Constituição Federal de 1988, que consagra aplicabilidade imediata das normas definidoras de direitos e garantias fundamentais. Nesse mesmo sentido, Sarlet[281], ao reconhecer o caráter principiológico da redação do citado parágrafo, exalta a necessidade de maximização de eficácia à função de defesa dos direitos subjetivos à liberdade, à igualdade e às garantias individuais, atribuindo-lhes, sem maiores digressões, a "*aplicabilidade imediata e justiciabilidade"*.

À luz desse quadro delineado, bem como conforme a avaliação das manifestações do Supremo Tribunal Federal contidas no Capítulo 4, conclui-se que o resultado da colisão em sentido estrito entre os direitos fundamentais subjetivos atinentes à proteção de dados e à privacidade tem conduzido, no plano jurisprudencial, à prevalência do bem coletivo da segurança pública sobre aqueles direitos. Esse resultado, entretanto, não implica necessariamente equívoco na ponderação realizada. Como ressalta Robert Alexy, há de se reconhecer a existência de uma margem de discricionariedade na atribuição de pesos aos

---

[277] SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional**. 10. ed. Porto Alegre: Livraria do Advogado, 2009.

[278] BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade n.º 4923. Relator: Min. Luiz Fux. Julgamento em 8 nov. 2017. Tribunal Pleno. Diário da Justiça Eletrônico, Brasília, DF, n. 64, p. 1, 5 abr. 2018. Disponível em: https://jurisprudencia.stf.jus.br/pages/search?base=acordaos&document=6532329. Acesso em: 14 jun. 2025.

[279] BRASIL. Supremo Tribunal Federal. Habeas Corpus n.º 126292. Relator: Min. Teori Zavascki. Julgamento em 17 fev. 2016. Tribunal Pleno. Diário da Justiça Eletrônico, Brasília, DF, n. 100, p. 1, 17 maio 2016. (RTJ, v. 238, n. 1, p. 118). Disponível em: https://jurisprudencia.stf.jus.br/pages/search?base=acordaos&document=6532331. Acesso em: 14 jun. 2025.

[280] BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade n.º 3937. Relator: Min. Marco Aurélio; Relator para o acórdão: Min. Dias Toffoli. Julgamento em 24 ago. 2017. Tribunal Pleno. Diário da Justiça Eletrônico, Brasília, DF, n. 19, p. 1, 1 fev. 2019. Disponível em: https://jurisprudencia.stf.jus.br/pages/search?base=acordaos&document=6532330. Acesso em: 14 jun. 2025.

[281] SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional**. 10. ed. Porto Alegre: Livraria do Advogado, 2009.

princípios em colisão, na medida em que, embora se deva perseguir uma resposta objetiva e racionalmente fundamentada, não há uma única solução correta ou absolutamente exata em todos os casos dessa natureza. Trata-se, portanto, de um exercício legítimo de ponderação, dentro dos limites do possível em um Estado Constitucional comprometido com a realização dos direitos fundamentais em harmonia com os interesses coletivos.

Restaria, então, examinar o dia seguinte desse juízo de ponderação, isto é, se os demais requisitos para a restrição de direitos fundamentais foram devidamente observados no contexto dessa mitigação. Nesse ponto, revisita-se a lição de Virgílio Afonso da Silva[282], que cogita, inclusive, a possibilidade de se atribuir caráter absoluto à reserva legal no âmbito do Direito Penal, destacando a centralidade desse princípio para proteção das liberdades individuais. O próprio autor, contudo, reconhece que essa tese não é pacífica, sendo objeto de intenso debate na doutrina especializada, especialmente diante do forte caráter dogmático da tese de que não há direito fundamental absoluto.

A pesquisa, dessa forma, buscou averiguar se o arcabouço normativo brasileiro legitima, de forma adequada e razoável, a intervenção na esfera da privacidade da proteção de dados, preservando, todavia, o núcleo essencial desse direito em consonância com o postulado do limite dos limites dos direitos fundamentais. É oportuno recordar, pela pertinência ao tema, a reflexão de Stefano Rodotà[283] sobre o impacto das circunstâncias fáticas e avanços tecnológicos na delimitação dos direitos fundamentais. O autor destaca que há um descompasso estrutural relevante entre a velocidade das inovações tecnológicas e a capacidade, significativamente mais lenta, das estruturas sociais e institucionais de adaptação a essas transformações. Essa simetria revela rápida obsolescência de soluções jurídicas elaboradas para responder a problemas técnicos específicos ou situações pontuais. Requer do legislador e do intérprete o dever de formular princípios gerais e orientadores que dialoguem com as transformações estruturais e de longo prazo, superando as limitações próprias de normas fragmentadas e casuísticas. Essa constatação, amplamente reconhecida na literatura especializada, reforça a urgência de uma base normativa dotada de flexibilidade densidade, capaz de oferecer respostas coerentes e eficazes aos desafios impostos pela sociedade da informação.

Essa constatação é particularmente relevante no contexto dos mandados de geolocalização, na medida em que, como se demonstrou ao longo deste trabalho, o direito à proteção de dados pessoais e à autodeterminação informativa no Brasil ainda não se consolidou de forma orgânica, como ocorreu em diversos países europeus. O sistema de proteção de dados

[282] SILVA, Virgílio Afonso da. **Direito constitucional brasileiro**. São Paulo: Edusp, 2021.
[283] RODOTÀ, Stefano. **A vida na sociedade da vigilância – a privacidade hoje**. Rio de Janeiro: Renovar, 2008.

no ordenamento jurídico brasileiro, até tempos recentes, apresentava uma estrutura fragmentada, marcada por legislações esparsas e fortemente influenciados por doutrina e jurisprudência estrangeiras. Essa carência de sistematização adequada gerou, nos pronunciamentos jurisdicionais, dificuldades na conceituação precisa de dados cadastrais, dados pessoais e dados pessoais sensíveis, bem como no enquadramento jurídico adequado das medidas de obtenção do conteúdo desses diversos tipos de informação. Por outro lado, a Lei Geral de Proteção de Dados, embora tenha representado um avanço significativo ao conferir maior sistematicidade e densidade à tutela dos dados pessoais, acabou tendo sua incidência afastada nos casos em exame, em razão de expressa exclusão prevista no seu próprio artigo 4º e incisos.

Assim, pragmaticamente, resta responder à pergunta proposta no presente trabalho: A expedição de mandados judiciais de geolocalização com fundamento no artigo 22 do Marco Civil da Internet, para investigação de crimes diversos daqueles previstos nos artigos 13-A e 13-B do Código de Processo Penal, configura violação ao princípio da legalidade estrita e aos direitos fundamentais à privacidade e à proteção de dados pessoais, especialmente quando envolve pessoas não diretamente relacionadas à conduta delituosa?

Essa pergunta revelou-se assertiva diante das nuances associadas ao tema. Os dados de geolocalização se inserem em uma zona de intersecção que podem ser visualizadas como a sobreposição dos diagramas de Venn. De um lado, tem-se os dados considerados meramente cadastrais e, de outro, os reputados como dados sensíveis. A conceituação jurídica atribuída à natureza desses dados é decisiva para delimitar a extensão dessa área de sobreposição e, por consequência, o regime de proteção que lhes será aplicado.

De fato, a localização de um indivíduo pode, em determinadas circunstâncias, ser inferida a partir do endereçamento de IP ou da triangulação dos sinais provenientes das Estações Rádio-Base (ERB’s). Nesses casos, os mandados de geolocalização seriam destinados às empresas de telecomunicações, restringindo-se à disponibilização de informações relativas aos registros de conexão, os quais poderiam possibilitar uma geolocalização inferida. De todo modo, as informações sobre as conexões às Estações Rádio-Base possuem finalidade, primariamente, ao controle de faturamento ou, em casos específicos, para localização da origem de chamadas de emergência, essas disciplinadas pelas Resoluções da Anatel. Essa finalidade específica não se converte em respaldo legal para a expedição de mandados geolocalização voltados à apuração de crimes diversos daqueles expressamente previstos nos artigos 13-A e 13-B do Código de Processo Penal. Ademais, as informações utilizadas para determinar a posição geográfica do usuário jamais poderiam ser classificadas como dados meramente cadastrais quando obtidas

por meio dos registros de aplicações de internet, em mandados dirigidos às empresas de tecnologia. Por sua natureza dinâmica, por envolver envio de dados e tratamento de informações pelas plataformas, bem como pelo potencial de revelar aspectos íntimos e detalhados da vida dos indivíduos, esses dados que possibilitariam a geolocalização ultrapassam o escopo dos registros cadastrais ou de informar apenas os aplicativos acessados e seus horários. O artigo 22 do Marco civil da Internet autoriza a requisição judicial apenas dos registros de conexão e de acesso a aplicações de internet, não abrangendo, de forma expressa, dados de geolocalização.

Assim, a obtenção de informações de localização por meio de mandados dirigidos a empresas de telecomunicações ou de tecnologia, quando fundamentada exclusivamente no artigo 22 do Marco Civil, não encontra respaldo legal suficiente, sobretudo em investigações que não envolvam os crimes expressamente previstos nos artigos 13-A e 13-B do Código de Processo Penal. A ausência de previsão legal clara para o uso desses dados em outros tipos de investigação configura violação ao princípio da legalidade estrita, segundo o qual toda restrição a direitos fundamentais deve estar prevista em lei. A interpretação extensiva do artigo 22 para abranger a geolocalização, sem base legislativa específica, extrapola os limites constitucionais e afronta diretamente os direitos à privacidade e à proteção de dados pessoais, transformando-se em norma de retenção massiva de dados. A coleta indiscriminada de informações de natureza pessoal, mesmo que por inferência, sem rigorosos critérios de delimitação temporal, espacial e subjetiva, expõe os titulares a riscos desproporcionais e danos irreversíveis à sua esfera privada.

Respondida a questão central que norteou o presente trabalho, as teses aqui desenvolvidas abrem espaço para reflexões complementares que merecem aprofundamento. Entre elas, destaca se a análise dos impactos dos dados de localização na presunção de inocência e no equilíbrio do conjunto dos elementos de prova. Importa investigar qual o valor jurídico e probatório deve ser atribuído às informações obtidas por meio de tecnologias de geolocalização, sobretudo quando utilizadas para embasar elementos de acusação ou, ao contrário, para fins de defesa.

Outra questão relevante diz respeito à legitimidade ética e jurídica da utilização do histórico de localização da vítima ou de terceiros em seu eventual desfavor, à semelhança do debate já travado sobre a admissibilidade da análise da vida pregressa. Além disso, suscita-se o questionamento acerca da compatibilidade de práticas do Estado e suas políticas públicas que associem, de forma generalizada, a incidência de delitos em determinadas regiões que acarretem a intensificação do policiamento ou a adoção de medidas repressivas mais severas, em nome da segurança pública.

Essas e outras problemáticas evidenciam os complexos desafios decorrentes da influência da tecnologia e da produção massiva e passiva de dados no cotidiano dos indivíduos, apontando para a necessidade de detida reflexão e maior contribuição da academia, de modo a assegurar que o avanço tecnológico não se transforme em instrumento de injustiça ou de erosão dos direitos fundamentais.

REFERÊNCIAS

ABREU, Jaqueline de Souza. **Guarda obrigatória de registros de telecomunicações no Brasil: sobre as origens da retenção de dados e as perspectivas para direitos fundamentais**. *In*: Anais do IV Simpósio Internacional LAVITS: Vigilância, Tecnopolíticas, Territórios**.** Salvador: LAVITS, 2016. Disponível em: <https://lavits.org/wp-content/uploads/2017/08/P5_De_Souza_Abreu.pdf>. Acesso em: 4 jun. 2025.

ALEXY, Robert. **Teoria da argumentação jurídica: a teoria do discurso racional como teoria da fundamentação jurídica.** 4ª. Rio de Janeiro: Forense, 2017.

ALEXY, Robert. **Teoria dos direitos fundamentais**. Tradução: Virgílio Afonso da Silva. 5ª ed. São Paulo : Malheiros Editora, 2008.

ALIMONTI, Veridiana. **Autodeterminação informacional na LGPD: antecedentes, influências e desafios**. *In*: CUEVA, Ricardo Villas Bôas; DONEDA, Danilo; MENDES, Laura Schertel (Orgs.). **Lei geral de proteção de dados (Lei nº 13.709/2018): a caminho da efetividade: contribuições para a implementação da LGPD [livro eletrônico]**. ePUB. São Paulo: Thomson Reuters Brasil, 2020.

ARISTÓTELES. **Clássicos da Filosofia: Cadernos de Tradução n.º 14 Metafísica, livros IV e VI**. Trad. Lucas Angioni. Campinas: Editora Unicamp, 2003.

AZEVEDO, Antonio Junqueira. **Entrevista: Antonio Junqueira de Azevedo**. RTDC: Revista Trimestral de Direito Civil, v. 9, n. abr./jun. 2008, p. 299–308, 2008.

AZEVEDO, Cynthia Picolo Gonzaga de; LIMA, Eliz Marina Bariviera de; SILVA, Felipe Rocha da; *et al*. **Nota técnica: análise comparativa entre o anteprojeto de LGPD penal e o PL 1515/2022**. [s.l.]: Instituto de Referência em Internet e Sociedade (IRIS); Laboratório de Políticas Públicas e Internet (LAPIN), 2022. Disponível em: <https://bit.ly/3U0OuU0>. Acesso em: 10 jun. 2025.

BADARÓ, Gustavo Henrique. **Processo penal**. 10. ed. São Paulo: Thomson Reuters Brasil, 2024. Disponível em: <https://next-proview.thomsonreuters.com/launchapp/title/rt/monografias/104402244/v12/page/I>. Acesso em: 16 maio 2025.

BARRETO, Alesandro Gonçalves. **eBook: Manual de Investigação Cibernética: à luz do Marco Civil da Internet**. 1. ed. Rio de Janeiro: Brasport, 2016. Disponível em: <https://www.editorabrasport.com.br/investigacao-cibernetica-e-book>. Acesso em: 12 jun. 2025.

BELTRÃO, Silvio Romero. **Direito Da Personalidade – Natureza Juridica, Delimitação Do Objeto E Relações Com O Direito Constitucional**. Dimensões Jurídicas da Personalidade na Ordem Constitucional Brasileira, n. 1, p. 203–228, 2013. Disponível em: <https://www.cidp.pt/revistas/ridb/2013/01/2013_01_00203_00228.pdf>.

BIONI, Bruno. **Proteção de dados pessoais**. 1. ed. Rio de Janeiro: Forense, 2019. Disponível em: https://www.lexml.gov.br/urn/urn:lex:br:rede.virtual.bibliotecas:livro:2019;001142886. Acesso em: 12 jun. 2025.

BOBBIO, Norberto. **As ideologias e o poder em crise: pluralismo, democracia, socialismo, comunismo, terceira via e terceira força**. Trad. João Ferreira. 3.ª ed. Brasília: Editora Universidade de Brasília, 1994.

BRASIL. Agência Nacional de Telecomunicações. **Resolução nº 738, de 21 de dezembro de 2020**. Altera o Regulamento dos Serviços de Telecomunicações para incluir disposições sobre sigilo, prevenção à fraude e ações de apoio à segurança pública. Disponível em: https://informacoes.anatel.gov.br/legislacao/resolucoes/2020/1495-resolucao-738. Acesso em: 05 jun. 2025.

BRASIL. **Constituição Federal**. 1988 Disponível em <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em 14 jun. 2018.

BRASIL. **Decreto n. 678, de 6 de novembro de 1992**. Promulga a Convenção Americana sobre Direitos Humanos (Pacto de San José da Costa Rica), adotada em 22 de novembro de 1969. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/dº0678.htm. Acesso em: 27 mai. 2025.

BRASIL. **Decreto-Lei nº 3.689, de 3 de outubro de 1941. Código de Processo Penal**. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 06 de maio de 2025.

BRASIL. **Lei n.° 9.296, de 24 de julho de 1996**. Dispõe sobre a interceptação de comunicações telefônicas de qualquer natureza, para fins de investigação criminal e instrução processual penal. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 24 mai. 2025.

BRASIL. **Lei n.° 12.965/2014, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 24 mai. 2025.

BRASIL. Supremo Tribunal Federal. **Sessão de julgamento – Tema 1148 – RE n.º 1.301.250/RJ – 16 out. 2024**. Participação dos Ministros Alexandre de Moraes e Cristiano Zanin. YouTube, 16 out. 2024. Disponível em: https://www.youtube.com/watch?v=tkGYtwsnR1c. Acesso em: 7 jun. 2025.

BRASIL. Supremo Tribunal Federal. **Sessão de julgamento – Tema 1148 – RE n.º 1.301.250/RJ – 23 abr. 2025**. Voto do Ministro André Mendonça. YouTube, 23 abr. 2025. Disponível em: https://www.youtube.com/watch?v=Gr7y0wV7W_A&t=4s. Acesso em: 7 jun. 2025.

CAIANIELLO, Michele. **Increasing Discretionary Prosecutor's Powers: The Pivotal Role of the Italian Prosecutor in the Pretrial Investigation Phase.** *In*: OXFORD HANDBOOKS EDITORIAL BOARD (Org.). **Oxford Handbook Topics in Criminology and Criminal Justice**. [s.l.]: Oxford University Press, 2012, p. 0. Disponível em: <https://doi.org/10.1093/oxfordhb/9780199935383.013.122>. Acesso em: 16 jun. 2025.

CARDONA, Tamires Diniz. **Sentidos de cuidado por educadores/cuidadores de crianças acolhidas institucionalmente**. Dissertação de Mestrado, Universidade Federal de Pernambuco, Recife, . Disponível em: <https://repositorio.ufpe.br/bitstream/123456789/39962/1/DISSERTA%C3%87%C3%83O%20Tamires%20Diniz%20Cardona.pdf>. Acesso em: 16 jun. 2025.

CASTELDELLI, Valine Silva. **Convenção de Palermo, tráfico de pessoas e geolocalização via sinais da estação rádio base: a gênese do art. 13-b do código de processo penal e a inserção sub-reptícia da violação à intimidade e vida privada na persecutio criminis brasileira**. Tese de Doutorado, Universidade Federal de Santa Catarina, Florianópolis, 2021.

CASTELLS, Manuel. **La interacció entre les tecnologies de la informació i la comunicació i la societat xarxa: un procés de canvi històric**. CONEIXEMENT I SOCIETAT, v. 1, p. 8–21, 2003. Disponível em: https://catalunyaeuropa.net/desigualtats/admin/assets/uploads/files/d7541-la_interaccio_entre_les_tecnologies_de_l.pdf. Acesso em: 28 abr. 2025.

CELESTE, Edoardo. **Constitucionalismo digital: mapeando a resposta constitucional aos desafios da tecnologia digital**. Direitos Fundamentais & Justiça, Trad. Paulo Rená da Silva Santarém. v. 15, n. 45, p. 63–91, 2021.

CHAPMAN, Brian. **Police State**. London: Macmillan Education UK, 1971. (Key Concepts in Political Science). Disponível em: <https://link.springer.com/book/10.1007/978-1-349-00944-2>. Acesso em: 16 jun. 2025.

CORDEIRO, Karine da Silva; SCHAFER, Jairo Gilberto. **Restrições a direitos fundamentais**. *In*: ASENSI, Felipe Dutra; PAULA, Daniel Giotti de (Orgs.). Tratado de Direito Constitucional: Constituição, política e sociedade. 1. ed. Rio de Janeiro: Elsevier, 2014, v. 1.

COUTINHO, Francisco Pereira. **Data Retention in Portugal: Big Brother is (No Longer) Watching**. 2023. Disponível em: <https://papers.ssrn.com/abstract=4216870>. Acesso em: 16 jun. 2025.

DONEDA, Danilo. **A LGPD como elemento estruturante do modelo brasileiro de proteção de dados**. *In*: CUEVA, Ricardo Villas Bôas; DONEDA, Danilo; MENDES, Laura Schertel (Orgs.). Lei Geral de Proteção de Dados (Lei nº 13.709/2018) [livro eletrônico]: a caminho da efetividade – contribuições para a implementação da LGPD. 1. ed. São Paulo: Thomson Reuters Brasil, 2020.

DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados**. 3. ed. São Paulo: Thomson Reuters Brasil, 2021.

DWORKIN, Ronald. **Levando os direitos a sério**. Trad. Nelson Boeira. São Paulo: Martins Fontes, 2002. (Justiça e direito).

FERRAJOLI, Luigi. **Direito e razão: teoria do garantismo penal**. [s.l.]: editora revista dos tribunais São Paulo, 2010.

FOUCAULT, Michel. **A Arqueologia do Saber**. Trad. Luiz Felipe Baeta Neves. 7. ed. Rio de Janeiro: Forense Universitária, 2009.

FOUCAULT, Michel. **A verdade e as formas jurídicas Tradução de Roberto Cabral de Melo Machado e Eduardo Jardim Morais**. Rio de Janeiro: NAU Editora, 2002.

FREITAS, Marcio Luiz Coelho de. **Privacidade no Direito Penal e o dilema da vigilância na era digital: a regulação da internet como instrumento de tutela de direitos fundamentais**. Tese de Doutorado, Universidade de Brasília, Brasília, 2022. Disponível em: <https://repositorio.unb.br/handle/10482/44262>. Acesso em: 16 jun. 2025.

FREITAS JÚNIOR, Horival Marques. **Repercussão geral das questões constitucionais**. Dissertação de Mestrado, Universidade de São Paulo, São Paulo, 2014. Disponível em: <http://www.teses.usp.br/teses/disponiveis/2/2137/tde-11022015-082405/>. Acesso em: 7 jun. 2025.

GARCIA, Rafael de Deus. **Processo penal e algoritmos: o Direito à privacidade aplicável ao uso de algoritmos no policiamento**. Tese (Doutorado em Direito), Universidade de Brasília, Brasília, 2022.

GETSCHKO, Demi. **As origens do Marco Civil da Internet**. *In*: LEITE, George S.; LEMOS, Ronaldo (Orgs.). Marco Civil da Internet. 1. ed. Rio de Janeiro: Atlas, 2014, p. 13. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788522493401/>. Acesso em: 5 jun. 2025.

GOMES, Luiz Flávio; CERNICCHIARO, Raúl. **Interceptação telefônica: lei 9.296, de 24.07.96**. São Paulo: Revista dos Tribunais, 1997.

KELLER, Clara Iglesias; PEREIRA, Jane Reis Gonçalves. **Data protection in times of Covid-19: the risks for surveillance in Brazil**. Internet Policy Review, 2020. Disponível em: <https://policyreview.info/articles/news/data-protection-times-covid-19-risks-surveillance-brazil/1462>. Acesso em: 28 abr. 2025.

KUJAWSKI, Fabio Ferreira; THOMAZ, Alan Campos Elias. **Da proteção aos registros, dados pessoais e comunicações privadas – um enfoque sobre o Marco Civil da Internet**. *In*: LEITE, George S.; LEMOS, Ronaldo (Orgs.). Marco Civil da Internet. 1. ed. Rio de Janeiro: Atlas, 2014, p. 27–30. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788522493401/>. Acesso em: 5 jun. 2025.

LANDAU, David. **Abusive Constitutionalism**. UC Davis Law Review, v. 47, p. 72, 2013.

LEITE, George S.; LEMOS, Ronaldo. **Marco Civil da Internet**. 1. ed. Rio de Janeiro: Atlas, 2014. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788522493401/. Acesso em: 5 jun. 2025.

LENSKI, Gerhard. **Power and Privilege: A Theory of Social Stratification**. New York: McGraw-Hill, 1966. Disponível em: <https://ia801402.us.archive.org/19/items/in.ernet.dli.2015.118923/2015.118923.Power-And-Privilege-A-Theory-Of-Social-Stratification.pdf>. Acesso em: 16 jun. 2025.

LEO, Guglielmo. **Le indagini sulle comunicazioni e sugli spostamenti delle persone: prime riflessioni riguardo alla recente giurisprudenza europea su geolocalizzazione e tabulati telefonici**. Sistema Penale, p. 19, 2021. Disponível em: <https://www.sistemapenale.it/pdf_contenuti/1622409272_leo-2021a-giurisprudenza-europea-geolocalizzazione-tabulati-indagini.pdf>. Acesso em: 3 jun. 2025.

LOPES JR., Aury. **Direito Processual Penal**. 22. ed. Rio de Janeiro: SRV, 2025. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788553625673/>. Acesso em: 12 maio 2025.

LOPES JR., Aury. **Direito processual penal**. 16. ed. São Paulo: Saraiva Educação, 2019. Disponível em: <https://cptl.ufms.br/files/2020/05/Direito-Processual-Penal-Aury-Lopes-Jr.-2019-1.pdf>. Acesso em: 16 jun. 2025.

LORENZONI, Pietro Cardia. **Jurisdição Constitucional de crise: análise e proposta hermenêuticas para a jurisdição constitucional extraordinária brasileira**. Tese de Doutorado, Universidade do Vale do Rio dos Sinos - Programa de Pós-Graduação em Direito, São Leopoldo, 2022. Disponível em: <https://www.repositorio.jesuita.org.br/bitstream/handle/UNISINOS/12688/Pietro%20Cardia%20Lorenzoni_PROTEGIDO.pdf?sequence=1&isAllowed=y>. Acesso em: 16 jun. 2025.

LYYTINEN, Kalle; YOO, Youngjin. **Ubiquitous computing**. Communications of the ACM, v. 45, n. 12, p. 63–96, 2002.

MARIA BEATRIZ SEABRA DE BRITO. **Novas tecnologias e legalidade da prova em processo penal: natureza e enquadramento do GPS como método de obtenção de prova.** Mestre, universiadade Nova de Lisboa, Lisboa, 2017. Disponível em: <http://hdl.handle.net/10362/31036>. Acesso em: 16 jun. 2025.

MCLUHAN, Marshall. **Os meios de comunicação: como extensões do homem**. [s.l.]: Editora Cultrix, 1974.

MENDES, Gilmar Ferreira. **Direitos fundamentais e controle de constitucionalidade: estudos de direito constitucional**. 4. ed. São Paulo: Saraiva, 2011.

MENDES, Gilmar Ferreira; COELHO, Inocêncio Mártires; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional**. 2. ed. São Paulo: Saraiva, 2008.

MENDES, Laura Schertel Ferreira. **Autodeterminação informativa: a história de um conceito**. Revista de Ciências Jurídicas Pensar, v. 25, n. 14, p. 1–18, 2020.

MOLON, Alessandro. **Marco Civil da Internet, uma construção da sociedade**. *In*: LEITE, George S.; LEMOS, Ronaldo (Orgs.). Marco Civil da Internet. Rio de Janeiro: Atlas, 2014, p. xxvii–xxx. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788522493401/>. Acesso em: 5 jun. 2025.

NUCCI, Guilherme de S. **Curso de Direito Processual Penal**. 21. ed. Rio de Janeiro: Forense, 2024. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786559649280/. Acesso em: 12 maio 2025.

NUNES, D. H.; DE SOUZA LEHFELD, L. C. **Cidadania Digital: Direitos, Deveres, Lides Cibernéticas E Responsabilidade Civil No Ordenamento Jurídico Brasileiro**. Libertas: Revista de Pesquisa em Direito, v. 4, n. 2, 2018. Disponível em: <https://periodicos.ufop.br/libertas/article/view/1300>. Acesso em: 16 jun. 2025.

NUNES, D.; MARQUES, A. L. P. C. **Inteligência artificial e direito processual: vieses algorítmicos e os riscos de atribuição de função decisória às máquinas**. Revista dos Tribunais Online, Revista de Processo, v. 285, p. 421–447, 2018.

OLIVEIRA, Luciano. Não fale do Código de Hamurábi. **A pesquisa sócio-jurídica na pós-graduação em Direito**, 2004.

OLIVEIRA, Marco Aurélio Bellizze; LOPES, Isabela Maria Pereira. **Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018**. *In*: FEIGELSON, Bruno; SIQUEIRA, Antonio Henrique Albani (Orgs.). Comentários à Lei Geral de Proteção de Dados: Lei 13.709/201. São Paulo: Thomson Reuters Brasil, 2019.

O'ROURKE, Mollye. **Fourth and Fifth Circuits Split Over Geofencing in Fourth Amendment Interpretation**. Lincoln Memorial University Law Review Archive, v. 12, n. 2, 2025. Disponível em: <https://digitalcommons.lmunet.edu/lmulrev/vol12/iss2/8>.

ORTELLADO, Pablo; RIBEIRO, Márcio Moretto; ZEINE, Letícia. **Existe polarização política no Brasil? Análise das evidências em duas séries de pesquisas de opinião**. Opinião Pública, v. 28, n. 1, p. 62–91, 2022. Disponível em: <https://periodicos.sbu.unicamp.br/ojs/index.php/op/article/view/8669212>. Acesso em: 17 jun. 2025.

OWSLEY, Brian L. **The best offense is a good defense: Fourth Amendment implications of geofence warrants**. Hofstra Law Review, v. 50, n. 4, 2022. Disponível em: <https://scholarlycommons.law.hofstra.edu/hlr/vol50/iss4/4>. Acesso em: 17 jun. 2025.

PEREIRA, Eliomar da Silva. **Teoria da investigação criminal**. 1. ed. São Paulo: Editora Almedina Brasil, 2010.

PEREIRA, Jane Reis G. **Interpretação constitucional e direitos fundamentais**. 2. ed. Rio de Janeiro: Saraiva Jur, 2017. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788553600281/>. Acesso em: 30 abr. 2025.

PINHEIRO, Guilherme Pereira; PINHEIRO, Alexandre Pereira. **COVID-19 e geolocalização: entre a saúde e a proteção de dados pessoais**. Revista Jurídica, v. 24, 2022. Disponível em: <https://doi.org/10.20499/2236-3645.RJP2022v24e132-2252>. Acesso em: 28 abr. 2025.

ROBL FILHO, Ilton Norberto. **Direito à intimidade e à vida privada na era digital**. *In*: **Democracia, direitos humanos e desenvolvimento sustentável: quais os desafios da Itália**

e do Brasil? Napoli: Editoriale Scientifica, 2024, p. 239–248. (Nuove autonomie, 30). Disponível em: <https://www.torrossa.com/en/resources/an/5844570>. Acesso em: 4 jun. 2025.

ROCHA, Maria João de Almeida. **A interseção entre a proteção de dados pessoais e a investigação criminal: contributo para uma análise jurídica crítica do regime aplicável ao tratamento de dados pessoais para fins de aplicação da lei**. Dissertação de Mestrado, Faculdade de Direito, Universidade de Lisboa, Lisboa, 2023. Disponível em: <https://repositorio.ulisboa.pt/bitstream/10451/61324/1/scnd_td_Maria_Rocha.pdf>. Acesso em: 3 jun. 2025.

RODOTÀ, Stefano. **A vida na sociedade da vigilância – a privacidade hoje**. Rio de Janeiro: Renovar, 2008.

ROSENVALD, Nelson; MONTEIRO FILHO, Carlos Edison do Rêgo. **Danos causados a dados pessoais: novos contornos**. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/332618/danos-causados-a-dados-pessoais--novos-contornos>. Acesso em: 29 abr. 2024.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional**. 10. ed. Porto Alegre: Livraria do Advogado, 2009.

SARLET, Ingo Wolfgang. **Proteção de dados pessoais como direito fundamental na Constituição Federal brasileira de 1988: contributo para a construção de uma dogmática constitucionalmente adequada**. Direitos Fundamentais e Justiça, v. 14, 2020. Disponível em: <https://dfj.emnuvens.com.br/dfj/article/view/875>. Acesso em: 22 abr. 2025.

SCHENK, Leonardo Faria. **Breve relato histórico das reformas processuais na Itália: um problema constante: a lentidão dos processos cíveis**. Revista Eletrônica de Direito Processual, v. 2, 2008. Disponível em: <https://www.e-publicacoes.uerj.br/redp/article/view/23735>. Acesso em: 2 jun. 2025.

SILVA, Virgílio Afonso da. **Direito constitucional brasileiro**. São Paulo: Edusp. 2021.

SILVA, Viviani Ghizoni; SILVA, Philipe Benoni Melo e; ROSA, Alexandre Morais da. **Fishing expedition e encontro fortuito na busca e apreensão**. Florianópolis: EMais, 2019.

SIQUEIRA, Dirceu Pereira; ROCHA, Maria Luiza de Souza; SILVA, Rodrigo Ichikawa Claro. **Atividades notariais e registrais, judicialização e acesso à justiça: o impacto da desjudicialização para a concretização dos direitos da personalidade**. Revista Jurídica Cesumar – Mestrado, v. 18, p. 305–355, .

SPANGHER, Giorgio. **Il processo penale dopo trent'anni**. **Sovrastrutture retrospettive**. Archivio Penale, 2020. Disponível em: <https://archiviopenale.it/File/DownloadArticolo?codice=9153b659-2351-4337-92ed-72f65aa42fa4&idarticolo=21714>. Acesso em: 2 jun. 2025.

STRECK, Lênio Luiz. **Verdade e consenso: constituição, hermenêutica e teorias discursivas**. [s.l.]: Saraiva Educação SA, 2014.

TAMANAHA, Brian Z. **On the rule of law: History, politics and theory**. Reino Unido: Cambridge University Press, 2011.

TEPEDINO, Gustavo; OLIVIA, Milena Donato. **Fundamentos de Direito Civil - Vol. 1 - Teoria Geral do Direito Civil**. 5. ed. Rio de Janeiro: Forense, 2024. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788530994471>. Acesso em: 18 jun. 2025.

TOFFOLI, José Antonio Dias. **Gravações ambientais, interceptações telefônicas e escutas no processo penal.** *In*: MENDES, Gilmar Ferreira; FREITAS, Matheus Pimenta de (Orgs.). **C**onstituição, Direito Penal e Novas Tecnologias. São Paulo: Almedina, 2024, p. 127. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788584936496/>. Acesso em: 4 jun. 2025.

WACHTER, Sandra; MITTELSTADT, Brent. **A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI**. Columbia Business Law Review, v. 2019, p. 494, 2019. Disponível em: <https://heinonline.org/HOL/Page?handle=hein.journals/colb2019&id=506&div=&collection=>.

WARREN, Samuel; BRANDEIS, Louis. **The Right to Privacy**. Civilistica.com, v. 2, n. 3, p. 1–22, 2013. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/127>. Acesso em: 18 jun. 2025.

WILDER-SMITH, Annelies; FREEDMAN, David O. **Isolation, quarantine, social distancing and community containment: pivotal role for old-style public health measures in the novel coronavirus (2019-nCoV) outbreak**. Journal of Travel Medicine, v. 27, 2020.

ZAGURSKI, Adriana Timoteo dos Santos. **Backlash: uma reflexão sobre deliberação judicial em casos polêmicos**. REVISTA DA AGU, 2017. Disponível em: <https://revistaagu.agu.gov.br/index.php/AGU/article/view/926>. Acesso em: 18 jun. 2025.

ZANATTA, Rafael Augusto; BIONI, Bruno Ricardo; IGLESIAS KELLER, Clara; *et al*. **Os dados e o vírus: tensões jurídicas em torno da adoção de tecnologias de combate à Covid-19**. Revista Brasileira de Direitos Fundamentais & Justiça, v. 14, p. 231–256, 2020. Disponível em: <https://doi.org/10.30899/dfj.v14i1.1031>. Acesso em: 26 abr. 2025.

ZUBOFF, Shoshana. **Big Other: Surveillance Capitalism and the Prospects of an Information Civilization**. Journal of Information Technology, v. 30, p. 75–89, 2015.