



**UNIVERSIDADE DE BRASÍLIA
FACULDADE DE DIREITO**

IARA SALGADO MUSSEL SANTOS CRIZÓSTIMO

**A PROTEÇÃO DOS DADOS PESSOAIS NA PERSECUÇÃO PENAL: LIMITES,
DESAFIOS E O RESGATE DA FRATERNIDADE COMO PARADIGMA
REGULATÓRIO**

*The Protection of Personal Data In Criminal Prosecution: Limits, Challenges and The
Recovery of Fraternity as a Regulatory Paradigm*

Brasília
2025

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE DIREITO

**A PROTEÇÃO DOS DADOS PESSOAIS NA PERSECUÇÃO PENAL: LIMITES,
DESAFIOS E O RESGATE DA FRATERNIDADE COMO PARADIGMA
REGULATÓRIO**

Autor: Iara Salgado Mussel Santos Crizóstimo

Orientador: Prof. Dr. Reynaldo Soares da Fonseca

Monografia apresentada como requisito
parcial à obtenção do grau de Bacharel, no
Programa de Graduação da Faculdade de
Direito da Universidade de Brasília.

Brasília
2025

FOLHA DE APROVAÇÃO

IARA SALGADO MUSSEL SANTOS CRIZÓSTIMO

A Proteção dos Dados Pessoais na Persecução Penal: Limites, Desafios e o Resgate da Fraternidade como Paradigma Regulatório

Monografia apresentada como requisito parcial à obtenção do grau de Bacharel, no Programa de Graduação da Faculdade de Direito da Universidade de Brasília.

Aprovada em: ____ de _____ de _____.

BANCA EXAMINADORA

Prof. Dr. Reynaldo Soares da Fonseca
(Orientador – Presidente)

Marja Mühlbach
Mestre
(Membro)

Alexandre Satyro de Medeiros
Mestre
(Membro)

AGRADECIMENTOS

Esta monografia representa não apenas a conclusão do curso de Bacharelado em Direito, mas a concretização de uma jornada com muitos desafios, aprendizados, superação e crescimento pessoal e profissional. Por isso, é com profundo reconhecimento que faço estes agradecimentos àqueles que, de diferentes formas, contribuíram para que este projeto se concretizasse.

Primeiramente, a meus avós, Tássio e Gleice, que foram os grandes pilares da minha trajetória. Com generosidade, coragem e amor, me proporcionaram todas as condições para que eu pudesse me dedicar aos estudos e conquistar o ingresso na Universidade de Brasília, no curso de direito. Cada conquista minha carrega força, valores e ensinamentos que recebi deles. Esta monografia é fruto do esforço e da fé que depositaram em mim.

A minha mãe, Ceres, mesmo à distância, sempre presente em minha vida com amor, palavras de encorajamento e fé no meu caminho. Sua força, exemplo e carinho incondicional foram essenciais para que eu chegasse até aqui. Cada conquista minha carrega um pouco de tudo o que aprendi com você, mesmo que de longe.

Ao meu pai, Leandro, agradeço profundamente por todo o apoio, pelos conselhos sempre sábios e pela confiança em minha trajetória. Sua orientação profissional foi essencial em muitos momentos de dúvida, e sua presença firme me trouxe segurança para seguir em frente. Obrigada por ser exemplo de integridade, dedicação e sabedoria.

Ao meu companheiro, Guilherme, agradeço pelo apoio constante e pela paciência nos momentos difíceis. Sua presença, escuta e palavras de encorajamento foram fundamentais para que eu conseguisse manter a serenidade e a motivação ao longo deste caminho. Obrigada por caminhar ao meu lado com tanto amor e compreensão.

Ao meu orientador, Reynaldo Soares da Fonseca, pela dedicação, paciência e valiosas contribuições ao longo do processo de elaboração deste trabalho e também por suas valiosas lições em sala de aula, nas matérias de Processo Penal e Direito de Fraternidade, as quais me inspiraram para a pesquisa.

Aos membros da banca examinadora, Alexandre Satyro e Marja Mühlbach, por aceitarem, acompanharem e avaliarem o meu trabalho. Agradeço também pelas lições dadas em sala de aula, muito proveitosas e construtivas.

Aos meus amigos, agradeço pela presença constante, pelas palavras de incentivo e, sobretudo, por todo apoio ao longo da trajetória universitária. Obrigada pelas conversas leves, pelas risadas nos dias difíceis e por me lembrarem que não estou sozinha nessa caminhada. A amizade de vocês foi um alívio e um impulso ao longo dessa jornada.

À toda equipe do Gabinete do Desembargador Diaulas Costa Ribeiro, pelas conversas, ensinamentos e colaboração diária que auxiliaram na minha trajetória profissional. Agradeço especialmente ao Roberto, por todo o acolhimento e amizade que construímos ao longo do estágio, por todos os conselhos profissionais e por todos os ensinamentos.

Ao Excelentíssimo Desembargador Diaulas Costa Ribeiro, minha sincera gratidão pela confiança, exemplo de retidão e generosidade intelectual. A convivência diária e os ensinamentos transmitidos na prática foram fundamentais para o meu crescimento profissional e acadêmico. É uma honra poder aprender sob sua orientação.

Por fim, a todos aqueles que direta ou indiretamente contribuíram para minha jornada acadêmica e para a construção deste trabalho.

FICHA CATALOGRÁFICA

CIP - Catalogação na Publicação	
Sp	Salgado Mussel Santos Crizóstimo, Iara. A Proteção dos Dados Pessoais na Persecução Penal: Limites, Desafios e o Resgate da Fraternidade como Paradigma Regulatório / Iara Salgado Mussel Santos Crizóstimo; Orientador: Reynaldo Soares da Fonseca. Brasília, 2025. 71 f. Trabalho de Conclusão de Curso (Graduação - Direito) Universidade de Brasília, 2025. 1. Constitucionalismo Digital. 2. Proteção de Dados Pessoais. 3. Persecução Penal. 4. LGPD Penal. 5. Fraternidade. I. Soares da Fonseca, Reynaldo, orient. II. Título.

REFERÊNCIA BIBLIOGRÁFICA

CRIZÓSTIMO, Iara Salgado Mussel Santos. (2025). A proteção dos dados pessoais na persecução penal: limites, desafios e o resgate da fraternidade como paradigma regulatório, dissertação ou tese. Monografia Final de Curso, Faculdade de Direito, Universidade de Brasília, Brasília, DF, 71 p.

Sumário

INTRODUÇÃO	11
1. O CONSTITUCIONALISMO DIGITAL E A PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO FUNDAMENTAL	12
1.1. O Constitucionalismo Digital	13
1.2. Os desafios da proteção de dados no constitucionalismo digital	18
1.3. Panorama histórico da proteção de dados pessoais	23
1.4. O Direito à Proteção de Dados como Direito Fundamental	29
2. A INVESTIGAÇÃO CRIMINAL NO CONTEXTO DIGITAL	32
2.1. Novas Tecnologias e a Persecução Penal	33
2.2. O anteprojeto de LGPD penal e o PL 1.515/2022: entre a eficiência e a proteção dos direitos fundamentais	47
3. A REGULAMENTAÇÃO DOS DADOS PESSOAIS NO PROCESSO PENAL SOB A ÓTICA FRATERNAL	55
3.1. A aplicação jurídica da fraternidade na civilização tecnológica	56
3.2. A fraternidade como resposta aos desafios na persecução penal na era digital	61
CONSIDERAÇÕES FINAIS	63

RESUMO

A monografia em questão tem como objetivo analisar o impacto do uso das novas tecnologias na persecução penal, tendo em vista a recente inserção do direito fundamental à proteção de dados pessoais no rol de direitos fundamentais pela Emenda Constitucional nº 115/2022. Parte-se da construção da teoria do constitucionalismo digital como base para equilibrar as transformações tecnológicas com a proteção dos direitos fundamentais no ambiente virtual. Em seguida, a pesquisa destaca os desafios relacionados ao uso de dados e algoritmos na persecução penal, evidenciando o risco de discriminação algorítmica, seletividade penal e violações à proteção de dados pessoais. Além disso, examina-se criticamente o anteprojeto da LGPD Penal e o PL nº 1.515/2022, realizando uma análise comparativa entre os dois. Propõe-se a fraternidade como um paradigma regulatório capaz de orientar a atuação estatal na era digital. O estudo adota uma abordagem interdisciplinar e normativa, com ênfase na compatibilidade entre a inovação tecnológica e os direitos fundamentais, em especial à proteção de dados pessoais, propondo um modelo de persecução penal fraterno.

Palavras-chave: proteção de dados pessoais, persecução penal, constitucionalismo digital, discriminação algorítmica, LGPD Penal, PL 1515/2022, fraternidade, direitos fundamentais.

ABSTRACT

The present monograph aims to analyze the impact of the use of new technologies in criminal prosecution, in light of the recent inclusion of the fundamental right to the protection of personal data in the list of fundamental rights by Constitutional Amendment N° 115/2022. It begins with the construction of the theory of digital constitutionalism as a foundation to balance technological transformations with the protection of fundamental rights in the virtual environment. The research then highlights the challenges related to the use of data and algorithms in criminal prosecution, emphasizing the risks of algorithmic discrimination, penal selectivity, and violations of personal data protection. Furthermore, it critically examines the draft bill of the Penal LGPD and Bill N° 1,515/2022, offering a comparative analysis between the two. Fraternity is proposed as a regulatory paradigm capable of guiding state action in the digital age. The study adopts an interdisciplinary and normative approach, with emphasis on the compatibility between technological innovation and fundamental rights, especially the protection of personal data, proposing a fraternal model of criminal prosecution.

Key-words: personal data protection, criminal prosecution, digital constitutionalism, algorithmic discrimination, penal LGPD, bill n°. 1515/2022, fraternity, fundamental rights.

Lista de Tabelas

Tabela 1	–	Análise Comparativa Anteprojeto LGPD Penal e PL nº 1.515/2022.....	53
----------	---	--	----

Lista de Siglas e Abreviaturas

ADI	Ação Direta de Inconstitucionalidade
APL	Anteprojeto de Lei
ARE	Recurso Extraordinário com Agravo
CDC	Código de Defesa do Consumidor
CF	Constituição Federal
CNJ	Conselho Nacional de Justiça
EC	Emenda Constitucional
GDPR	General Data Protection Regulation
GPS	Global Positioning System
HC	Habeas Corpus
IP	Internet Protocol
LGPD	Lei Geral de Proteção de Dados
MCI	Marco Civil da Internet
ONU	Organização das Nações Unidas
PL	Projeto de Lei
RE	Recurso Extraordinário
RHC	Recurso Ordinário em Habeas Corpus
RIPD	Relatório de Impacto de Proteção de Dados
STF	Supremo Tribunal Federal
STJ	Superior Tribunal de Justiça

INTRODUÇÃO

A era digital transformou significativamente as dinâmicas sociais, políticas e jurídicas. No contexto da revolução informacional, o ultra processamento de dados impactou a estruturação das relações sociais, econômicas e estatais. Desse modo, os dados pessoais tornaram-se ativos estratégicos de poder e elementos sensíveis da personalidade humana. Com esse cenário, emergem desafios relacionados à proteção dos direitos fundamentais na era digital, principalmente no que se refere à atuação estatal no exercício de seu poder punitivo.

A promulgação da Emenda Constitucional nº 115/2022 incluiu a proteção de dados pessoais no rol dos direitos fundamentais, o que representa um marco normativo significativo na consolidação de uma nova racionalidade constitucional. Desse modo, o constitucionalismo digital emerge como uma vertente teórica que busca dar respostas às mudanças estruturais provocadas pela era digital, propondo a reafirmação dos valores fundamentais do Estado Democrático de Direito no ciberespaço.

No âmbito da persecução penal, a utilização das tecnologias, como dados pessoais e algoritmos são de extrema necessidade no combate à criminalidade, nas investigações e na automação dos processos. Todavia, a utilização de ferramentas como o reconhecimento facial e a geolocalização suscitam preocupações quanto à violação da intimidade, à discriminação algorítmica, à seletividade penal e ao enfraquecimento das garantias constitucionais, como o devido processo legal, a ampla defesa, a dignidade da pessoa humana e a proteção dos dados pessoais.

Diante desse contexto, a monografia propõe uma análise crítica sobre os limites e os desafios da proteção de dados pessoais na persecução penal brasileira. Para tanto, parte-se do reconhecimento do direito à proteção de dados como direito fundamental autônomo e propõe-se a construção de um modelo regulatório inspirado na fraternidade, compreendida como valor constitucional e paradigma ético-jurídico capaz de orientar a atuação estatal no contexto digital.

Nesse percurso, serão analisados o desenvolvimento normativo da proteção de dados no ordenamento jurídico brasileiro e no direito comparado, a análise teórica do constitucionalismo digital como resposta às novas formas de poder informacional, os riscos decorrentes da utilização ilimitada das tecnologias na persecução penal e as propostas legislativas em trâmite, com destaque para o anteprojeto da LGPD Penal e o PL nº 1.515/2022. Ao final, busca-se afirmar a necessidade de um modelo de persecução penal que utilize as novas tecnologias com base na fraternidade, compatibilizando a inovação com os fundamentos axiológicos do Estado Democrático de Direito.

1. O CONSTITUCIONALISMO DIGITAL E A PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO FUNDAMENTAL

As novas tecnologias impuseram desafios substanciais à dogmática constitucional, especialmente no que tange à privacidade, à intimidade e, mais recentemente, aos dados pessoais. A digitalização da vida humana alterou sinteticamente a dinâmica social, e, desse modo, gerou desequilíbrios entre os sujeitos de direito e o Estado, fazendo emergir novas formas de poder, centralizadas nas mãos de grandes corporações tecnológicas e nas estruturas estatais. Neste contexto, o constitucionalismo digital emerge como uma resposta teórica e normativa às mutações sociais provocadas pelo surgimento das relações sociais do ciberespaço.

Este capítulo tem por objetivo apresentar e delimitar o constitucionalismo digital como uma vertente teórica da teoria constitucional tradicional, porém centrada na proteção dos direitos fundamentais no ambiente virtual. A partir da análise das transformações estruturais causadas pelas tecnologias, busca-se compreender como o direito à proteção de dados pessoais emerge como um novo direito fundamental, com autonomia, e não como um desdobramento da privacidade.

A análise se inicia pela construção teórica do conceito de constitucionalismo digital, com base nas contribuições de autores como Edoardo Celeste, Gilmar Mendes, Victor Oliveira Fernandes, Reynaldo Soares da Fonseca, Ana Cláudia Rodrigues de Faria e Bruno Fernandes de

Paula. Em seguida, são abordados os aspectos históricos, conceituais e os fundamentos axiológicos que sustentam essa corrente.

Na sequência, será traçada a evolução da inserção do direito à proteção de dados pessoais no ordenamento jurídico brasileiro, dando destaque à Lei Geral de Proteção de Dados (LGPD), ao Marco Civil da Internet (MCI) e à Emenda Constitucional nº 115/2022, esta última responsável por elevar o direito à proteção de dados à condição de direito fundamental expresso.

Por fim, será realizada uma análise crítica da concepção do direito à proteção de dados como um direito autônomo, com base na doutrina constitucional contemporânea, nos ensinamentos de Ingo Wolfgang Sarlet e Danilo Doneda, realizando um paralelo com a dignidade da pessoa humana, a autodeterminação informativa e o controle dos fluxos de informação em sociedades digitalizadas.

A exposição proposta neste capítulo fornece o embasamento teórico para as discussões posteriores sobre os desafios da proteção de dados pessoais no processo penal, tema central desta monografia.

1.1. O Constitucionalismo Digital

Neste tópico, propõe-se analisar o conceito de constitucionalismo digital como concepção que servirá de base teórica para este trabalho com o objetivo de estabelecer uma relação contextual com o que será estudado nos seguintes capítulos.

A intensidade a qual as tecnologias avançam de maneira global reflete diretamente no mundo jurídico. Partindo-se da ideia de Norberto Bobbio¹, a adaptação às mudanças sociais é uma característica intrínseca dos ordenamentos jurídicos complexos, pois quando o direito não se adapta, surgem problemas que necessitam de intervenção para que se garanta a funcionalidade do sistema². Uma vez que o ciberespaço surgiu como um

¹ BOBBIO, Norberto. **Teoria do Ordenamento Jurídico**. 6. ed. Apresentação: Tércio Sampaio Ferraz Júnior. Tradução: Maria Celeste C. J. Santos; rev. téc: Cláudio de Cicco. Brasília: Universidade de Brasília. 1995.

² No capítulo 4 da obra de Bobbio, intitulado como “A completude do ordenamento jurídico”, o autor destaca que há um processo natural de envelhecimento dos códigos, ocasionado pela rápida transformação da sociedade. As mudanças sociais fazem com que as legislações

novo ambiente para interações, propagações e afirmações, as relações se transformaram. Com isso, a fim de garantir a funcionalidade do sistema jurídico e político, tornou-se necessário identificar as possíveis ameaças ao Estado Democrático de Direito, pois, através das tecnologias, iniciou-se uma nova disputa de poder econômico e político, em que agentes não estatais, como as *big techs*³, tornam-se as principais controladoras das relações.

Conforme Celeste⁴, os tempos atuais são considerados importantes para o Direito Constitucional, porque o sistema está reagindo às novas formas de controle, e dessa forma, gerando desafios para o Estado Democrático. Dessa forma, diversas medidas regulatórias emergiram para combater o desequilíbrio gerado pela tecnologia digital. Assim, o constitucionalismo digital se traduz em um conjunto de princípios, baseados nos princípios constitucionais, os quais irão fundamentar as normas emergentes no contexto digital. Sendo assim, a designação de constitucionalismo digital, para Celeste, vem de um declínio do constitucionalismo moderno, sendo, portanto, uma nova ideologia. Nesse sentido, o constitucionalismo digital não soluciona os desafios gerados pelas tecnologias, mas é um fio condutor das respostas, sendo a terminologia utilizada como “guarda-chuva que abrange as mais diversas iniciativas jurídicas e políticas, estatais e não-estatais, voltadas à afirmação de direitos fundamentais na internet”⁵

pareçam anacrônicas, insuficientes e inadequadas. Nesse sentido, pode-se realizar um paralelo com as mudanças que acontecem no momento atual. O surgimento das novas tecnologias, por ter gerado transformações significativas nas relações sociais, fez as legislações e os códigos parecerem insuficientes para o novo momento. Desse modo, tendo em vista que a adaptação é um elemento do direito, o ordenamento passa a acompanhar e atuar em cima das transformações.

BOBBIO, Norberto. **Teoria do Ordenamento Jurídico**. Apresentação: Tércio Sampaio Ferraz Júnior. Tradução: Maria Celeste C. J. Santos; rev. téc: Cláudio de Cicco. Brasília: Universidade de Brasília. 6. ed. 1995. p. 108-109.

³ *Big techs* são as empresas globais do setor de tecnologia da informação, as quais exercem influência econômica, política e social.

HECK, Ralph Leal. Algoritmos que nos governam: reflexões filosóficas sobre propriedades críticas da atual estrutura da revolução informacional. *Philosophos - Revista de Filosofia*, Goiânia, v. 29, n. 1, 2024. DOI: 10.5216/phi.v29i1.78173. Disponível em: <https://revistas.ufg.br/philosophos/article/view/78173>. Acesso em: 17 jul. 2025.

⁴ CELESTE, Edoardo. **Constitucionalismo Digital: Mapeando A Resposta Constitucional Aos Desafios Da Tecnologia Digital**. Direitos Fundamentais & Justiça, Belo Horizonte, ano 15, n. 45, p. 63-91, jul./dez. 2021.

⁵ MENDES, Gilmar; FERNANDES, Victor Oliveira. **Constitucionalismo Digital e Jurisdição Constitucional: uma agenda de pesquisa para o caso brasileiro**. *Revista Justiça do direito*, v. 3, n. 2, p. 6-51, maio-ago, 2020. p. 4.

Com o avanço das tecnologias, emergem desequilíbrios dignos de atenção, principalmente no que diz respeito à proteção dos direitos fundamentais e ao equilíbrio entre os poderes do Estado⁶. Primeiramente, a ampliação das formas de transmissão de informações gerou uma grande ameaça, pois interfere diretamente em todos os direitos fundamentais relacionados à informação, como a liberdade de expressão e a privacidade. O uso ilimitado das tecnologias digitais possui o condão de colocar esses direitos em risco real e concreto.

Em segundo lugar, os efeitos da era digital ultrapassam a esfera individual e interferem na estrutura do próprio Estado, sendo uma potencial ameaça para o equilíbrio entre os poderes. Grandes empresas de tecnologia passaram a deter um poder capaz de controlar o pensamento, refletindo em invasões mentais e manipulações, o que gera grandes impactos em um Estado, como por exemplo no resultado de eleições. Assim, a temática do surgimento das novas tecnologias é sensível e necessita de uma análise concreta e um direcionamento pelos poderes públicos, uma vez que, se negligenciadas, são capazes de afetar as relações privadas e também as públicas, interferindo diretamente nos fundamentos constitucionais.

Com esses aspectos, tem-se que o constitucionalismo digital é teoria base na proteção dos direitos fundamentais e no equilíbrio entre os poderes no contexto atual, o mundo digital. É através da tecnologia digital que as relações privadas e públicas vêm se modificando, e logo necessitam de novos fundamentos e novas proteções. Com essas mudanças, torna-se necessário gerar contramedidas normativas que sejam congruentes com a própria Constituição e eficazes no sistema.

Destaca-se que o constitucionalismo digital não é um conceito totalmente novo. Como elucida Edoardo Celeste⁷, com as transformações ocasionadas pelo surgimento da sociedade da informação, logo na década de 2000, o conceito de constitucionalismo informacional emerge com o entendimento de que os atores privados exercem poder sobre as informações através da tecnologia da informação. Assim, inicialmente, o

⁶ CELESTE, Edoardo. **Constitucionalismo Digital: Mapeando A Resposta Constitucional Aos Desafios Da Tecnologia Digital**. Direitos Fundamentais & Justiça, Belo Horizonte, ano 15, n. 45, p. 63-91, jul./dez. 202. p. 3.

⁷ *Ibid.*, p. 8.

conceito surge como uma contramedida do avanço privado na informação. Desse modo, Fitzgerald entende que o direito privado dos Estados exerce um papel constitucional central na limitação dos atores privados⁸, os quais começaram a se posicionar nas relações como detentores de poder da informação. Todavia, a teoria de Fitzgerald apresentou duas problemáticas. A primeira relacionada à dificuldade de submeter os atores privados à jurisdição do Estado, e a segunda, relacionada à transnacionalidade da informação, que dificulta a regulação, tendo em vista o possível choque de direito privado entre os Estados envolvidos.

Em outro viés, ainda nos anos 2000, Berman (2000) também considera a capacidade dos atores privados em controlar os códigos do ciberespaço como um potencial instrumento regulatório⁹. Berman, nessa perspectiva, analisa a possibilidade desses atores estarem sujeitos ao direito constitucional. Surge em sua teoria o conceito de constitucionalismo constitutivo, a qual se propõe ser uma solução para os problemas apontados na teoria de Fitzgerald, em que apesar da dificuldade de submeter os atores privados à jurisdição, o constitucionalismo constitui-se como um condutor para regular essas relações. Assim, no constitucionalismo constitutivo, a imperatividade constitucional deve ser estendida aos atores privados, não devendo os atores privados agirem sem qualquer limitação¹⁰. Portanto, percebe-se que desde o início da era digital, as teorias mostraram-se preocupadas com os efeitos que uma transformação sem limitações poderia gerar.

Na década posterior, Suzor (2010) desenvolve um estudo que toma como base as comunidades virtuais, mesclando as teorias de Fitzgerald e de Berman, sendo portanto uma teoria mista. Para ele, a regulação não deve vir exclusivamente do Estado ou dos entes privados¹¹. Ele argumenta que a liberdade da internet gerou uma utopia que deslegitimou as leis estatais, o

⁸ CELESTE, Edoardo. **Constitucionalismo Digital: Mapeando A Resposta Constitucional Aos Desafios Da Tecnologia Digital**. Direitos Fundamentais & Justiça, Belo Horizonte, ano 15, n. 45, p. 63-91, jul./dez. 2021. p. 8.

⁹ *Ibid.*

¹⁰ *Ibid.*

¹¹ FONSECA, Reynaldo Soares da; FARIA, Ana Cláudia Rodrigues de. **Os desafios do constitucionalismo Digital**. In: **Estudos Sobre As Aplicações Jurídicas Da Fraternidade – Uma Homenagem Aos Professores Reynaldo Soares Da Fonseca E Marcelo Navarro Ribeiro Dantas**. Editora Fundação Fênix. Porto Alegre, 2024. p. 34.

que gerou uma contraproposta de restringir o poder dos agentes privados na internet, além de limitar o poder político dos Estados. Assim, sua abordagem prevê uma limitação mista, tanto privada quanto pública.

Já no ano de 2015, Gill, Redeker e Gasser¹² publicam novo estudo acerca do constitucionalismo digital. Para eles, o desenvolvimento tecnológico e a quantidade de usuários crescendo de maneira descomunal fez com que fosse necessário desenvolver uma área voltada a defender e afirmar direitos humanos no ciberespaço, atingindo um novo patamar de proteção. Com isso, a linha argumentativa do constitucionalismo digital ganhou forma para fundamentar a necessidade de proteção dos direitos fundamentais no contexto digital. Assim, firmou-se como uma relação de limites da esfera pública e da esfera privada com o intuito de proteger a dignidade humana nos moldes do constitucionalismo.

À luz dessas exposições, Celeste propõe construir uma nova sistematização teórica da definição do constitucionalismo digital, a qual será utilizada como embasamento neste trabalho na análise da proteção de dados pessoais. Para Celeste, o constitucionalismo digital é uma “ideologia que visa estabelecer e garantir a existência de um quadro normativo para a proteção de direitos fundamentais e o equilíbrio de poderes no ambiente digital”¹³. Dessa forma, é composto por valores e princípios que norteiam a constitucionalização do ambiente digital, o qual consiste no “processo de produção de contramedidas normativas vis-à-vis à alteração do equilíbrio relativo do ecossistema constitucional produzido pela tecnologia digital”¹⁴. Abrange, portanto, tanto o âmbito nacional, que modifica o quadro jurídico interno, quanto o transnacional, que são normas desenvolvidas dentro de organizações regionais ou internacionais ou até mesmo quando Estados representam uma só unidade¹⁵.

¹² FONSECA, Reynaldo Soares da; FARIA, Ana Cláudia Rodrigues de. **Os desafios do constitucionalismo Digital**. In: **Estudos Sobre As Aplicações Jurídicas Da Fraternidade – Uma Homenagem Aos Professores Reynaldo Soares Da Fonseca E Marcelo Navarro Ribeiro Dantas**. Editora Fundação Fênix. Porto Alegre, 2024. p. 34.

¹³ CELESTE, Edoardo. **Constitucionalismo Digital: Mapeando A Resposta Constitucional Aos Desafios Da Tecnologia Digital**. Direitos Fundamentais & Justiça, Belo Horizonte, ano 15, n. 45, p. 63-91, jul./dez. 202. p. 17.

¹⁴ *Ibid.*

¹⁵ *Ibid.* p. 21-22.

Ainda, Gilmar Mendes¹⁶ entende que o constitucionalismo digital corresponde a uma corrente teórica do Direito Constitucional contemporâneo, em harmonia com a conceituação de Celeste.

Portanto, conceituar o constitucionalismo digital é crucial para o que será explorado nos próximos tópicos, no que se relacionam aos desafios à proteção de dados pessoais e o papel de medidas normativas adotadas no Brasil. O constitucionalismo digital, dessa forma, explica o surgimento de normas regulamentadoras da tecnologia digital, considerando-se restabelecer o *status quo* dos poderes e proteger os direitos fundamentais. A constitucionalização do ambiente digital é conceituada por Celeste como o processo de emergência das normas e é o que recentemente vem ocorrendo no Brasil e no mundo. Com isso, será analisada em sequência a criação das principais normas protetivas dos direitos fundamentais no Brasil.

1.2. Os desafios da proteção de dados no constitucionalismo digital

Diante da exposição acerca do surgimento do constitucionalismo digital como conceito, neste tópico será abordado quais são os atuais desafios que a nova ideologia enfrenta e quais mudanças ela ocasionou no ordenamento jurídico brasileiro.

Na era digital, o constitucionalismo enfrenta diversos desafios os quais demandam reflexão e busca por soluções nos parâmetros constitucionais. Nesse viés, destacam-se os desafios relacionados à privacidade, à liberdade de expressão e à regulação das plataformas digitais¹⁷. Especificamente, o presente trabalho dará enfoque aos desafios relacionados à privacidade, que se fragmentará no direito autônomo da proteção de dados pessoais.

De início, faz-se necessário realizar uma breve exposição acerca das gerações de normas de proteção de dados pessoais de acordo com o momento histórico em que surgiram, pois assim é possível perceber o

¹⁶ MENDES, Gilmar; FERNANDES, Victor Oliveira. **Constitucionalismo Digital e Jurisdição Constitucional: uma agenda de pesquisa para o caso brasileiro**. Revista Justiça do direito, v. 3, n. 2, p. 6-51, maio-ago, 2020.

¹⁷ FONSECA, Reynaldo Soares da; FARIA, Ana Cláudia Rodrigues de. Os desafios do constitucionalismo Digital. In: **Estudos Sobre As Aplicações Jurídicas Da Fraternidade – Uma Homenagem Aos Professores Reynaldo Soares Da Fonseca E Marcelo Navarro Ribeiro Dantas**. Editora Fundação Fênix. Porto Alegre, 2024. p. 37.

contexto atual e qual o âmbito das relações sociais que urge ser regulado. Isso, pois relacionar meramente a proteção de dados como uma evolução histórica da privacidade é uma “construção dogmática falha”¹⁸, uma vez que a proteção de dados tornou-se um direito fundamental autônomo que abrange as mais diversas áreas, não só a privacidade relacionada à individualidade.

Não é novidade que as inovações tecnológicas e o aumento do processamento de dados pessoais em rede mundial de computadores tornaram necessária a atualização dos direitos da personalidade, realizando uma mudança no paradigma vigente sobre o direito à privacidade¹⁹. Assim, o direito à proteção de dados pessoais se distanciou do direito à privacidade, pois este enquanto possui uma aplicação mais restrita às informações pessoais relacionadas à vida privada, a tutela dos dados pessoais passou a atuar de maneira mais ampla, considerando não só informações da vida privada individual, mas a personalidade como um todo dos indivíduos e dos grupos em que eles se inserem na sociedade da informação²⁰. A proteção de dados, dessa forma, pode ser aplicada para além da esfera individual, abrangendo também a esfera pública, como nas persecuções penais, uma vez que o poder público também é detentor de dados pessoais. Assim, surge o primeiro ponto a ser tratado neste estudo, qual seja a aplicação do direito fundamental à proteção de dados como um desafio da hodiernidade.

As normas sobre a proteção de dados sofreram mudanças em suas áreas de eficácia. As primeiras legislações surgiram na década de 1970 e foram reações diretas ao processamento de dados no âmbito público e privado. Constitui-se a primeira geração de normas, as quais surgiram no contexto do Estado Social forte, no qual buscava-se a eficiência da administração pública para a prestação das obrigações estatais. Para isso, foi necessário implementar bases de dados centralizadas. Todavia, a opinião pública logo foi de encontro com a proposta, pois identificaram que a coleta e o tratamento de dados poderia ser uma ameaça, pois a proteção à

¹⁸ FONSECA, Reynaldo Soares da; PAULA, Bruno Fernandes de. **Da privacidade à proteção de dados pessoais: fundamentos teóricos e evolução histórica**. *Ver-o-Direito: revista de direito público com ênfase na competência da justiça federal*, v. 4, n. 1, jul. 2021. p. 10.

¹⁹ *Ibid.*, p. 11.

²⁰ *Ibid.*, p. 12.

privacidade encontrava-se em um plano secundário, visto que o foco era garantir prestações sociais²¹.

Em uma reação à primeira geração, a segunda foi marcada pela relação direta entre a proteção de dados pessoais e a privacidade e a liberdade, além da criação de autoridades administrativas responsáveis pela coleta e tratamento. A partir da segunda geração, surge um elemento essencial da proteção de dados, a qual é base até os dias de hoje: o consentimento do titular²². Todavia, uma decisão do Tribunal Constitucional Alemão²³, em 1983, gerou relevante impacto e criou caminhos para a terceira geração. A Corte, em decisão sobre o censo demográfico (*Volkszählungsurteil*), reconheceu o direito à autodeterminação informativa, no qual o indivíduo, além de dar o consentimento ao tratamento dos dados, tem o poder de decidir os limites em que serão utilizados.

A partir disso, surgiram legislações para disciplinar a participação ativa dos cidadãos no tratamento de seus próprios dados, garantindo uma limitação no tratamento dos dados e em sua utilização, distanciando-se da inicial de consentimento do “tudo ou nada”²⁴, no sentido de poder ou não ser utilizados em sua totalidade. Com isso, o titular tornou-se essencial para delimitar o uso e a finalidade dos dados. Assim, o envolvimento do titular se tornou fundamental em todo o processo de tratamento. Contudo, a terceira geração mostrou-se utópica, uma vez que os cidadãos não chegavam a de fato interferir no processo²⁵.

Com esses desafios, a quarta geração de normas se destacou por fortalecer o controle do cidadão e por retirar do controle dos indivíduos alguns

²¹ FONSECA, Reynaldo Soares da; PAULA, Bruno Fernandes de. **Da privacidade à proteção de dados pessoais: fundamentos teóricos e evolução histórica**. *Ver-o-Direito*: revista de direito público com ênfase na competência da justiça federal, v. 4, n. 1, jul. 2021. p. 12.

²² *Ibid.*, p. 13.

²³ SCHWABE, Jürgen; MARTINS, Leonardo. **Cinquenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão**. Decisão do Tribunal Constitucional alemão de 1983. Montevideo: Konrad AdenauerStiftung, 2005, pp. 233-245. Disponível em: http://www.kas.de/wf/doc/kas_7738-544-1-30.pdf. Acesso em: 30 jun. 2025. p. 237

²⁴ FONSECA, Reynaldo Soares da; PAULA, Bruno Fernandes de. **Da privacidade à proteção de dados pessoais: fundamentos teóricos e evolução histórica**. *Ver-o-Direito*: revista de direito público com ênfase na competência da justiça federal, v. 4, n. 1, jul. 2021. p. 13.

²⁵ *Ibid.*

pontos relevantes do tratamento, como os dados sensíveis²⁶, os quais são aqueles que geram maior valor para o controle e tratamento, vez que possuem informações importantes capazes de direcionar processos decisórios. Dessa forma, pode-se notar que ao longo dos avanços tecnológicos, as normas de proteção tiveram âmbitos diferentes até chegar no paradigma atual, em que os dados são ativos econômicos relevantes para a iniciativa privada e o setor público, necessitando do consentimento e da participação ativa dos cidadãos no controle.

O contexto histórico em que o atual paradigma se insere é marcado pela tecnologia presente na rotina de vários cidadãos e que os meios de comunicação foram remodelados²⁷. Na hodiernidade, o contato com a internet e com as tecnologias começam bem antes da fase adulta. Em aproximadamente 20 anos (dos anos 2000 a 2020) o mundo vivenciou uma mudança repentina nas relações sociais, agora presentes e fortalecidas principalmente pelo mundo digital. Nesse contexto, os dados pessoais alimentam o novo mundo a todo momento e produzem informações capazes de modificar comportamentos, desde a escolha de uma roupa em uma loja *online* até a influência no processo eleitoral. O paradigma atual é bastante complexo, pois a vida digital já atingiu todos os setores da sociedade, trazendo vantagens e desvantagens, pois ao mesmo tempo que é o meio de trabalho de milhões de pessoas, é o meio que criminosos encontraram para realizar crimes cibernéticos. Ainda, ao mesmo tempo que favorece o acesso à informação, é um meio facilitador da desinformação e da alienação.

Portanto, o constitucionalismo digital enfrenta um desafio que vai além da proteção da privacidade no âmbito pessoal, pois enfrenta o desafio de proteger a própria democracia e a personalidade dos indivíduos. As normas protetoras dos dados pessoais, no atual paradigma, não são apenas uma abstenção, elas abrangem uma tutela coletiva inegociável. Assim, é

²⁶ FONSECA, Reynaldo Soares da; PAULA, Bruno Fernandes de. **Da privacidade à proteção de dados pessoais: fundamentos teóricos e evolução histórica**. *Ver-o-Direito*: revista de direito público com ênfase na competência da justiça federal, v. 4, n. 1, jul. 2021. p. 13.

²⁷ FUX, Luiz; FONSECA, Gabriel Campos Soares da. **Segurança da informação e proteção de dados como pressupostos para o Poder Judiciário na era digital: uma análise da Resolução CNJ 361/2020 e da Resolução STF 724/2020**. In: BARATA, Bruno; ALMEIDA, Laryssa; FROTA, Leandro. (Coord.). *Ensaio sobre a transformação digital no direito: estudos em homenagem ao Ministro Kássio Nunes Marques*. Brasília: OAB Editora, 2021.

importante se questionar e refletir acerca do paradigma atual, pois um dos principais desafios é garantir a proteção dos dados pessoais diante dos avanços tecnológicos nas diversas áreas. A coleta massiva de dados e os sistemas de vigilância e monitoramento violam, a cada dia, milhões de indivíduos em todo o mundo, sendo essa coleta utilizada para violar outros direitos.

Diante disso, o constitucionalismo digital é uma ideologia que deve fundamentar as normas emergentes reguladoras das relações digitais, pois não abrange somente as relações de direito privado, atingindo também as relações públicas bases de um Estado, como a própria democracia. Dado que a facilidade e a rapidez em que as informações e desinformações são disseminadas, a efetiva proteção dos dados pessoais é um desafio, tendo em vista a dificuldade de criar normas que contemplem todos os aspectos dos dados pessoais. Além disso, o ciberespaço criou um novo meio para o cometimento de crimes e o uso de dados para essa finalidade cresce a cada dia.

Com esses aspectos, relevante adentrar que, no Brasil, a Lei Geral de Proteção de Dados e o reconhecimento da proteção dos dados pessoais como direito fundamental são avanços legislativos importantes, porém insuficientes, visto que não abrangem toda a seara de proteção no contexto digital, como exemplo, a utilização dos dados na persecução penal. Todavia, as propostas legislativas atuais tendem a avançar para essa temática. E, com o intuito de estudar a base desses avanços, é importante destacar o panorama histórico da proteção de dados e qual o momento de proteção atual.

1.3. Panorama histórico da proteção de dados pessoais

A preocupação com a proteção dos dados pessoais não é recente. Este subcapítulo tem por objetivo realizar um panorama das principais legislações que instrumentalizam o desenvolvimento normativo da proteção de dados no Brasil, com intuito identificar os parâmetros nos quais elas são aplicadas e quais as lacunas ainda existentes.

O marco inaugural normativo surgiu na Alemanha, com a Lei de Proteção de Dados do estado alemão de Hesse, em 1970²⁸. A partir dela, a proteção de dados passou a estar associada a uma necessidade de proteger a privacidade e a liberdade individuais, sobretudo em razão da crescente capacidade tecnológica decorrente do processamento e armazenamento de informações, que passou a representar um risco aos direitos fundamentais.

O enfoque das legislações de proteção de dados atualmente está interligado aos marcos regulatórios europeus. Todavia, o caráter global do assunto fez com que se verificasse que existe um “núcleo duro” da proteção de dados, como aponta Daniel Doneda²⁹. Esse núcleo comum é resultante das diversas dinâmicas e influências não só da Europa, mas também dos Estados Unidos, o que evidencia uma tendência global de padronização dos fundamentos essenciais da proteção de dados.

O desenvolvimento tecnológico precoce e acentuado na Europa e nos Estados Unidos proporcionaram condições para que logo existissem problemas relacionados ao tratamento de dados. Doneda traz um referencial histórico importante para o entendimento do pioneirismo americano e europeu. A tutela da privacidade sempre esteve presente no contexto norte-americano, em instrumentos como o “The right to privacy”, de Samuel Warren e Louis Brandeis, de 1890³⁰. Ainda, o caso *Olmstead v. United States*³¹, de 1928, foi fundamental, pois, apesar de haver voto vencido de

²⁸ DONEDA, Danilo. **Panorama histórico da proteção de dados pessoais**. In: DONEDA, Danilo; MENDES, Laura Schertel; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz (coord.). Tratado de proteção de dados pessoais. 2. ed. Rio de Janeiro: Forense, 2023. p. 3.

²⁹ *Ibid.*, p. 5.

³⁰ “The right to privacy” é a doutrina que fundou o direito à privacidade no contexto do common law, especialmente nos Estados Unidos. Os avanços tecnológicos da fotografia instantânea e da imprensa passaram a atingir a vida privada das pessoas. Nesse contexto, os autores argumentam acerca da privacidade, no sentido de que ela precisava ser ampliada a fim de evitar a exposição indevida. Warren e Brandeis descrevem a evolução do direito à privacidade como um direito autônomo, embasado na personalidade.

WARREN, Samuel; BRANDEIS, Louis. **The right to privacy**. Harvard Law Review, v. 4, n. 5, p. 193-220, 15 dez. 1890. Disponível em: <https://civillistica.emnuvens.com.br/redc/article/download/127/97>. Acesso em: 1 de jul. de 2025.

³¹ Este caso foi um marco da Suprema Corte Norte-Americana, pois se discutiu a legalidade das escutas telefônicas feitas sem autorização judicial realizadas pela polícia na obtenção de provas. A Corte decidiu por 5 votos a 4 que não houve violação a Quarta Emenda, que protege contra buscas e apreensões. O voto de Brandeis foi histórico, pois argumentou que as escutas telefônicas violavam o espírito da emenda, mesmo que não fosse física. Além disso, argumentou que o avanço tecnológico exigia novas interpretações sobre a proteção constitucional à privacidade.

Brandeis, trouxe o início da mudança argumentativa na concepção do direito à privacidade frente aos avanços tecnológicos. Posteriormente outro caso emblemático veio à tona, o *Katz v. United States* em 1967³² no qual de fato houve a mudança e o reconhecimento de que o direito à privacidade vai além da esfera física do indivíduo e passa a ser analisada a partir da personalidade e do que a sociedade entende como razoável. No caso, ainda que se tratasse de ameaças ao governo, a interpretação que se deu é que os danos sofridos pela negligência da proteção da privacidade também devem ser considerados.

Nesses aspectos, desde a década de 60, nos Estados Unidos, percebe-se a preocupação com os avanços tecnológicos e a segurança individual. Outros países também mostraram suas preocupações. A Lei de Proteção de Dados do Estado alemão de Hesse, de 1970, conforme ilustra Doneda³³, pode ser considerada a pioneira na matéria. Herbert Burket³⁴ argumenta que essa lei era diferente das demais leis de proteção porque ela trouxe cláusulas de confidencialidade pela primeira vez, no mesmo nível de outras cláusulas que abordavam questões importantes, como conflitos de poder. Ou seja, pela primeira vez a proteção de dados foi tratada como uma cláusula autônoma, e não como mera decorrência do direito à privacidade.

Ainda, é importante destacar a mencionada decisão de 1983 do Tribunal Constitucional Alemão³⁵, pois ela foi fundamental para o

UNITED STATES. **Supreme Court of the United States. Olmstead v. United States**, 277 U.S. 438 (1928). Disponível em: <https://supreme.justia.com/cases/federal/us/277/438/>. Acesso em: 1 jul. 2025.

³² *Katz v. United States* redefiniu os limites da Quarta Emenda discutidos no caso *Olmstead v. United States*. A Corte decidiu por 7 votos a 1 que houve violação da Quarta Emenda, mesmo sem invasão física, pois no caso analisado em que houve instalação de dispositivos de escuta em uma cabine telefônica. No caso, foi reconhecido que a medida não foi razoável diante da expectativa de privacidade que a sociedade entende como razoável. Assim, rejeitou a tese do caso anterior no sentido da ausência de necessidade da invasão ser física. UNITED STATES. Supreme Court of the United States. **Katz v. United States**, 389 U.S. 347 (1967). Disponível em: <https://supreme.justia.com/cases/federal/us/389/347/>. Acesso em: 1 jul. 2025.

³³ DONEDA, Danilo. **Panorama histórico da proteção de dados pessoais**. In: DONEDA, Danilo; MENDES, Laura Schertel; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz (coord.). Tratado de proteção de dados pessoais. 2. ed. Rio de Janeiro: Forense, 2023. p. 8.

³⁴ BURKET, Hebert. **Privacy-Data Protection: a German/European perspective**. In.: ENGEL, C.; KELLER, K. H. (ed). Governance of Global Networks in the Light of Differing Local Values. Baden-Baden: Nomos, 2000. p. 46. Tradução livre.

³⁵ SCHWABE, Jürgen; MARTINS, Leonardo. **Cinquenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão**. Decisão do Tribunal Constitucional alemão de 1983 Montevideo: Konrad AdenauerStiftung, 2005, pp. 233-245. Disponível em: http://www.kas.de/wf/doc/kas_7738-544-1-30.pdf. Acesso em: 30 jun. 2025. p. 237

desenvolvimento do direito à proteção de dados pessoais, uma vez que foi reconhecido como uma garantia constitucional. No caso, era contestada uma lei federal que regia sobre atividade estatística do Estado, mais precisamente sobre o censo demográfico. A Corte reconheceu que o processamento de dados e informações detalhadas acerca dos cidadãos geram ameaças à privacidade e à liberdade individual. Por isso, reconheceu a necessidade do controle do indivíduo sobre suas próprias informações para a proteção da personalidade³⁶.

Ademais, em 1995, na Europa, a Diretiva 95/46/CE³⁷ foi adotada para promover a proteção das pessoas no que tange ao tratamento de dados pessoais e à livre circulação destes. A diretiva representou um importante passo na construção do direito à proteção de dados, pois estabeleceu princípios fundamentais como a legalidade e a transparência, a finalidade específica e a segurança. Além disso, logo no artigo 2º definiu o conceito de dados pessoais, tratamento dos dados pessoais, ficheiro de dados pessoais, responsável, subcontratante, terceiro, destinatário e consentimento. A definição do conceito, dos limites de aplicação, dos princípios e das categorias específicas do tratamento foram basilares para o início do novo paradigma da era digital. Em 2018, a Diretiva foi substituída pelo Regulamento Geral de Proteção de Dados, que inspirou a Lei Geral de Proteção de Dados brasileira³⁸.

Especificamente em relação ao contexto brasileiro, a construção normativa ocorreu de maneira gradual e mais recente. A primeira manifestação expressa relacionada a uma preocupação com dados pessoais ocorreu com o remédio constitucional do *habeas data*³⁹, que garante o direito

³⁶ DONEDA, Danilo. **Panorama histórico da proteção de dados pessoais**. In: DONEDA, Danilo; MENDES, Laura Schertel; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz (coord.). Tratado de proteção de dados pessoais. 2. ed. Rio de Janeiro: Forense, 2023. p. 9.

³⁷ UNIÃO EUROPEIA. 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. Jornal Oficial das Comunidades Europeias, L 281, p. 31-50, 23 out. 1995. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046>. Acesso em: 1 jul. 2025.

³⁸ DONEDA, Danilo. **Panorama histórico da proteção de dados pessoais**. In: DONEDA, Danilo; MENDES, Laura Schertel; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz (coord.). Tratado de proteção de dados pessoais. 2. ed. Rio de Janeiro: Forense, 2023. p. 5.

³⁹ Previsto no artigo 5º, LXXII, da CF/88, o *habeas data* se relaciona com a proteção de dados frente ao Estado, pois é um remédio constitucional que visa garantir o acesso a dados que estão sob guarda de órgãos públicos ou a retificação de dados incorretos.

de acesso e a retificação de dados pessoais. Posteriormente, o Código de Defesa do Consumidor⁴⁰ trouxe inovação normativa para a proteção de dados no ordenamento jurídico interno. O artigo 43 do CDC estabelece que é direito do consumidor acessar as informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes, o que condiz com a preocupação da retenção de dados por fornecedores, produtores e prestadores de serviço.

Após, a Lei do Cadastro Positivo⁴¹ foi a primeira norma a tratar de conceitos tradicionais da proteção de dados, com a inclusão de conceitos como o de dados sensíveis em seu artigo 3º, §3º, inciso II⁴². Ainda, a Lei de Acesso à Informação⁴³, em seu artigo 31⁴⁴, trouxe a transparência e o consentimento ao ordenamento.

⁴⁰ BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, ano 128, n. 176, p. 1, 12 set. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 1 jul. 2025.

⁴¹ BRASIL. **Lei nº 12.414, de 9 de junho de 2011**. Dispõe sobre a formação e consulta a bancos de dados com informações de adimplemento de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Diário Oficial da União: seção 1, Brasília, DF, ano 148, n. 109, p. 1, 10 jun. 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 1 jul. 2025.

⁴² Art. 3º Os bancos de dados poderão conter informações de adimplemento do cadastrado, para a formação do histórico de crédito, nas condições estabelecidas nesta Lei.

§ 3º Ficam proibidas as anotações de:

II - informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas.

⁴³ BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, ano 148, n. 222, p. 1, 18 nov. 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 1 jul. 2025.

⁴⁴ Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.

§ 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem:

I - terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e

II - poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem.

O Marco Civil da Internet⁴⁵ estabeleceu princípios, garantias, direitos e deveres dos usuários da rede no Brasil. Foi o primeiro instituto a incluir expressamente a proteção de dados pessoais “na forma da lei” como um dos princípios do uso da internet no país, em seu art. 3º, III. Embora limitada a eficácia normativa, o Marco Civil da Internet fortaleceu as bases para que fosse consolidada a LGPD⁴⁶, pois afirmou a necessidade de um diploma legal específico sobre o tema.

A promulgação da LGPD, com vigência em 2020, representou a consolidação da proteção de dados pessoais no ordenamento jurídico nacional. Inspirada no GDPR europeu, instituiu os fundamentos da proteção de dados, o âmbito de aplicação, os conceitos principais, os requisitos do tratamento dos dados pessoais, os direitos do titular, o tratamento de dados pelo poder público, a transferência internacional de dados, a fiscalização e a criação da Autoridade Nacional de Proteção de Dados e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade.

Importante salientar que, apesar de toda a construção da proteção de dados realizada pela LGPD, ela não abarcou acerca do tratamento de dados para fins de investigação criminal e segurança pública por uma opção do próprio Poder Legislativo⁴⁷. O artigo 4º, III⁴⁸, da referida lei exclui expressamente de seu escopo o tratamento de dados pessoais para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais. Essa lacuna

⁴⁵ BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União: seção 1, Brasília, DF, ano 151, n. 78, p. 1, 24 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 1 jul. 2025.

⁴⁶ BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: seção 1, Brasília, DF, ano 155, n. 157, p. 1-3, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 1 jul. 2025.

⁴⁷ CHUY, José Fernando Moraes. **O sistema de Investigação Brasileiro, a “LDGP Penal” e a Efetiva Garantia de Direitos Fundamentais**. p. 1. Disponível em: https://web.adpf.org.br/wp-content/uploads/2021/03/2-Artigo_JOSE-FERNANDO-MORAES-CHUY.pdf. Acesso em 2 de jul. 2025.

⁴⁸ Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:

III - realizado para fins exclusivos de:

- a) segurança pública;
- b) defesa nacional;
- c) segurança do Estado; ou
- d) atividades de investigação e repressão de infrações penais

legislativa em relação a essas matérias gera relevante impacto nos direitos fundamentais dos cidadãos e por isso será objeto de estudo neste trabalho.

Ademais, a constitucionalização da proteção de dados foi finalmente realizada com a Emenda Constitucional nº 115/2022⁴⁹, que inseriu esse direito expressamente no rol dos direitos fundamentais. É o marco definitivo do processo de amadurecimento do constitucionalismo digital brasileiro, pois assegura a proteção jurídica reforçada e reconhecida como um direito humano fundamental.

Esses três últimos instrumentos normativos, embora distintos em escopo e momento histórico, compõem um sistema que visa garantir a privacidade, a autodeterminação informativa e a segurança jurídica no ambiente digital, os quais são aspectos fundamentais para a funcionalidade do Estado Democrático de Direito no ambiente virtual. Para isso, a EC nº 115/2022 foi basilar, pois estabeleceu o mínimo que deve ser objetivado nesse contexto: a proteção dos dados pessoais.

Dessa forma, é necessário compreender constitucionalmente o direito fundamental à proteção de dados dentro de uma perspectiva sistemática⁵⁰, em diálogo com os demais direitos fundamentais, especialmente no que se refere à sua aplicação prática em diferentes esferas do ordenamento jurídico. A efetividade desse direito exige uma abordagem sistemática, integrada e multidisciplinar capaz de garantir sua observância mesmo diante de lacunas legislativas ou conflitos normativos.

1.4. O Direito à Proteção de Dados como Direito Fundamental

Em primeiro lugar, é necessário destacar que direitos humanos e direitos fundamentais não significam o mesmo. Conforme explica Ingo

⁴⁹ BRASIL. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Diário Oficial da União: Seção 1, Brasília, DF, 11 fev. 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 2 jul. 2025.

⁵⁰ SARLET, Ingo Wolfgang. **Fundamentos Constitucionais: o Direito Fundamental à Proteção de Dados**. In: DONEDA, Danilo; MENDES, Laura Schertel; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz (coord.). Tratado de proteção de dados pessoais. 2. ed. Rio de Janeiro: Forense, 2023. p. 26.

Wolfgang Sarlet⁵¹, os direitos humanos são aqueles reconhecidos e protegidos internacionalmente, em tratados e convenções, enquanto os direitos fundamentais são aqueles positivados dentro do âmbito constitucional de cada Estado. No entanto, há uma interseção entre eles: os direitos humanos, quando incorporados ao direito interno, adquirem o status de direito fundamental.

O direito à proteção de dados pessoais exemplifica essa dualidade. Embora não tenha sido originalmente previsto de forma expressa nos principais tratados internacionais da ONU ou nas convenções Europeias e Interamericana⁵², passou a ser reconhecido como um direito implicitamente consagrado. Posteriormente, foi catalogado no Regulamento Geral de Proteção de Dados da Europa, tornando explícita a vontade internacional de regular a proteção de dados no âmbito transnacional.

Partindo-se para o núcleo essencial dos direitos fundamentais, é possível abordá-lo sob dois aspectos: o material e o formal⁵³. No aspecto material, ou seja, considerando-se o conteúdo das normas, a proteção de dados se relaciona diretamente com a dignidade humana, a privacidade, a autonomia e a formação da personalidade. No formal, a consagração como direito fundamental depende da incorporação ao texto constitucional, como ocorreu no caso brasileiro por meio do rito das emendas constitucionais.

A conexão entre a proteção de dados e a dignidade da pessoa humana é particularmente relevante. Sarlet destaca que a dignidade é o fundamento axiológico central do Estado Democrático de Direito, e que o controle sobre os próprios dados é condição indispensável para o exercício da liberdade, da autonomia e da identidade pessoal. A proteção de dados, portanto, não apenas reforça a privacidade, mas também assegura a autodeterminação do indivíduo em relação às suas informações.

A concepção da proteção de dados a qual surgiu com a decisão do Tribunal Constitucional alemão sobre o Censo de 1983 foi essencial para firmar a concepção da autodeterminação informativa, que é base para a

⁵¹ SARLET, Ingo Wolfgang. **Fundamentos Constitucionais: o Direito Fundamental à Proteção de Dados**. In: DONEDA, Danilo; MENDES, Laura Schertel; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz (coord.). Tratado de proteção de dados pessoais. 2. ed. Rio de Janeiro: Forense, 2023. p. 30.

⁵² *Ibid.*, p. 28.

⁵³ *Ibid.*

proteção de dados. Essa concepção estabelece que cada indivíduo deve ter o controle sobre a coleta, o uso e a difusão de seus dados pessoais. Sendo assim, trata-se de um princípio com duas dimensões, a individual e a coletiva, que orienta tanto a proteção individual quanto a promoção de uma comunicação livre e democrática no ambiente digital. Acrescente-se que o exercício desse direito exige, como pressuposto constitucional, o consentimento livre e informado do titular de dados⁵⁴.

Importa destacar que, embora frequentemente associado ao direito à privacidade, o direito à proteção de dados possui, em verdade, um objeto jurídico mais amplo. Enquanto a privacidade visa proteger a intimidade e a vida privada, a proteção de dados abrange todo o ciclo da informação, desde a coleta até o tratamento e compartilhamento. Isso ocorre mesmo quando os dados não dizem respeito diretamente à intimidade, mas ainda assim impactam a dignidade e a liberdade do titular.

Dessa forma, o direito à proteção de dados pessoais deve ser compreendido como um direito fundamental autônomo, com base na dignidade humana, na privacidade e na autonomia, mas com escopo próprio e específico. Sua positivação constitucional no Brasil reflete o reconhecimento de que os dados pessoais, independentemente de seu conteúdo, derivam da própria personalidade do indivíduo. O tratamento indevido desses dados pode violar direitos fundamentais, tanto em sua dimensão individual quanto coletiva, exigindo, portanto, uma tutela jurídica robusta e eficaz. Tanto é, que a proteção de dados pessoais foi inserida no texto constitucional através da Emenda Constitucional 115/2022, atingindo um patamar além do infraconstitucional como era com a LGPD.

Diante da consolidação do direito à proteção de dados pessoais como um direito fundamental autônomo através de marcos normativos nacionais, percebe-se o surgimento de um novo paradigma jurídico sensível às transformações tecnológicas da hodiernidade. Nesse contexto, o constitucionalismo digital se apresenta como uma resposta às crises emergentes relacionadas às novas dinâmicas sociais. A nova

⁵⁴ SARLET, Ingo Wolfgang. **Fundamentos Constitucionais: o Direito Fundamental à Proteção de Dados**. In: DONEDA, Danilo; MENDES, Laura Schertel; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz (coord.). Tratado de proteção de dados pessoais. 2. ed. Rio de Janeiro: Forense, 2023. p. 31.

constitucionalidade impõe ao Estado e aos entes privados o dever de respeitar e garantir o controle dos indivíduos sobre seus dados pessoais, tendo em vista a coleta massiva de informações sensíveis. Assim, a compreensão da proteção dos dados pessoais como um instrumento de efetivação da dignidade humana revela-se ainda mais necessário quando tratada dentro da temática estatal de segurança pública e persecução penal, uma vez que há um grande risco de se extrapolar os limites constitucionais. É nesse aspecto que se insere o próximo capítulo, dedicado a examinar os desafios jurídicos existentes entre a persecução penal e o direito fundamental à proteção de dados.

2. A INVESTIGAÇÃO CRIMINAL NO CONTEXTO DIGITAL

A transformação digital impactou as relações econômicas, sociais e privadas, e provocou uma reconfiguração profunda das práticas estatais, em especial no campo da segurança pública e da persecução penal. A investigação criminal, na qual tradicionalmente se utilizavam mecanismos físicos de coleta de provas, se vê, hoje, diante de novas ferramentas e dinâmicas processuais, marcadas pelo uso de algoritmos, inteligência artificial, bases de dados e técnicas avançadas de vigilância. Nesse contexto, surgem questionamentos centrais acerca da compatibilidade dessas inovações com os direitos e garantias fundamentais, especialmente no que tange à proteção dos dados pessoais.

Este capítulo visa examinar os impactos das novas tecnologias na persecução penal à luz do direito fundamental à proteção de dados pessoais, construído no capítulo anterior. O ponto de partida é a análise das transformações tecnológicas e do surgimento do chamado regime algorítmico, que vem progressivamente substituindo o regime documental tradicional nas investigações criminais. As ferramentas digitais, tais como os softwares de reconhecimento facial, os sistemas de geolocalização, as bases de dados interoperáveis e os algoritmos de predição criminal, alteram profundamente as formas de produção de provas, reforçando, ao mesmo tempo, uma lógica de vigilância estatal que pode comprometer os princípios

do devido processo legal, do contraditório, da ampla defesa e da dignidade da pessoa humana.

Na sequência, será discutida a importância da proteção de dados e seus desdobramentos na persecução penal, com especial atenção para os riscos de seletividade penal e discriminação algorítmica, problemáticas que vêm sendo amplamente denunciadas pela criminologia crítica e pelas pesquisas empíricas recentes. Ademais, será feita uma análise de jurisprudências relevantes do STF e STJ que envolvem a temática e demonstram que a nova realidade tecnológica exige uma reinterpretação das cláusulas constitucionais clássicas.

Em razão da nova realidade, torna-se urgente a construção de limites jurídicos precisos ao tratamento de dados pessoais para fins penais, o que justifica o debate normativo em torno do Anteprojeto da LGPD Penal e do Projeto de Lei nº 1.515/2022, que visam disciplinar essa matéria sensível, ainda marcada por uma preocupante lacuna regulatória.

A partir dessa análise, pretende-se compreender como o direito à proteção de dados pessoais pode e deve atuar como limite jurídico à atuação do Estado na investigação penal em ambientes digitais, preservando a legalidade, a proporcionalidade e o respeito à dignidade da pessoa humana.

2.1. Novas Tecnologias e a Persecução Penal

Os avanços tecnológicos transformaram os modos de convivência social e a forma de produção do conhecimento. Nesse sentido, o progressivo desenvolvimento tecnológico contribui para a utilização dos dados pessoais além da esfera privada. Assim, atua o poder público, no âmbito da segurança pública e da persecução penal, visando aprimorar a eficiência e a eficácia das investigações e atuar na prevenção de crimes⁵⁵. Softwares dedicados à análise de relatórios policiais, registros de ocorrências, dados de criminalidade e a identificação de indivíduos visam prever crimes futuros e identificar possíveis localidades com maior probabilidade de ocorrência. Essa

⁵⁵ ARRUDA, Ana Julia Pozzi; RESENDE, Ana Paula Bougleux Andrade; FERNANDES, Fernando Andrade. **Sistemas de Policiamento Preditivo e Afetação de Direitos Humanos à Luz da Criminologia Crítica**, Revista de Direito Público, Brasília, v. 18, n. 100, p. 664-689, out.-dez. 2021. p. 664.

prática é conhecida como policiamento preditivo⁵⁶. Todavia, o uso das tecnologias tanto no policiamento preditivo, quanto no próprio processo penal, gerou um novo cenário, o qual necessita de atenção, pois a adoção crescente de mecanismos tecnológicos, embora otimizem o trabalho policial e forneçam respostas penais ao processo, suscitam profundas discussões sobre as garantias fundamentais, tendo em vista o potencial que possuem de violar os direitos e ampliar as desigualdades sociais.

Como o constitucionalismo digital surge como uma teoria norteadora dos novos modos de regulamentação das relações digitais, ele é aplicável também à persecução penal. O Estado, nessa perspectiva, diante do novo paradigma digital, possui um papel crucial para a proteção dos indivíduos, uma vez que a nova realidade produz efeitos sensíveis sobre os direitos fundamentais. Temáticas como a produção de provas no processo penal e o uso do reconhecimento facial nas atividades de policiamento são alvos de estudo, pois o uso irrestrito de dados e algoritmos nas investigações coloca em risco toda a construção que a Lei Geral de Proteção de Dados representa para o contexto atual.

Diante desse contexto, a Criminologia Crítica é essencial para analisar a problemática do policiamento preditivo e da discriminação algorítmica, pois evidencia as conexões entre o poder econômico e o sistema de justiça criminal⁵⁷. A Criminologia Crítica é a corrente teórica que questiona a introdução e o funcionamento do sistema jurídico-penal, observando que a economia e a sociedade podem reforçar o paradigma da dominação e os estereótipos do indivíduo infrator, o que contribui para a seletividade penal e a manutenção da ordem social desigual⁵⁸. A ideia difundida acerca da imparcialidade dos algoritmos é alarmante, pois, na verdade, frequentemente reproduzem padrões historicamente estruturados, que impõem logísticas de

⁵⁶ FERREIRA, André da Rocha. **Tratamento de dados pessoais em investigações criminais: o direito fundamental à autodeterminação informativa como limite constitucional**. Revista Brasileira de Ciências Criminais. vol. 185. ano 29. p. 115-159. São Paulo: Ed. RT, novembro 2021. p. 141.

⁵⁷ ARRUDA, Ana Julia Pozzi; RESENDE, Ana Paula Bougleux Andrade; FERNANDES, Fernando Andrade. **Sistemas de Policiamento Preditivo e Afetação de Direitos Humanos à Luz da Criminologia Crítica**, Revista de Direito Público, Brasília, v. 18, n. 100, p. 664-689, out.-dez. 2021. p. 666-667.

⁵⁸ *Ibid.*, p. 665-666.

controle social, as quais já existem no direito penal quando se trata da seletividade⁵⁹.

Em todo o contexto da era digital, o Direito Penal e o Processo Penal precisam das bases algorítmicas e das informações derivadas dos bancos de dados, pois assim como a vida social migrou para o ambiente digital, os delitos também passaram a ser praticados nele. O aumento do acesso instantâneo e da globalização fizeram com que o crime organizado, antes nacional, passasse a ter um caráter transnacional de maneira muito mais célere. De acordo com o Senado Federal, os crimes digitais subiram em 45% no ano de 2024⁶⁰, e, inclusive, em razão disso, o Senado possui propostas para diminuir a invasão de dados para práticas delituosas, o que revela uma preocupação estatal no aumento da criminalidade cibernética.

Todavia, a investigação dos crimes cibernéticos não é uma tarefa simples, pois exige o acesso a dados para a identificação de servidores e localizações. A persecução penal, com essa crescente, necessita que sejam observados princípios do constitucionalismo digital, a fim de que o próprio Estado não se torne um invasor de dados. No artigo de Rafael de Deus Garcia⁶¹, ele observa que o Estado se materializa e formaliza através dos documentos que gera a partir da engrenagem estatal, ou seja, os agentes estatais operam a máquina estatal e geram diversos efeitos na sociedade, os quais são compreendidos por ela de diversos modos. A ampliação dos processos tecnológicos no âmbito criminal afasta os cidadãos dos processos de decisão, uma vez que ao contrário do que teoricamente representam, os processos tecnológicos não são transparentes e são utilizados como uma forma de controle estatal⁶². Os algoritmos utilizados na esfera pública, desse modo, criam uma dinâmica de poder com opacidade técnica, baixa visibilidade e inacessibilidade, o que dificulta a sua contestação no processo penal.

⁵⁹ FERREIRA, André da Rocha. **Tratamento de dados pessoais em investigações criminais: o direito fundamental à autodeterminação informativa como limite constitucional**. Revista Brasileira de Ciências Criminais. vol. 185. ano 29. p. 115-159. São Paulo: Ed. RT, novembro 2021. p. 137.

⁶⁰ <https://www12.senado.leg.br/radio/1/noticia/2025/01/16/crimes-digitais-sobem-45-e-senado-tem-propostas-para-frear-sequestro-de-dados>. Acesso em 17 junho de 2025.

⁶¹ GARCIA, Rafael de Deus. **Um velho direito à privacidade para um novo tipo de policiamento: algoritmos e inteligência artificial no processo penal e na segurança pública**. 2021. p. 3.

⁶² *Ibid.*, p. 5.

Conforme elucida André Ferreira⁶³, o uso de dados pessoais e as tecnologias de processamento possuem potencial positivo em diversos aspectos, principalmente ao se observar a crescente da criminalidade no ambiente virtual. Adotar uma postura radical à utilização de dados pessoais nas investigações é inefetivo diante da complexidade dos crimes digitais. O que se torna necessário, em verdade, é utilizar os benefícios trazidos pela tecnologia e adotar mecanismos eficientes na proteção dos dados pessoais a fim de se evitar confrontos com o devido processo legal e o próprio direito fundamental à proteção de dados. O Brasil já possui atos normativos de proteção de dados, como explicitado no capítulo anterior, mas nenhum deles é específico para as questões criminais. O anteprojeto sobre o uso de dados na segurança pública foi o mais recente passo nesse sentido.

Em um primeiro momento, é importante destacar que o processo penal atravessa um momento de mudança de paradigma, no qual o regime documental está perdendo lugar para o regime algorítmico. Essa mudança, todavia, não deve ser feita sem qualquer questionamento. É necessário que o constitucionalismo digital seja usado como teoria para se estabelecer os critérios da imputabilidade penal, do acesso às provas, do exercício do contraditório e da ampla defesa, e que sejam eles resguardados diante da adoção de ferramentas tecnológicas, sob pena de esvaziar o processo penal de seus compromissos constitucionais.

A introdução do regime algorítmico na persecução penal tem gerado desequilíbrio nas garantias processuais mais relevantes, como o contraditório, a ampla defesa e o devido processo legal. A dança processual, em qualquer área do direito, é guiada não só pelo direito de ser ouvido, mas também nas prerrogativas de conhecer e poder contestar as razões que fundamentam as decisões. Conforme salienta Rafael de Deus Garcia⁶⁴, a lógica dos algoritmos foi projetada para ser inacessível, apesar de serem instituídos na gestão burocrática do Estado com o objetivo de aumentar a

⁶³ FERREIRA, André da Rocha. **Tratamento de dados pessoais em investigações criminais: o direito fundamental à autodeterminação informativa como limite constitucional**. Revista Brasileira de Ciências Criminais. vol. 185. ano 29. p. 115-159. São Paulo: Ed. RT, novembro 2021. p. 117.

⁶⁴ GARCIA, Rafael de Deus. **Um velho direito à privacidade para um novo tipo de policiamento: algoritmos e inteligência artificial no processo penal e na segurança pública**. 2021. p. 6.

transparência. Isso ocorre porque, como explica o autor, existem três elementos que os diferenciam dos documentos tradicionais do processo e que dificultam o acesso dos cidadãos aos elementos que podem ser utilizados contra eles⁶⁵.

O primeiro é a materialidade. Os documentos tradicionais podem ser fisicamente identificados, ao passo que os algoritmos atravessam a esfera da materialidade. Desse modo, não sendo palpáveis, a grande maioria dos indivíduos não possuem o fácil acesso à tecnologia que é capaz de alcançar e traduzir a linguagem informática. O segundo deles é a invisibilidade, pois os documentos podem ser escondidos, mas a sua apresentação material ainda é acessível, mesmo que sigilosa. Os algoritmos possuem alto grau de invisibilidade, mesmo quando apresentados e disponíveis. Isso ocorre devido à necessidade de um conhecimento técnico e específico, isto é, para que os dados utilizados nos algoritmos sejam visíveis e compreensíveis, é necessário um conhecimento técnico mínimo. Outro elemento é a temporalidade, pois o algoritmo é mais fluido e dinâmico, ao passo que o documento tradicional é estagnado no tempo em que foi assinado e publicado, sendo assim, por não possuir um elemento temporal identificável, torna-se difícil o acesso exato.

Com esses elementos, tem-se que o processo penal enfrenta desafios com a mudança de paradigma. Nas investigações, para o compartilhamento dos dados pessoais e o uso dos algoritmos, é necessário ponderar as ações estatais que visam o interesse público e empoderar o titular dos dados pessoais, o qual conforme a construção histórica retratada no capítulo anterior, possui o direito de consentir e limitar o uso dos próprios dados e a destinação da coleta⁶⁶. Luiz Fernando Rodrigues observa que para Mendroni⁶⁷, a autoridade policial e o Ministério Público devem utilizar dados para a investigação, porém, esses dados são obtidos de bases nas quais o

⁶⁵ GARCIA, Rafael de Deus. **Um velho direito à privacidade para um novo tipo de policiamento: algoritmos e inteligência artificial no processo penal e na segurança pública**. 2021. p. 6.

⁶⁶ RODRIGUES, Luiz Fernando. **A importância do compartilhamento de dados pessoais para fins de investigação criminal e os possíveis reflexos da LGPD**. In: ARAS, Vladimir B.; MENDONÇA, Andrey B.; CAPANEMA, Walter Aranha; SILVA, Carlos Bruno F. da; COSTA, Marcos Antônio da S. (Org.) *Proteção de Dados Pessoais e Investigação Criminal*. Ministério Público Federal. Brasília: ANPR, 2020. p. 442.

⁶⁷ MENDRONI, Marcelo Batlouni. **Curso de investigação criminal**. 3. ed. rev. e amp. São Paulo: Atlas, 2013.

cidadão não está ciente de que ao disponibilizar seus dados está disponibilizando-os também para fins de investigação, o que entra em conflito com o paradigma do consentimento.

A atividade de investigação criminal é destinada ao fornecimento de elementos mínimos sobre a autoria e a materialidade do delito, a fim de dar início à ação penal, pública ou privada. A troca de informações, na era da comunicação, é fundamental para as atividades de inteligência e para o controle social da atividade criminosa, ainda mais que as próprias comunicações facilitaram o aumento de delitos no ambiente digital. O acesso aos dados é de suma importância para as investigações, mas o uso sem limitações viola os direitos fundamentais e fomenta atividades discriminatórias do próprio Estado, enraizadas historicamente. E a partir disso, surge a atual crise do contraditório, em que o uso ilimitado dos dados reduz a possibilidade de contradizer as informações obtidas, a validade e as interpretações dos dados, o que prejudica o exercício da defesa, uma vez que as decisões baseadas na análise estatística dos dados é legitimada por ter sido obtida de fontes digitais.

André da Rocha Ferreira⁶⁸ traz em seu artigo que é praticamente impossível que um crime, atualmente, não deixe uma pegada digital, pois, assim como em qualquer outra atividade do cotidiano, em algum momento, o *inter criminis* passará pela internet, deixando informações de conexão, seja na própria consumação do delito nos crimes praticados na internet ou nos atos preparatórios. Por isso, coletar dados e utilizá-los é importante para as investigações criminais, pois é decisivo na solução de diversos crimes. É inegável o interesse público na utilização dos dados para fins de investigação criminal a fim de que possa se atingir a própria finalidade de averiguar a autoria e a materialidade dos delitos.

O problema central de toda essa temática é a legalidade do uso dos dados nas investigações criminais. Sabe-se que a operação de tratamento dos dados envolve uma série de atividades que são necessárias para as investigações, porém estão sujeitas aos limites constitucionais, mais

⁶⁸ FERREIRA, André da Rocha. **Tratamento de dados pessoais em investigações criminais: o direito fundamental à autodeterminação informativa como limite constitucional**. Revista Brasileira de Ciências Criminas. vol. 185. ano 29. p. 115-159. São Paulo: Ed. RT, novembro 2021. p. 120.

especificamente do próprio constitucionalismo digital. É uma questão complexa, que envolve um debate de diversas áreas do direito e das ciências sociais e políticas, mas é uma questão que urge regulamentação. A ausência de uma estrutura legal clara e precisa para o uso das tecnologias na investigação penal acarreta uma assimetria de poder que favorece o Estado em detrimento do investigado, porque é feito sem qualquer limite.

Ao utilizar dados cujo significado não é publicamente inteligível, devido aos elementos da imaterialidade, da invisibilidade e da atemporalidade concernentes aos algoritmos e aos dados, o sistema penal perde a postura garantista, a qual exige clareza, previsibilidade e possibilidade do contraditório. É uma mudança de paradigma que exige estabelecer os limites constitucionais sob o prisma digital. Assim como no surgimento da era das comunicações foi necessário estabelecer limites da interceptação das comunicações telefônicas⁶⁹, na era digital, torna-se necessário estabelecer limites do uso de dados com a edição de legislações específicas.

Os sistemas baseados em big data, inteligência artificial e o uso de algoritmos tornam os critérios de suspeição e ação estatal ainda mais opacos, pois automatizam padrões historicamente enviesados. A lógica algorítmica, em vez de combater a seletividade penal ainda presente no sistema penal brasileiro, tende a reproduzir e fortalecer a seletividade com ainda mais eficiência⁷⁰. É nesse sentido que o Supremo Tribunal Federal, na ADI 5059⁷¹, está analisando o caso dos dados telefônicos nas investigações criminais, discutindo a validade de dispositivo de lei federal que confere ao delegado o poder de requisitar dados telefônicos, independente de autorização judicial. Em eminente voto⁷², o Ministro Dias Toffoli afirma que a

⁶⁹ A inviolabilidade da correspondência, dos dados e das comunicações foi introduzida no rol dos direitos fundamentais assim como o direito à proteção dos dados pessoais. Do mesmo modo, surgiu como uma limitação constitucional ao poder punitivo. A Lei de Interceptações Telefônicas, a qual traça os limites para a permissão de ações de escuta telefônica, foi um instrumento regulador na mesma esfera.

⁷⁰ ARRUDA, Ana Julia Pozzi; RESENDE, Ana Paula Bougleux Andrade; FERNANDES, Fernando Andrade. **Sistemas de Policiamento Preditivo e Afetação de Direitos Humanos à Luz da Criminologia Crítica**, Revista de Direito Público, Brasília, v. 18, n. 100, p. 664-689, out.-dez. 2021. p. 679.

⁷¹ BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade 5059**. Relator: Min. Dias Toffoli. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=4483504> Acesso em: 11 jul. 2025.

⁷² Disponível em: https://www.migalhas.com.br/arquivos/2025/4/5B6DAC7E833276_votoquebra.pdf. Acesso em: 2 de jul. de 2025.

inserção do direito à proteção de dados no catálogo dos direitos fundamentais “reforça a relevância da adequada proteção dos dados pessoais na sociedade contemporânea”⁷³. No caso em tela, a discricionariedade no acesso a qualquer tipo de dado gera uma ameaça ao direito à proteção dos dados pessoais.

A coleta massiva e o uso preditivo das informações obtidas, por exemplo, diretamente da operadora de telefonia, produz uma nova racionalidade penal, em que a seletividade é fortalecida para além do juízo moral discriminatório, pois com os dados e os algoritmos, ela passa a ser baseada em estatísticas que reiteram padrões históricos de criminalização e marginalização. É nesse sentido que o simples acesso a dados diretamente da operadora, sem limitações, é um potencial instrumento de gestão seletiva, não apenas para o registro e a investigação, mas também para emoldurar ações futuras.

Nesse contexto, a fase pré-processual utiliza os dados e os algoritmos para atuar como uma verdadeira predadora, pois silenciosamente captura os dados dos indivíduos sem oportunizar o contraditório e a defesa. Legitimada pelo uso de dados supostamente objetivos⁷⁴, a nova forma de seletividade penal sistematiza dados históricos de modo a operar como uma espécie de “discriminação algorítmica”, pela qual determinados grupos são alvo de operações policiais, independente de comportamentos concretos. Isso acentua o risco de que se consolide um sistema penal ainda mais discriminatório, pois agora é legitimado pelos algoritmos.

A título de maior densificação e exemplificação desta ideia, far-se-á uma análise acerca do reconhecimento facial, que é uma nova realidade tecnológica no âmbito da segurança pública, muito importante para que sejam identificados fugitivos, mas que faz com que a vigilância passe a ser cotidiana a indivíduos da massa que não possuem nenhuma investigação concreta⁷⁵. Beatriz Daguer, Luiz Antonio Borri e Rafael Junior Soares trazem

⁷³ BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade 5059**. Relator: Min. Dias Toffoli. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=4483504> Acesso em: 11 jul. 2025. p. 9.

⁷⁴ Supostamente, pois em princípio seriam utilizados apenas para fins de investigação específica.

⁷⁵ DAGUER, Beatriz; BORRI, Luiz Antonio; SOARES, Rafael Junior. **O reconhecimento facial na segurança pública e a proteção de dados pessoais como garantia**

um estudo de Bruno Calabrich⁷⁶ que cita alguns casos em que foram constatados graves problemas de discriminação pelo uso do reconhecimento facial: o caso do algoritmo de recrutamento da área de recursos humanos da Amazon, que facilitava a contratação de homens em detrimento de mulheres; o caso do algoritmo de categorização de imagens do Google Photos, que identificava pessoas negras como gorilas; e o caso do algoritmo do programa COMPAS (Correctional Offender Management Profiling for Alternative Sanctions), software de auxílio a juizes norte-americanos na avaliação da probabilidade de reincidência na dosimetria da pena, que erroneamente identificava os réus negros como futuros criminosos por mais vezes que os réus brancos e rotulava estes como de baixo risco de reincidência. Ainda, no Brasil, foi realizado um levantamento que revelou que 90,6% das pessoas presas via reconhecimento facial em 2019 eram negras⁷⁷.

É neste contexto que se percebe um risco de resultados discriminatórios ao utilizar os algoritmos e softwares lastreados em ampla base de dados. Tendo em vista que a tecnologia depende da atuação humana, sua formatação é essencial para o funcionamento⁷⁸. Essa dependência humana, portanto, é perigosa, pois, no Brasil, é evidente a preocupação mínima do poder público em elaborar base legal para a adoção de mecanismos como o do reconhecimento facial, uma vez que até os dias de hoje não se tem uma legislação em vigor. A tecnologia continua sendo empregada de forma ostensiva, e crescendo para a segurança pública. Em uma sociedade em que a discriminação e a seletividade penal ainda são um problema, o uso descontrolado da inteligência artificial na esfera pública tem, conforme alega Alice Azevedo Magalhães e Tércio Spínola Gomes⁷⁹,

fundamental. Revista de Direito e as Novas Tecnologias. v. 16. ano 5. São Paulo: RT, jul-set. 2022. p. 7.

⁷⁶ CALABRICH, Bruno Freire de Carvalho. **Discriminação algorítmica e transparência na lei geral de proteção de dados pessoais.** Revista de Direito e as Novas Tecnologias, v. 8, jul-set. 2020.

⁷⁷ SANTOS, Jéssica Guedes. **Reconhecimento facial entre a criminologia, a mídia e a LGPD penal.** Internet & Sociedade, v. 2, n. 1, jun. 2021. p. 224.

⁷⁸ DAGUER, Beatriz; BORRI, Luiz Antonio; SOARES, Rafael Junior. **O reconhecimento facial na segurança pública e a proteção de dados pessoais como garantia fundamental.** Revista de Direito e as Novas Tecnologias. v. 16. ano 5. São Paulo: RT, jul-set. 2022. p. 8.

⁷⁹ MAGALHÃES, Alice Azevedo; GOMES, Tércio Spínola. **Regulação de sistemas de reconhecimento facial para fins de segurança pública no Brasil: riscos e desafios.** Revista Humanidades & Inovação, v. 8, n. 47, 2021. p. 174.

potencial para afetar negativamente toda a população, pois amplia as discriminações, atuando de maneira maquiada, uma vez que essa atuação é legitimada pelo discurso da imparcialidade algorítmica, o que dificulta a identificação das injustiças.

A implementação das novas tecnologias na persecução penal ameaça fortemente os direitos fundamentais como a privacidade, a igualdade, a dignidade da pessoa humana, a presunção de inocência e a proteção de dados pessoais. Utilizar de maneira massiva os dados pessoais para categorizar os indivíduos ou grupos, embora tenha aparência de neutralidade, já é demonstrado através das pesquisas que gera resultados discriminatórios e perigosos para o sistema democrático. Assim, a expansão das tecnologias pode levar a um cenário de vigilância permanente⁸⁰, porque a utopia tecnológica de reconhecer e coibir criminosos fomenta a prática antecipatória de vigilância⁸¹.

Diante disso, a tecnologia possui um papel potencializador da seletividade penal, e com isso, é necessário remodelar o tratamento jurídico da proteção de dados pessoais, tendo em vista a atual importância e os impactos na vida da sociedade⁸². Beatriz Daguer, Luiz Antonio Borri e Rafael Junior Soares⁸³ concluem que se não houver, no Brasil, uma norma específica que garanta a neutralidade dos softwares e ofereça diretrizes e limites aos programadores e ao Estado no uso de dados, bem como que garanta o acesso aos cidadãos da finalidade e do tratamento dos dados, a utilização do sistema de reconhecimento facial na segurança pública passa a ser permeada por incerteza jurídica, por seletividade de um sistema que

⁸⁰ Fenômeno conhecido como “*ban-opticon*” ou “*superpanóptico*”, em que a vigilância se torna um instrumento de controle individual e coletivo.

⁸¹ ARRUDA, Ana Julia Pozzi; RESENDE, Ana Paula Bougleux Andrade; FERNANDES, Fernando Andrade. **Sistemas de Policiamento Preditivo e Afetação de Direitos Humanos à Luz da Criminologia Crítica**, Revista de Direito Público, Brasília, v. 18, n. 100, p. 664-689, out-dez. 2021. p. 669.

⁸² DAGUER, Beatriz; BORRI, Luiz Antonio; SOARES, Rafael Junior. **O reconhecimento facial na segurança pública e a proteção de dados pessoais como garantia fundamental**. Revista de Direito e as Novas Tecnologias. vol. 16. ano 5. São Paulo: Ed. RT, jul.-set. 2022. p. 8.

⁸³ *Ibid.*, p. 9.

segrega e por punição de pessoas vulneráveis e inocentes, tal qual já se observa atualmente, como elucidam Araújo, Cardoso e Paula⁸⁴.

Neste contexto do reconhecimento facial adotado para a segurança pública, utilizando-se o método hipotético-dedutivo e ampliando-se para toda a esfera penal, na persecução penal não é diferente. Urge estabelecer um aprimoramento e conduzir normativamente o uso das novas tecnologias no processo penal. “As tecnologias emergentes devem ser reguladas e balizadas pelo Poder Legislativo e pelas agências reguladoras, isto é, o Direito deve se empenhar em obstaculizar as externalidades negativas e não inibir as novas tecnologias”⁸⁵. A LGPD foi importante marco normativo para o avanço da tutela na proteção de dados pessoais, ainda mais com a posterior inclusão da proteção de dados como um direito fundamental, através da EC nº115/22. Todavia, não foi projetada para o âmbito penal⁸⁶, o que gera uma lacuna legislativa significativa diante das problemáticas crescentes relacionadas ao uso de dados na esfera penal. Assim, o projeto da LGPD Penal é uma importante iniciativa para o que é preciso atualmente. Todavia, a efetividade e a abrangência das suas disposições, como será retratado no próximo tópico, ainda são objetos de debate.

É imprescindível a limitação ao tratamento e compartilhamento de dados na persecução penal, pois a atividade estatal não está imune à limitação da autodeterminação informativa, conforme enfatizado pelo STF ADI 6387⁸⁷. Assim, o conceito de “devido processo informacional”⁸⁸ surge como um corolário da autodeterminação informativa e exige que o processo

⁸⁴ ARAÚJO, Rômulo de Aguiar; CARDOSO, Naiara Deperon; PAULA, Amanda Marcélia. **Regulação e uso do reconhecimento facial na segurança pública do Brasil**. Revista de Doutrina Jurídica, Brasília/DF, v. 112, 2021. p. 5.

⁸⁵ MONTEIRO, Guilherme Ornelas. **Instrumentos de reconhecimento facial e os contornos da lei geral de proteção de dados ante a privacidade nas cidades (in)inteligentes**. Revista de Direito e Atualidades, v. 1, n. 1, jan-mar. 2021. p. 35.

⁸⁶ O art. 4º, III, exclui a sua aplicação para fins de investigação criminal e segurança pública.

⁸⁷ Na ADI 6387, o Supremo Tribunal Federal reconheceu a proteção de dados pessoais como direito fundamental autônomo, antes da inserção dele no rol pela EC nº 115/2022. O Conselho Federal da OAB destacou que o ordenamento constitucional considera o direito à proteção de dados em paralelo com o direito à autodeterminação informativa. A ADI discute a constitucionalidade de dispositivo que obrigava empresas de telefonia a compartilhar com o IBGE dados pessoais de consumidores, a fins de apoio à produção estatística durante a pandemia de COVID-19. Dessa forma, mesmo se tratando de dados ao Estado, o STF reconheceu a proteção.

⁸⁸ FERREIRA, André da Rocha. **Tratamento de dados pessoais em investigações criminais: o direito fundamental à autodeterminação informativa como limite constitucional**. Revista Brasileira de Ciências Criminais. v. 185. ano 29. p. 115-159. São Paulo: RT, novembro 2021. p. 148.

decisório algorítmico seja amparado por princípios e regras que garantam a sua validade⁸⁹.

Ademais, o STF e o STJ possuem decisões relevantes que discutem essa problemática da limitação do uso de dados na persecução penal. Para analisar como a temática vem sendo aplicada nos tribunais superiores, propõe-se a seguir um panorama jurisprudencial. Com isso, é possível verificar com maior concretude em que situação encontra-se o entendimento jurisprudencial da temática e quais os desafios e controvérsias que estão sendo encontrados.

No HC nº 168.052, o STF discute a legalidade da prova obtida através do acesso a conversas registradas no aplicativo de WhatsApp a partir da apreensão do aparelho e o ingresso em domicílio posterior, sem autorização judicial. O Ministro Gilmar Mendes destacou que o acesso ao conteúdo do celular sem a autorização judicial configura violação constitucional. Observou que a consulta aos dados armazenados não se confunde com a quebra do sigilo das comunicações, mas que o acesso sem a autorização viola a privacidade. Ainda, o Ministro mencionou precedentes internacionais e a necessidade da proteção dos dados pessoais, citando a decisão do Tribunal Constitucional alemão e a legislação europeia de proteção de dados, que inspirou a LGPD. Em suma, o STF reconheceu a ilicitude do acesso sem autorização, mas não declarou a nulidade do processo, pois havia outras provas válidas que fundamentaram a condenação, contudo, é possível perceber a preocupação da Suprema Corte na temática.

Além disso, o STF no HC nº 91.867, também foi discutida a quebra do sigilo telefônico dos correus, com o acesso ao aparelho feito sem a autorização judicial. A defesa alegava a nulidade das provas, todavia o Ministro Gilmar Mendes, relator do acórdão, esclareceu novamente que comunicação telefônica e registros telefônicos recebem proteção jurídica distinta e que não se pode interpretar a cláusula do artigo 5º, XII da CF/88 no sentido de proteção aos dados enquanto registro, da forma como argumentou no HC nº 168.052. O entendimento é de que a proteção constitucional é à comunicação de dados, e não aos dados registrados no aparelho. Neste caso, os policiais responsáveis pelo flagrante teriam verificado o registro das

⁸⁹ Conceito introduzido no voto do Ministro Gilmar Mendes na ADI do IBGE.

últimas chamadas efetuadas e recebidas dos celulares apreendidos e, ao analisar esses dados contidos no celular, teriam chegado a números pertencentes aos pacientes. É nesse sentido que se destaca que comunicação telefônica e registro telefônico são distintos. Quando se diz em inviolabilidade do sigilo, o que se protege é a comunicação, a troca de informações privativa, e não os dados em si. Ao analisar o registro da agenda telefônica, entendeu-se que não é uma quebra do sigilo de dados, mas apenas a colheita de informações para o inquérito. Isso é diferente de acessar os dados, por exemplo, registrados na empresa de telefonia. Dessa forma, esse julgado é importante para estabelecer o conceito de dado e de sigilo, basilares para o entendimento da proteção de dados.

No STJ, o RHC nº 89.981/MG também tratou do tema. Discutiu-se a ilegalidade da prova obtida a partir de mensagens armazenadas em aparelho telefônico apreendido sem autorização judicial. A questão central foi a verificação da licitude da prova obtida pela polícia, que realizou vistoria no aparelho e acessou mensagens do WhatsApp. O STJ entendeu que apesar de não se tratar de interceptação telefônica, houve a violação da intimidade e da vida privada. O voto do Ministro relator Reynaldo Soares da Fonseca ressaltou o entendimento de que a prova obtida de dados armazenados em aparelho celular, sem autorização judicial, é ilícita. No mesmo sentido foi decidido no RHC nº 51.531/RO, em que foram declaradas nulas as provas obtidas no celular sem autorização judicial.

No ARE nº 1.042.075/RJ (Tema 977 de Repercussão Geral), o STF entendeu que a polícia pode acessar os dados armazenados em aparelho celular abandonado na cena do crime e que tal medida não viola o direito fundamental ao sigilo das comunicações telefônicas. Todavia, entendeu-se que quando não se trata de celular abandonado, a polícia somente poderá acessar os dados contidos nele com autorização judicial ou do proprietário.

Caso de relevante debate também é o RE nº 1.301.250/RJ, em que trata da constitucionalidade das decisões judiciais que determinaram a quebra do sigilo de dados pessoais, em especial registros de acesso à internet e endereços de IP. Neste caso, o Ministério Público do Rio de Janeiro requereu a identificação dos IPs que tenham utilizado o Google Maps ou Waze, aplicativos de serviço de GPS, ou o Google Busca em um período

compreendido anteriormente ao dia da morte de Marielle Franco. No caso, foi requerida identificação dos usuários que pesquisaram “Mariele Franco”, “Vereadora Mariele Franco”, “Agenda Vereadora Mariele”, “Casa das Pretas”, “Rua dos Inválidos, 122” ou “Rua dos Inválidos”⁹⁰. O caso envolve importante debate, pois envolve ordem judicial genérica de fornecimento dos registros de conexão e de acesso dos usuários em um caso de completa relevância social. O julgamento não está sendo unânime, tendo em vista a complexidade da temática, sendo divergentes da relatora Ministra Rosa Weber os Ministros Alexandre de Moraes e Cristiano Zanin.

Por fim, no HC nº 222.141, do STF, discutiu-se a legalidade de atos do Ministério Público relacionados ao congelamento e acesso a dados telemáticos de uma investigada, sem prévia autorização judicial. A decisão enfatizou a proteção dos direitos à privacidade, à autodeterminação informativa e à proteção de dados pessoais. Ademais, reafirmou que a proteção de dados pessoais não envolve apenas o sigilo do conteúdo, mas também o controle sobre o uso, o acesso e os limites dos dados pelo titular. Ressalte-se que este último julgamento foi o mais recente encontrado.

Por conseguinte, enquanto as novas tecnologias são de suma importância para a investigação criminal e para o processo penal como um todo, além de promover melhorias para a segurança pública, o uso ilimitado e a ausência de uma base legal específica podem promover erros seletivos e estigmatizados, o que pode levar a injustiças e violações de direitos fundamentais. Assim, é basilar que a legislação brasileira avance nessa temática, priorizando a transparência, a proporcionalidade e os direitos fundamentais, a fim de evitar que as tecnologias se tornem um instrumento fortalecedor das desigualdades e minorante da democracia.

Nesse cenário, a aplicação dos princípios do constitucionalismo digital devem ser os pilares de uma nova arquitetura normativa. A proteção de dados pessoais, enquanto direito fundamental, deve operar como barreira de contenção contra abusos e excessos investigativos, garantindo que o

⁹⁰ SILVA NETO, Arthur Corrêa da. **Dos impactos do julgamento no STF no RE 1.301.250: caso Marielle Franco**. Consultor Jurídico, São Paulo, 3 abr. 2025. Disponível em: www.conjur.com.br. Acesso em: 3 jul. 2025.

paradigma digital não seja construído à custa da liberdade individual e do devido processo legal.

2.2. O anteprojeto de LGPD penal e o PL 1.515/2022: entre a eficiência e a proteção dos direitos fundamentais

A inovação tecnológica conduz o Estado a adotar novas ferramentas para a segurança pública e para a persecução penal, tendo em vista que possuem importante papel no combate à criminalidade no ambiente virtual. O uso dos algoritmos e dos dados pessoais sem a devida limitação é capaz de gerar uma discriminação algorítmica, com a consequente violação dos direitos fundamentais. Por isso, é fundamental que se tenha uma base legal específica para a utilização desses instrumentos e a efetividade da persecução penal no contexto digital.

No Brasil, esse debate resultou na elaboração do Anteprojeto da Lei de Proteção de Dados para a Segurança Pública e Persecução Penal⁹¹, a “LGPD Penal”, a qual foi entregue à Câmara dos Deputados em 2020⁹². O projeto legislativo surge para preencher a lacuna que a LGPD deixou. Paralelamente, em junho de 2022, o Projeto de Lei nº 1515/2022⁹³ foi proposto com o mesmo objetivo. Apesar das duas propostas versarem o mesmo tema, possuem algumas divergências significativas em relação às garantias dos titulares dos dados. Desse modo, a presente análise se concentra na comparação entre os dois e também se estende aos desafios gerais da regulamentação das tecnologias no processo penal brasileiro.

O Anteprojeto da LGPD Penal foi feito por uma comissão de juristas e foi estruturado em 68 artigos, visando dispor princípios, diretrizes, garantias processuais e prerrogativas fundamentais em relação ao tratamento de

⁹¹ CÂMARA DOS DEPUTADOS (Brasil). **Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Persecução Penal: elaborado pela Comissão de Juristas instituída pelo Ato do Presidente da Câmara dos Deputados de 26 de novembro de 2019**. Brasília, 2021. Disponível em: [DADOSAnteprojetoComissaoprotecaodadossegurancapersecucaoFINAL.pdf](#) Acesso em: 3 jul. 2025.

⁹² CHUY, José Fernando Moares. **O sistema de Investigação Brasileiro, a “LDGP PENAL e a Efetiva Garantia de Direitos Fundamentais**. p. 2.

⁹³ ARMANDO, Coronel. **PL 1515/2022**. Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais. Disponível em: [Portal da Câmara dos Deputados](#). Acesso em: 3 jul. 2025.

dados pessoais para a segurança pública e a persecução penal, estando inclusive esses aspectos explícitos na exposição de motivos⁹⁴. A elaboração do anteprojeto foi multidisciplinar e democrática e enfrentou desafios ao ser criada, uma vez que o direito penal é um campo sensível e perigoso⁹⁵, pois pode determinar a medida mais grave relacionada ao indivíduo: a privação da liberdade. O documento buscou harmonizar a legislação brasileira com os institutos internacionais, que já se encontram em um nível adequado de proteção de dados⁹⁶, como a Diretiva 680/2016 da União Europeia⁹⁷.

Um dos pontos fortes do Anteprojeto é que ele consiste em consolidar uma base principiológica robusta⁹⁸. Considerando os aspectos do constitucionalismo digital, o anteprojeto da LGPD Penal está em consonância com a ideologia, pois busca restabelecer o equilíbrio constitucional desbalanceado pelas novas tecnologias, abrangendo princípios, normas e valores constitucionais aplicados ao âmbito penal no contexto digital. O artigo 2º da LGPD Penal⁹⁹ replica alguns fundamentos da LGPD e acrescenta alguns relativos ao processo penal. Essa base principiológica é fundamental para ponderar decisões que envolvam o uso de dados pessoais nas investigações em concordância com o constitucionalismo digital.

⁹⁴ PONTE, Amanda Leite de Farias. **Da necessidade de limites ao tratamento e compartilhamento de dados por órgãos de inteligência do Estado à luz da Lei Geral de Proteção de Dados em matéria penal**. Caderno Virtual, Brasília, v. 1, n. 54, 2022. p. 10.

⁹⁵ AZEVEDO, Cynthia Picolo Gonzaga de et al. **Nota técnica: análise comparativa entre o anteprojeto de LGPD penal e o PL 1515/2022**. Instituto de Referência em Internet e Sociedade (IRIS) e Laboratório de Políticas Públicas e Internet (LAPIN), novembro de 2022. p. 5.

⁹⁶ CHUY, José Fernando Moares. **O sistema de Investigação Brasileiro, a “LGPD Penal” e a Efetiva Garantia de Direitos Fundamentais**. p. 4.

⁹⁷ A Diretiva 680/2016 da União Europeia regulou o tratamento de dados pessoais para fins de segurança pública e persecução penal separado do seu marco normativo de proteção de dados, o Regulamento 679/2016.

⁹⁸ ROSA, Raíssa Roese. **O Anteprojeto da Lgpd Penal e a Necessidade de Cooperação Internacional para o Compartilhamento Extraterritorial de Dados Pessoais para Fins Penais**. 2022. Monografia (Pós-Graduação) - Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa. p. 7.

⁹⁹ Art. 2º A disciplina da proteção de dados pessoais em atividades de segurança pública e persecução penal tem como fundamentos:

I – a dignidade, os direitos humanos, o livre desenvolvimento da personalidade, e o exercício da cidadania pelas pessoas naturais;

II – a autodeterminação informativa;

III – o respeito à vida privada e à intimidade;

V – a presunção de inocência;

IV – a liberdade de manifestação do pensamento, de expressão, de informação, de comunicação e de opinião;

VI – confidencialidade e integridade dos sistemas informáticos pessoais; e

VII – garantia do devido processo legal, da ampla defesa, do contraditório, da motivação e da reserva legal.

A proposta legislativa estabelece maior transparência e controle sobre o uso das tecnologias de monitoramento¹⁰⁰, além de prever que a utilização dessas tecnologias deve ser prevista em lei específica, deve elencar os direitos dos titulares e deve ser fundamentada em um relatório de impacto de vigilância, detalhando a natureza dos dados, a finalidade do tratamento e quantidade de titulares potencialmente afetados¹⁰¹. Um importante passo da legislação é que ela veda a utilização contínua e genérica de tecnologias de vigilância¹⁰², como o reconhecimento facial retratado no tópico anterior, com exceção de quando houver conexão com a persecução penal individualizada. Além disso, atribui ao CNJ a responsabilidade de emitir recomendações sobre o uso dessas tecnologias, publicar relatórios anuais sobre tecnologias de monitoramento pelas autoridades e realizar auditorias diante de denúncias de descumprimento da lei¹⁰³.

Ao que tange à transferência internacional de dados, o APL¹⁰⁴ se mostra consistente e alinhado aos modelos internacionais, em especial o modelo europeu, uma vez que prevê mecanismos de obtenção de uma decisão adequada, oferecimento de garantias adequadas de proteção e a incidência de derrogações excepcionais¹⁰⁵. A similitude ao sistema internacional é basilar para a cooperação internacional no combate aos crimes transnacionais, agora facilitados pela tecnologia, e isto é algo que as

¹⁰⁰ AZEVEDO, Cynthia Pico Gonzaga de *et al.* **Nota técnica: análise comparativa entre o anteprojeto de LGPD penal e o PL 1515/2022**. Instituto de Referência em Internet e Sociedade (IRIS) e Laboratório de Políticas Públicas e Internet (LAPIN), novembro de 2022. p. 21.

¹⁰¹ *Ibid.*

¹⁰² Art. 42. Qualquer modalidade de uso compartilhado de dados pessoais entre autoridades competentes somente será possível nas hipóteses previstas em lei, desde que observados os propósitos legítimos e específicos para o tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei.

§ 1º. É vedado o compartilhamento direto e contínuo de bancos de dados estabelecidos no âmbito de atividades de segurança pública com autoridades competentes para fins de persecução penal, as quais somente terão acesso a dados dessa origem para investigação ou processo criminal específico, observadas as demais disposições deste artigo.

¹⁰³ DAGUER, Beatriz; BORRI, Luiz Antonio; SOARES, Rafael Junior. **O reconhecimento facial na segurança pública e a proteção de dados pessoais como garantia fundamental**. Revista de Direito e as Novas Tecnologias. vol. 16. ano 5. São Paulo: RT, jul-set. 2022. p. 6.

¹⁰⁴ Nos artigos 50 a 53.

¹⁰⁵ VIOLA, Mário; HERINGER, Leonardo; CARVALHO, Celina. **O Anteprojeto da LGPD Penal e as regras sobre transferência internacional de dados pessoais**. Instituto de Tecnologia & Sociedade do Rio. Agosto, 2021. p. 9.

autoridades brasileiras¹⁰⁶ enfrentam com dificuldades devido à falta da regulamentação efetiva¹⁰⁷. Em um ponto forte, o APL propõe, na sua exposição de motivos, a cooperação jurídica internacional para a transferência de dados entre os países, mas destaca que é necessário proteger os direitos fundamentais dos titulares¹⁰⁸. Ainda, prevê que o compartilhamento deve se atentar às finalidades penais e deve ser restrito à finalidade almejada¹⁰⁹, conforme expresso no art. 56, §2º¹¹⁰.

Em contrapartida do APL, o Projeto de Lei nº 1.515/2022, apresentado em estrutura similar ao APL, alterou em alguns pontos o conteúdo relacionado à proteção e ao tratamento dos dados pessoais, o que reflete em um enfraquecimento dos direitos e das garantias projetadas no APL. A análise comparativa realizada por Cynthia Picolo Gonzaga de Azevedo *et al*, na Nota Técnica “Análise comparativa entre O ANTEPROJETO DE LGPD PENAL E O PL 1515/2022”, revela que o PL nº 1.515/2022 resulta na supressão de garantias fundamentais dos titulares e na ampliação da discricionariedade do Estado¹¹¹.

Isso ocorre, pois, segundo os autores, o PL expandiu o escopo para incluir o tratamento de dados para defesa nacional, segurança do Estado e atividades de inteligência, que são áreas que o Anteprojeto deixou para regulações futuras¹¹². Tal ampliação possui uma problemática, porque a defesa nacional e a segurança do Estado possuem fundamentos e

¹⁰⁶ Registre-se que o Brasil é signatário da Convenção de Budapeste, mediante promulgação do Decreto nº 37/2021, que visa à cooperação internacional para o combate ao cibercrime. Desse modo, a ausência de legislação aqui pontuada é referente à legislação específica brasileira.

¹⁰⁷ AZEVEDO, Cynthia Picolo Gonzaga de *et al*. **Nota técnica: análise comparativa entre o anteprojeto de LGPD penal e o PL 1515/2022**. Instituto de Referência em Internet e Sociedade (IRIS) e Laboratório de Políticas Públicas e Internet (LAPIN), nov. 2022. p. 27.

¹⁰⁸ ROSA, Raíssa Roese. **O Anteprojeto da Lgpd Penal e a Necessidade de Cooperação Internacional para o Compartilhamento Extraterritorial de Dados Pessoais para Fins Penais**. 2022. Monografia (Pós-Graduação) - Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa. p. 18.

¹⁰⁹ *Ibid.*, p. 12.

¹¹⁰ § 2º As transferências de dados efetuadas com base neste artigo serão limitadas aos dados estritamente necessários para a finalidade almejada.

¹¹¹ AZEVEDO, Cynthia Picolo Gonzaga de *et al*. **Nota técnica: análise comparativa entre o anteprojeto de LGPD penal e o PL 1515/2022**. Instituto de Referência em Internet e Sociedade (IRIS) e Laboratório de Políticas Públicas e Internet (LAPIN), nov. 2022. p. 3.

¹¹² NEVES, Cleuler Barbosa; MATOS, Gisele Gomes. **LGPD Penal e a lacuna regulatória para o tratamento dos dados pessoais para fins de criminais: APL e PL 1515/2022**. Revista Caderno Pedagógico – Studies Publicações e Editora Ltda., Curitiba, v. 22, n. 7, p. 1-30, 2025. p. 9.

finalidades institucionais de certo modo incompatíveis com o projetado no APL, uma vez que “as inovações propostas para acomodar essas duas atividades não são capazes de oferecer níveis de controle proporcionais aos riscos, impactos sociais, econômicos e políticos gerados”¹¹³.

Ademais, o PL promove uma debilitação de princípios basilares da Administração Pública como a proporcionalidade, o livre acesso e a transparência¹¹⁴. Além disso, houve a exclusão do princípio da autodeterminação informativa, o que indica um retrocesso legislativo, uma vez que todo o escopo fundamental relacionado à proteção de dados o qual fora construído foi ignorado, e assim, priorizou o poder estatal em detrimento das liberdades e garantias individuais¹¹⁵.

Desse modo, tendo em vista que a ausência de princípios bases constitucionais, dentro da ótica do constitucionalismo digital, o PL 1515 pode gerar grandes desafios para a proteção dos dados e dos titulares no contexto do processo penal, pois ele priorizou a segurança e a defesa nacional ante os direitos fundamentais individuais. Além disso, o PL ampliou as autorizações para o tratamento de dados pessoais, sem as hipóteses restritivas do APL¹¹⁶. Ele retira das regras de acesso e compartilhamento a autorização legal ou judicial e, desse modo, entra em risco o princípio da finalidade e da privacidade, pois o compartilhamento sem a necessidade de motivação, dá ao Estado a oportunidade de acessar e compartilhar os dados sem motivos específicos, o que aumenta a discricionariedade e o estado de vigilância.

Ao que se refere ao tratamento de dados considerados sigilosos e às decisões automatizadas, o PL 1515/2022 também apresenta descompasso com o APL. Ao suprimir o conceito de “dados sigiloso” e as garantias deles as quais eram dispostas no APL, o PL cria uma insegurança jurídica, uma vez que elimina uma ferramenta normativa que é fundamental tanto para a proteção de dados quanto para o processo penal¹¹⁷. Ademais, em relação às decisões automatizadas, o PL veda as decisões tomadas exclusivamente

¹¹³ AZEVEDO, Cynthia Pícolo Gonzaga de *et al.* **Nota técnica: análise comparativa entre o anteprojeto de LGPD penal e o PL 1515/2022**. Instituto de Referência em Internet e Sociedade (IRIS) e Laboratório de Políticas Públicas e Internet (LAPIN), novembro de 2022. p. 7.

¹¹⁴ *Ibid.*, p. 10.

¹¹⁵ *Ibid.*, p. 15.

¹¹⁶ *Ibid.*, p. 12.

¹¹⁷ *Ibid.*, p. 19.

com base no tratamento automatizado e há a previsão de que, quando a decisão é automatizada, haverá garantia do direito de solicitar a intervenção humana do responsável do tratamento¹¹⁸. Com isso, enquanto o APL protege os titulares de decisões que afetem seus direitos e que ensejem elevado risco para dos direitos fundamentais, a vedação do PL em relação às decisões automatizadas se refere apenas a tratamentos exclusivamente automatizados que produzam “efeitos adversos na esfera jurídica do titular dos dados ou que o afetem de forma significativa” (art. 20, PL). Nesse contexto, o PL procura proteger o titular em casos muito específicos, diferentemente do APL, que possui uma proteção mais ampla.

Além disso, o APL possui a preocupação de tornar público os relatórios de impacto de proteção de dados (RIPDs) com as informações sobre os mecanismos para a proteção dos direitos e das liberdades dos titulares, o que submete a autoridade ao exame e ao controle, priorizando a transparência. De maneira diversa, o PL exclui essa publicidade. O texto dele, por consequência, também suprime o direito do titular em receber notificações sobre decisões automatizadas, o que condiz com a opacidade do sistema¹¹⁹. O PL também suprimiu todo o capítulo relacionado à transparência que era previsto no APL. Percebe-se que há um esforço para enfraquecer as garantias fundamentais e fortalecer o controle dos dados pessoais pelo poder estatal. A falta de transparência é um desafio enfrentado pelo constitucionalismo digital no poder público, pois a dificuldade dos indivíduos em consentir no funcionamento do sistema com seus dados, impede o exercício do controle e da democracia e configuram uma gestão da informação na segurança pública e no processo penal “às cegas”.

À título de melhor elucidação da análise comparativa, a seguir encontra-se uma tabela comparativa entre o Anteprojeto da LGPD Penal e o PL 1515/2022.

¹¹⁸AZEVEDO, Cynthia Picolo Gonzaga de *et al.* **Nota técnica: análise comparativa entre o anteprojeto de LGPD penal e o PL 1515/2022.** Instituto de Referência em Internet e Sociedade (IRIS) e Laboratório de Políticas Públicas e Internet (LAPIN), novembro de 2022. p. 19-20.

¹¹⁹ *Ibid.*, p. 20.

Critério de comparação	Anteprojeto LGPD Penal	PL 1515/2022	Análise
Escopo regulado	Restritivo: abrange exclusivamente o tratamento de dados para fins de segurança pública e perseguição penal, nos conformes do artigo 4º da LGPD	Ampliativo: incluiu também a defesa nacional, segurança do Estado e atividade de inteligência	A ampliação do PL é controversa, uma vez que mescla setores que possuem fundamentos e princípios distintos, o que pode vir a comprometer a precisão normativa e eleva o risco de abuso estatal.
Fundamentos legais	Inclui a autodeterminação informativa, proporcionalidade, confidencialidade e integridade	Suprime esses fundamentos e inclui a eficiência como fundamento, fragilizando direitos fundamentais	A exclusão da autodeterminação informativa viola diretamente o direito fundamental reconhecido pela EC 115/2022 e o reconhecimento proferido pelo STF na ADI 6387, o que conduz a uma inconstitucionalidade material.
Definições	Apresenta definições detalhadas e em consonância com a LGPD	Amplia as definições e elimina conceitos importantes como o de “dados sigilosos”, “tecnologias de monitoramento” e “registros criminais”	Redefinir e omitir termos chave da LGPD compromete a segurança jurídica e facilita a interpretação extensiva em desfavor dos direitos fundamentais
Princípios	Proporcionalidade, livre acesso, transparência, responsabilização	Supremacia do interesse público	O princípio da supremacia do interesse público como princípio norteador vai de encontro com o sistema garantista do direito penal. A lógica do PL faz o Estado prevalecer sobre o

			indivíduo, o que pode vir a comprometer direitos fundamentais
Bases legais para tratamento	Prevê de modo claro e restritivo as hipóteses em que é autorizado o tratamento de dados pessoais	Apresenta autorizações amplas e vagas, com pouca vinculação ao previsto na LGPD	A delimitação vaga fere o princípio da legalidade, fundamental no processo penal
Acesso e compartilhamento de dados	Estabelece requisitos rigorosos de compartilhamento, com necessidade de autorização legal, judicial e decisão fundamentada	Estabelece compartilhamento amplo, inclusive com os entes privados, e não necessita de justificativa formal	O PL viola o princípio da finalidade e abre margem para uma discricionariedade do Estado, podendo contribuir e agravar a seletividade penal.
Dados sigilosos	Regras claras para o acesso e exigência de autorização judicial	Suprime o conceito de dado sigiloso e as garantias associadas à ele	A supressão do conceito de dados sigilosos compromete o ordenamento jurídico, pois desconsidera a dogmática penal e a constitucionalidade do sigilo
Decisões automatizadas	Regulação detalhada com direitos do titular e RIPD obrigatórios	Previsões genéricas e pouco efetivas, sem RIPD	O PL não se atenta aos riscos trazidos pelas decisões automatizadas, as quais poder proferir decisões enviesadas e com erros, o que contribui para a seletividade penal
Tecnologias de monitoramento	Possui um capítulo específico com RIPD e análise de impacto regulatório com controle do CNJ	Suprime regulações e impõe permissividade quase total	O PL permite o uso quase irrestrito das tecnologias de vigilância de massa, o que é incompatível com o regime constitucional

Direitos dos titulares	Garante os direitos ao acesso, à retificação, à exclusão, ao bloqueio e à informação sobre compartilhamento	Exclui o direito à anonimização e reduz a transparência sobre o compartilhamento	As supressões do PL representam retrocessos normativos considerando-se a LGPD e a EC 115/2022
Transparência	Possui capítulo específico com o dever de prestação de informações e relatórios anuais	Suprime capítulo de transparência e obrigações de prestação de contas	Não haver capítulo sobre a transparência agrava o cenário da opacidade estrutural do sistema penal, o que limita o controle sobre o uso de dados no processo penal

Tabela 1 - Análise Comparativa Anteprojeto LGPD Penal e PL nº 1.515/2022

Em suma, o Anteprojeto da LGPD Penal representa um passo importante e harmônico com os princípios do constitucionalismo digital, uma vez que, ao se considerar os desafios da proteção de dados pessoais, da seletividade penal e da discriminação algorítmica presentes no uso de mecanismos tecnológicos na persecução penal, é uma legislação alinhada aos padrões internacionais e constitucionais. Em contrapartida, o Projeto de Lei nº 1515/2022, ao mesclar a segurança pública e a persecução penal com a defesa nacional e a supremacia do interesse público, coloca em risco as garantias individuais relacionadas à proteção de dados conquistadas recentemente. Ainda, o PL pode agravar a seletividade penal e a discriminação algorítmica, além de priorizar o interesse público ante a proteção individual. A efetividade de qualquer das regulamentações depende de debate contínuo e aprofundado a fim de mitigar os pontos fracos e assegurar a busca pela eficiência e segurança, sem resultar em aprofundamento das desigualdades.

3. A REGULAMENTAÇÃO DOS DADOS PESSOAIS NO PROCESSO PENAL SOB A ÓTICA FRATERNAL

A proteção de dados pessoais, consolidada como direito fundamental através da Emenda Constitucional nº 115/2022, impõe ao Estado proteger os indivíduos das violações e implementar mecanismos normativos que

garantam a sua efetividade. No entanto, a realidade da persecução penal na era digital demonstra a continuidade de práticas que violam esse direito, por meio do uso indiscriminado de dados.

A partir dos fundamentos estabelecidos nos capítulos anteriores, com a construção do constitucionalismo digital como teoria base das novas formas de poder informacional e os riscos apresentados pelo uso das tecnologias na persecução penal, este capítulo propõe analisar a regulação do tratamento de dados pessoais no processo penal brasileiro à luz da fraternidade.

Para além da dogmática tradicional, busca-se introduzir a perspectiva fraternal como paradigma regulatório, pois, enquanto valor constitucional, ela permite repensar a relação do Estado com o indivíduo no âmbito do processo penal. Assim, supera-se a lógica puramente instrumental da segurança pública em favor de uma racionalidade solidária e humanizante.

Assim, este capítulo examina a possibilidade de construção de uma persecução penal fraterna, na qual o respeito à dignidade humana seja pilar fundamental. Serão abordadas as dimensões jurídicas da fraternidade, sua positivação implícita, os contornos de sua aplicabilidade na prática da persecução penal e as implicações dessa abordagem para o futuro da regulamentação de dados pessoais no âmbito penal.

3.1. A aplicação jurídica da fraternidade na civilização tecnológica

Em primeiro lugar, importa-se elucidar o princípio da fraternidade como um pilar em que deve se estabelecer a modernidade, em se tratando do pós-constitucionalismo moderno, em que a finalidade das constituintes não é apenas limitar o poder pelo poder, mas promover de fato os direitos fundamentais materialmente incorporados pela comunidade política¹²⁰. Dessa forma, o princípio da fraternidade é uma fonte constitucional e moral para construir a cultura da conciliação. Diante do contexto das novas tecnologias, torna-se cada vez mais necessário retomar o princípio da fraternidade, a fim de se concretizar o que está disposto na Constituição, no sentido de que o objetivo da República Federativa do Brasil é construir uma sociedade fraterna¹²¹.

¹²⁰ FONSECA, Reynado Soares da. **O Princípio Constitucional da Fraternidade: Seu Resgate no Sistema de Justiça**. Belo Horizonte: D'Plácido, 2019. p. 45.

¹²¹ Artigo 3º da CF/88: Constituem objetivos fundamentais da República Federativa do Brasil:

A partir da Revolução Francesa (1789), o princípio da fraternidade, junto à igualdade e à liberdade, foi sendo esquecido do tripé revolucionário, uma vez que não teve a mesma recepção e normatização jurídica como os demais, tanto que estes passaram a ser princípios-deveres positivados nas Constituições¹²². Todavia, a referência apenas à liberdade e à igualdade não foram suficientes para lidar com os problemas sociais¹²³. Todavia, a redescoberta da fraternidade no século XX e o advento da Declaração Universal dos Direitos Humanos de 1948 ressignificaram a fraternidade como um valor universal transformador das relações sociais e humanas¹²⁴. Assim, é evidente que, com a liquidez das relações sociais¹²⁵, a vivência da fraternidade é o que tornará possível a transformação das estruturas sociais, resguardando todo o processo político democrático conquistado até então¹²⁶.

A fraternidade opera como um “princípio regulador” da liberdade e da igualdade, pois impede que a liberdade se torne “arbítrio do mais forte” e que a igualdade se degrade em um “igualitarismo opressor”¹²⁷. Além disso, é representada pelos direitos de terceira geração¹²⁸, também conhecidos como direitos de solidariedade, que representam o desenvolvimento coletivo, a paz e o meio ambiente. Nesse viés coletivo, a fraternidade visa basear a

I - construir uma sociedade livre, justa e solidária;

II - garantir o desenvolvimento nacional;

III - erradicar a pobreza e a marginalização e reduzir as desigualdades sociais e regionais;

IV - promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação.

¹²² FONSECA, Reynaldo Soares da; ROSSETTO, Geralda Magella de Faria. **Dívida Fraternal E Política Compensatória: O Dilema Da Proteção, Promoção E Defesa Dos Direitos Humanos Na Civilização Tecnológica.**

¹²³ *Ibid.*

¹²⁴ LANGOSKI, Deisemara Turatti. BRAUN, Helenice da Aparecida Dambrós. **Ressignificação Direitos Humanos Fundamentais sob o prisma do Multiculturalismo e da Fraternidade.** p. 1170.

¹²⁵ O conceito de sociedade líquida desenvolvido pelo sociólogo polonês Zygmunt Bauman descreve que as transformações sociais contemporâneas são marcadas pela instabilidade e pela fragilidade. a modernidade líquida, nesse sentido, precisa recuperar o princípio da fraternidade a fim de se restabelecer.

¹²⁶ LANGOSKI, Deisemara Turatti. BRAUN, Helenice da Aparecida Dambrós. **Ressignificação Direitos Humanos Fundamentais sob o prisma do Multiculturalismo e da Fraternidade.** p. 1172.

¹²⁷ BAGGIO, Antonio Maria. A idéia de fraternidade em duas Revoluções: Paris 1789 e Haiti 1791. **O princípio esquecido: A fraternidade na reflexão atual das ciências políticas.** Tradução: Durval Cordas, Iolanda Gaspar, José Maria de Almeida. Vargem Grande Paulista, SP: Cidade Nova, 2008. v. 1, p. 54.

¹²⁸ BONAVIDES, Paulo. **Curso de Direito Constitucional.** 19. ed. São Paulo: Malheiros, 2006, p. 563–564.

valorização das diferenças culturais e contribuir para o bem-estar da humanidade como um todo¹²⁹.

A aplicação jurídica da fraternidade tem ganhado espaço no direito contemporâneo, indo além do aspecto moral e filosófico para a materialização de um direito fundamental autônomo cujo centro axiológico tem como base a dignidade da pessoa humana¹³⁰, inserindo-se como direito humano universal com previsão nos tratados internacionais¹³¹. Ademais, o Ministro Carlos Ayres Britto¹³² denomina que o “constitucionalismo fraternal” é aquele constitucionalismo do futuro, alcançando uma terceira fase, após a fase liberal e a social, em que é alcançada a dimensão da luta pela afirmação do valor do desenvolvimento, do meio ambiente e da democracia, o que condiz com a terceira geração de direitos da teoria de Paulo Bonavides. Desse modo, a fraternidade aplica-se atuando em prol da dignidade da pessoa humana, no sentido de promover ações afirmativas e proteções de direitos coletivos, sendo fundamental para a mitigação das problemáticas ocasionadas pelas transformações desiguais.

A civilização tecnológica, caracterizada pelo uso do *ciberespaço* como novo meio de interação social e pelo imenso sistema de processamento de dados, requer uma ação mais responsável por todas as esferas sociais. A ubiquidade computacional¹³³, conceito trazido por Gabriel Fonseca e pelo Ministro Luiz Fux, é a onipresença tecnológica marcada pelos equipamentos eletrônicos presentes a todo momento na rotina de vários cidadãos, e fez com que os meios de comunicação fossem remodelados. Com isso, amplificou-se a importância do tratamento dos dados pessoais, pois a todo momento existe uma troca de informações no *ciberespaço*, o que pode

¹²⁹ LANGOSKI, Deisemara Turatti. BRAUN, Helenice da Aparecida Dambrós. **Ressignificação Direitos Humanos Fundamentais sob o prisma do Multiculturalismo e da Fraternidade**. p. 1171.

¹³⁰ FONSECA, Reynado Soares da. **O Princípio Constitucional da Fraternidade: Seu Resgate no Sistema de Justiça**. Belo Horizonte: D'Plácido, 2019. p. 96.

¹³¹ *Ibid.*, p. 97.

¹³² *Ibid.*, p. 107.

¹³³ FUX, Luiz; FONSECA, Gabriel Campos Soares da. **Segurança da informação e proteção de dados como pressupostos para o Poder Judiciário na era digital: uma análise da Resolução CNJ 361/2020 e da Resolução STF 724/2020**. In: BARATA, Bruno; ALMEIDA, Laryssa; FROTA, Leandro. (coord.). *Ensaio sobre a transformação digital no direito: estudos em homenagem ao Ministro Kássio Nunes Marques*. Brasília: OAB Editora, 2021.

subsidiar inferências e perfilizações sobre os indivíduos, interferindo diretamente na privacidade e na manipulação.

As novas técnicas de coleta, armazenamento, tratamento e compartilhamento de dados pessoais transformaram as atividades econômicas e as ações estatais, criando-se um controle informacional que age como um instrumento de poder¹³⁴. Este cenário desafia o próprio regime democrático, pois pode levar a difusão de *fake news* e a depreciação da ciência¹³⁵, uma vez que é capaz de potencializar o processamento massivo de dados pessoais a fim de manipular o pensamento dos usuários da internet.

Com esses apontamentos, tem-se que a dívida fraternal e a política compensatória podem ser adotadas como fundamento e razão de decidir em demandas submetidas ao controle jurisdicional, brasileiro ou internacional, tendo, portanto, uma aplicação jurídica fundamental norteadora de decisões que, ante a ausência de legislação protetiva, atravessam conflitos com violações de direitos fundamentais e humanos¹³⁶. A dívida fraternal é justamente a dívida que se contraiu no processo histórico, muitas vezes não intencionalmente, mas por uma falha na percepção da existência de violação de certos direitos¹³⁷. É a responsabilidade de reparar situações em que houve a negação da fraternidade¹³⁸. A política compensatória, de modo equivalente, é o mecanismo jurídico que proporciona a convivência fraterna¹³⁹ de modo a materializar a dívida existente, como a conquista dos direitos trabalhistas, a licença maternidade, tombamentos de sítios quilombolas, cotas raciais. O Ministro Ayres Britto, em seu eminente voto na ADI 3330¹⁴⁰, sustentou que a

¹³⁴ FONSECA, Reynaldo Soares. **A Democracia Fraternal na Era Digital**. p. 1-2.

¹³⁵ *Ibid.*, p. 5.

¹³⁶ FONSECA, Reynaldo Soares da; ROSSETTO, GERALDA Magella de Faria. **Dívida Fraternal E Política Compensatória: O Dilema Da Proteção, Promoção E Defesa Dos Direitos Humanos Na Civilização Tecnológica**. p. 16.

¹³⁷ *Ibid.*, p. 20.

¹³⁸ *Ibid.*, p. 19.

¹³⁹ *Ibid.*

¹⁴⁰ BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 3330**, Relator: Min. Carlos Ayres Britto, Tribunal Pleno, julgado em 02 abr. 2008. Ementa: Ações afirmativas. Programa Universidade para Todos – ProUni. Conversão da MP 213/2004 na Lei 11.096/2005. Constitucionalidade. Diário da Justiça Eletrônico, Brasília, DF, 09 abr. 2008. Disponível em: [Supremo Tribunal Federal](http://supremo.tribunal.federal.gov.br). Acesso em: 26 jun. 2025.

política compensatória é uma forma de “superar iníquas hegemonias política, social, econômica e cultural”¹⁴¹.

A civilização tecnológica trouxe a necessidade de reordenar o agir humano, pois sendo inicialmente um novo espaço de interações, abriu portas para que as interações fossem feitas sem limites. Como consequência lógica, pôs-se em risco direitos fundamentais do Estado, e até mesmo a própria democracia. Um caso que é emblemático e necessário de ser citado, é o da Cambridge Analytica¹⁴², em que a utilização massiva de dados pessoais manipulou os resultados eleitorais. Dessa forma, a proteção dos dados pessoais exerce um valor público inegociável, tanto que a Emenda Constitucional nº 115/2022 a reconheceu como direito fundamental. É com esses aspectos que se conclui que a fim de se resgatar a responsabilidade coletiva em prol do bem comum, é necessário reconhecer que a era digital deixou uma dívida fraternal com a sociedade. Instabilidades nos direitos fundamentais, na democracia e até na persecução penal, por meio da discriminação algorítmica, fazem necessário resgatar o princípio da fraternidade a fim de se obter uma sociedade justa e igualitária.

A aplicação jurídica da fraternidade no contexto da civilização tecnológica visa compensar politicamente as desigualdades geradas pelo uso das tecnologias, pois a fraternidade promove ações responsáveis e constrói uma ética pautada na responsabilidade¹⁴³. Com isso, pode-se atingir um paradigma necessário para a Justiça, o qual inclui, pacifica e restaura as relações humanas¹⁴⁴ diante das transformações ocasionadas pelas tecnologias.

¹⁴¹ O objeto da ADI 3330 era declarar inconstitucional a criação do ProUni. O Ministro Relator Carlos Ayres Britto julgou improcedente a ação, sustentando que as políticas de bolsas representavam uma forma legítima de promoção da igualdade.

¹⁴² Neste emblemático caso, a empresa britânica coletou ilegalmente dados pessoais de milhares de usuários do Facebook, sem o consentimento. Esses dados foram utilizados para criar perfis psicológicos e influenciar nas decisões políticas por meio de propaganda manipulada e desinformação.

TOSCHI, Aline Seabra; LOPES, Herbert Emílio Araújo. **Dados de Tróia**. Proteção de dados pessoais e investigação criminal. 2020, p. 105.

¹⁴³ JONAS, Hans. **O Princípio Responsabilidade: ensaio de uma ética para a civilização tecnológica**. (Trad. Marijane Lisboa; Luiz Barros Montez). Rio de Janeiro: Contraponto, Ed. PUC-Rio, 2006.

¹⁴⁴ FONSECA, Reynado Soares da. **O Princípio Constitucional da Fraternidade: Seu Resgate no Sistema de Justiça**. Belo Horizonte: D'Plácido, 2019. p. 103.

Em síntese, o contexto da civilização tecnológica impõe ao Estado o dever de reconhecer o outro e garantir que a persecução penal não se torne um mecanismo de opressão. O resgate da fraternidade não é apenas simbólico, é necessário. Ela se materializa no reconhecimento de que os titulares dos dados não são objetos controláveis, mas são sujeitos de direitos. A proposta da LGPD Penal sob o paradigma da fraternidade é um resgate necessário para limitar o uso das tecnologias em prol do bem da sociedade. Portanto, ao colocar a fraternidade como um limite, é resgatada a noção de que o Estado deve proteger os seus, e não reprimi-los.

3.2. A fraternidade como resposta aos desafios na persecução penal na era digital

Assim como as novas tecnologias podem ser utilizadas para o controle informacional, afetando a democracia, elas também atuam no controle penal, de forma a segregar os perfis criminosos. A seletividade penal, nesse contexto, é maquiada por meio da legitimação do uso de algoritmos e base de dados nas persecuções penais. Nesse cenário, a criminologia crítica¹⁴⁵ aponta que o sistema penal enfrenta grandes desafios referentes à seletividade, pois a eleição de indivíduos como potencialmente criminosos com base em diferenças físicas e sociais é de grande modo influenciada pelos discursos de poder, pela mídia, pela cultura, e agora, pelas novas tecnologias. Na era digital, o uso dos algoritmos e das bases de dados de maneira ilimitada, devido a ausência de legislação que verse especificamente sobre o tema, intensifica essa problemática, materializando-se em técnicas de controle da informação que, ao invés de contribuir para o devido processo legal e a investigação de crimes, potencializa e legitima posturas discriminatórias e segregacionistas, especialmente quando se trata de grupos marginalizados e periféricos.

Diante disso, a fraternidade emerge como um princípio regulador capaz de oferecer uma resposta a tais problemáticas, como a da seletividade

¹⁴⁵ FERNANDES, Sérgio Ricardo Aquino; PELLENZ, Mayara; BASTIANI, Ana Cristina Bacega de. **Fraternidade como Alternativa à Seletividade do Direito Penal**. Florianópolis, n. 76, p. 155-182, ago. 2017. p. 16.

penal e à crise social vivenciada pelo direito penal¹⁴⁶. Ao ser incorporada pelo direito, a fraternidade fortalece a transparência na gestão da informação e no uso de dados pessoais nas investigações e nos processos penais. a presunção de inocência não pode ser um princípio ignorado na era digital a ponto de se construir uma base de dados ilimitada e seletiva. A utilização de instrumentos como o do reconhecimento facial são importantes para a prevenção e identificação de criminosos, isto é indubitável. Mas o cerne do problema é a utilização exacerbada a fins de selecionar indivíduos, violando assim diversos direitos fundamentais. A proposta da LGPD Penal, ao vedar a utilização de tecnologias de vigilância em tempo real e de forma contínua quando não há conexão com a persecução penal e sem autorização judicial reflete a necessidade de limitar e regular esses instrumentos¹⁴⁷.

A fraternidade, ao se atrelar diretamente ao princípio da dignidade humana, torna-se essencial para resgatar a responsabilidade coletiva e restituir o sistema de justiça que, mesmo na era tecnológica, garanta os direitos fundamentais, em especial o da proteção de dados pessoais, e o agir responsável do Estado. Dessa forma, tendo como base a fraternidade como paradigma regulatório da era digital, evita-se que o controle da informação se torne um mecanismo eficiente de violação de direitos. Na esfera penal, a aplicação jurídica da fraternidade manifesta-se em práticas que buscam superar a seletividade e reerguer a justiça de forma humanizada. Nisso se traduz a “justiça restaurativa”¹⁴⁸, que é a aplicação da fraternidade através do respeito aos direitos humanos e da humanização da aplicação do próprio direito penal. Por conseguinte, a aplicação do direito penal e processual penal através da fraternidade constrói um novo paradigma que é capaz de regular as complexidades que vieram com a era digital.

Portanto, urge o resgate da fraternidade como paradigma regulatório, pois, tendo em vista que a proteção dos dados pessoais é um direito fundamental, logo é um direito humano, deve ser igualmente protegida como

¹⁴⁶ FERNANDES, Sérgio Ricardo Aquino; PELLENZ, Mayara; BASTIANI, Ana Cristina Bacega de. **Fraternidade como Alternativa à Seletividade do Direito Penal**. Florianópolis, n. 76, p. 155-182, ago. 2017.

¹⁴⁷ SANTOS, Jéssica Guedes. **Reconhecimento facial: entre a criminologia, a mídia e a LGPD penal**. Internet & Sociedade, v. 2, n. 1., jun. 2021. p. 7.

¹⁴⁸ FONSECA, Reynado Soares da. **O Princípio Constitucional da Fraternidade: Seu Resgate no Sistema de Justiça**. Belo Horizonte: D'Plácido, 2019. p. 145.

qualquer outro direito. E mais, propõe-se aos legisladores tomar como base a fraternidade, a fim de se evitar potenciais crises sociais, pois desse modo, propõe-se a efetiva proteção dos direitos fundamentais. De modo mais concreto, propõe-se a criação de um marco regulatório específico conforme o modelo sugerido pelo Anteprojeto da LGPD Penal, a participação ativa do Judiciário no controle da violação da proteção de dados, a garantia de acesso a logs de funcionamento dos algoritmos pelos investigados e por seus defensores e a inserção expressa da fraternidade como princípio da LGPD Penal.

Em suma, os riscos identificados pelo uso das tecnologias na persecução penal abrangem elementos jurídicos sensíveis. Nesse sentido, a fraternidade opera como um princípio regulador das problemáticas emergentes. A regulação penal dos dados pessoais deve ir para além do consentimento, sendo construída com base na transparência, na dignidade da pessoa humana e, principalmente, na fraternidade. Ao concluir este capítulo, nota-se que a fraternidade orienta a fidelidade ao projeto constitucional de justiça. Essa é a principal contribuição de um paradigma regulatório fraterno para a proteção de dados na era digital.

CONCLUSÃO

A consolidação do direito à proteção de dados pessoais como direito fundamental pela Emenda Constitucional nº 115/2022 representa um marco relevante no enfrentamento dos desafios impostos pela era digital. No entanto, a ausência de regulamentação específica sobre o tratamento de dados na persecução penal revela, pela exclusão feita pela LGPD, uma lacuna preocupante, especialmente diante do uso crescente de tecnologias invasivas e algoritmos opacos por parte do Estado.

A monografia teve como objetivo central analisar os limites e os desafios do direito fundamental à proteção de dados na persecução penal diante do uso das novas tecnologias pelo Estado. A pesquisa partiu da construção da teoria do constitucionalismo digital, no primeiro capítulo, que se traduz em uma vertente do constitucionalismo moderno e se apresenta como uma resposta normativa às mudanças provocadas pelas tecnologias.

Essa teoria, portanto, propõe a reafirmação dos valores constitucionais do Estado Democrático de Direito no ambiente virtual.

Ainda, no primeiro capítulo, foi analisado o panorama histórico e conceitual da proteção de dados pessoais, evidenciando a sua evolução a partir do direito à privacidade, mas se fragmentando dele ao longo da história. Também foram analisados os principais marcos normativos do ordenamento jurídico brasileiro, enfatizando os aspectos principais do Marco civil da Internet, da Lei Geral de Proteção de Dados e da Emenda Constitucional nº115/2022. Com isso, foi demonstrado que o constitucionalismo digital oferece uma base teórica sólida para as normas emergentes, que versem sobre a proteção de dados.

Diante da lacuna legislativa deixada pela LGPD, o segundo capítulo analisa quais os impactos e desafios dessa ausência legislativa no âmbito penal. Assim, foram abordados os impactos das novas tecnologias na investigação criminal, destacando o surgimento do regime algorítmico e os riscos associados à discriminação algorítmica, à seletividade penal e à opacidade dos processos decisórios automatizados. A pesquisa evidenciou que, embora as tecnologias possam contribuir para a eficiência da persecução penal, sua utilização sem limites normativos compromete as garantias constitucionais essenciais. Foi realizada uma análise comparativa entre o Anteprojeto da LGPD Penal e o PL nº 1.515/2022 a qual revelou que apenas o primeiro está alinhado aos princípios do constitucionalismo digital, enquanto o segundo representa retrocessos normativos e riscos à proteção dos direitos fundamentais.

No terceiro capítulo, propôs-se o resgate da fraternidade como paradigma regulatório, compreendendo-a como valor constitucional limitador capaz de orientar a atuação estatal na era digital. A fraternidade foi apresentada como princípio regulador das relações jurídicas, especialmente no contexto da civilização tecnológica. Sua aplicação no processo penal permite superar a lógica punitivista e seletiva, promovendo uma justiça restaurativa, humanizada e comprometida com a dignidade da pessoa humana.

Dessa forma, conclui-se que a proteção de dados pessoais na persecução penal não pode ser tratada apenas como um desafio técnico ou

legislativo, mas como uma questão ética e constitucional. A proposta de um modelo regulatório fraterno, inspirado no constitucionalismo fraternal, representa uma alternativa viável e necessária para compatibilizar a inovação tecnológica com a justiça, as garantias fundamentais e a humanidade. Portanto, o impacto da pesquisa reside na contribuição para o debate jurídico e acadêmico contemporâneo sobre os limites da atuação estatal na era digital e na proposição de um novo paradigma regulatório que retrate o humanismo nas relações sociais.

REFERÊNCIAS BIBLIOGRÁFICAS

ARAÚJO, Rômulo de Aguiar; CARDOSO, Naiara Deperon; PAULA, Amanda Marcélia. **Regulação e uso do reconhecimento facial na segurança pública do Brasil**. Revista de Doutrina Jurídica, Brasília, v. 112, p. 5. 2021.

ARMANDO, Coronel. **PL 1515/2022**. Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais. Disponível em: [Portal da Câmara dos Deputados](https://portal.camara.gov.br/legis/pl1515-2022). Acesso em: 3 jul. 2025.

ARRUDA, Ana Julia Pozzi; RESENDE, Ana Paula Bougleux Andrade; FERNANDES, Fernando Andrade. **Sistemas de Policiamento Preditivo e Afetação de Direitos Humanos à Luz da Criminologia Crítica**, Revista de Direito Público, Brasília, v. 18, n. 100, p. 664-689, out.-dez. 2021. p. 664.

AZEVEDO, Cynthia Picolo Gonzaga de et al. **Nota técnica: análise comparativa entre o anteprojeto de LGPD penal e o PL 1515/2022**. Instituto de Referência em Internet e Sociedade (IRIS) e Laboratório de Políticas Públicas e Internet (LAPIN), nov. 2022. p. 21.

BAGGIO, Antonio Maria. A idéia de fraternidade em duas Revoluções: Paris 1789 e Haiti 1791. **O princípio esquecido: A fraternidade na reflexão atual das ciências políticas**. Tradução: Durval Cordas, Iolanda Gaspar, José Maria de Almeida. Vargem Grande Paulista. São Paulo: Cidade Nova, 2008. v. 1, p. 54.

BAUMAN, Zygmunt. **Modernidade líquida**. Tradução de Plínio Dentzien. Rio de Janeiro: Zahar, 2001.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019.

BOBBIO, Norberto. **Teoria do Ordenamento Jurídico**. 6. ed. Apresentação: Tércio Sampaio Ferraz Júnior. Tradução: Maria Celeste C. J. Santos; rev. téc: Cláudio de Cicco. Brasília: Universidade de Brasília. 1995.

BONAVIDES, Paulo. **Curso de Direito Constitucional**. 19. ed. São Paulo: Malheiros, 2006. p. 563–564.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 1515, de 7 de junho de 2022**. Estabelece Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, defesa nacional, segurança pública, investigação e repressão de infrações penais. Apresentado por Coronel Armando (PL-SC). Brasília, 7 jun. 2022. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2326300> Acesso em: 11 jul. 2025.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidente da República, [2016]. Disponível em: https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm Acesso em 11 jul. 2025.

BRASIL. **Crimes digitais sobem 45% e Senado tem propostas para frear sequestro de dados**. Rádio Senado, Brasília, 16 jan. 2025. Disponível em: <https://www12.senado.leg.br/radio/1/noticia/2025/01/16/crimes-digitais-sobem>

[-45-e-senado-tem-propostas-para-frear-sequestro-de-dados](#). Acesso em: 17 jun. 2025.

BRASIL. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e fixa a competência privativa da União para legislar sobre a matéria. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm Acesso em: 11 jul. 2025.

BRASIL. **Lei nº 12.414, de 9 de junho de 2011**. Dispõe sobre a formação e consulta a bancos de dados com informações de adimplemento de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Diário Oficial da União: seção 1, Brasília, DF, ano 148, n. 109, p. 1, 10 jun. 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 1 jul. 2025.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, ano 148, n. 222, p. 1, 18 nov. 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 1 jul. 2025.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. *Diário Oficial da União*: seção 1, Brasília, DF, ano 151, n. 77, p. 1, 24 abr. 2014. Disponível em: [L12965](#) Acesso em: 11 jul. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: seção 1, Brasília, DF, ano 155, n. 157, p. 1-3, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 1 jul. 2025.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, p. 1, 12 set. 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/Leis/L8078compilado.htm Acesso em: 11 jul. 2025.

BRASIL. Ministério da Justiça e Segurança Pública. **Anteprojeto de Lei Geral de Proteção de Dados Pessoais para Fins de Segurança Pública, Defesa Nacional e Atividades de Investigação Criminal**. Brasília, 2022. Disponível em: <https://www.conjur.com.br/dl/an/anteprojeto-lei-disciplina-protecao.pdf>. Acesso em: 11 jul. 2025.

BRASIL. Superior Tribunal de Justiça. **Recurso Ordinário em Habeas Corpus 51.531**. Relator: Min. Nefi Cordeiro. Disponível em: [https://scon.stj.jus.br/SCON/pesquisar.jsp?i=1&b=ACOR&livre=\(\(%27RHC%2](https://scon.stj.jus.br/SCON/pesquisar.jsp?i=1&b=ACOR&livre=((%27RHC%2)

[7.clap.+e+@num=%2751531%27\)+ou+\(%27RHC%27+adj+%2751531%27\).suce.\)&thesaurus=JURIDICO&fr=veja](#). Acesso em: 11 jul. 2025

BRASIL. Superior Tribunal de Justiça. **Recurso Ordinário em Habeas Corpus 89.981**. Relator: Min. Reynaldo Soares da Fonseca. Disponível em: [STJ - Jurisprudência do STJ](#). Acesso em: 11 jul. 2025.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade 3330**, Relator: Min. Carlos Ayres Britto. Disponível em: [Pesquisa de jurisprudência - STF](#) Supremo Tribunal Federal. Acesso em: 26 jun. 2025.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade 5059**. Relator: Min. Dias Toffoli. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=4483504> Acesso em: 11 jul. 2025.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade 6387**. Relatora: Min. Rosa Weber. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165> Acesso em: 11 jul. 2025.

BRASIL. Supremo Tribunal Federal. **Habeas Corpus 168.052**. Relator: Min. Gilmar Mendes. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=5635177> Acesso em: 11 jul. 2025.

BRASIL. Supremo Tribunal Federal. **Habeas Corpus 222.141**. Relator: Min. Gilmar Mendes. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=6516957> Acesso em: 11 jul. 2025.

BRASIL. Supremo Tribunal Federal. **Habeas Corpus 91.867**. Relator: Min. Gilmar Mendes. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=2534858>. Acesso em: 11 jul. 2025.

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário com Agravo 1.042.07**. Relator: Min. Dias Toffoli. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=5173898>. Acesso em: 11 jul. 2025.

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário 1.301.250**. Relatora: Min. Rosa Weber. Disponível em: [Supremo Tribunal Federal](#). Acesso em: 11 jul. 2025.

BURKET, Hebert. **Privacy-Data Protection: a German/European perspective**. In.: ENGEL, C.; KELLER, K. H. (ed). Governance of Global Networks in the Light of Differing Local Values. Baden-Baden: Nomos, 2000. p. 46. Tradução livre.

CALABRICH, Bruno Freire de Carvalho. **Discriminação algorítmica e transparência na lei geral de proteção de dados pessoais**. Revista de Direito e as Novas Tecnologias, v. 8, jul.-set. 2020.

CELESTE, Edoardo. **Constitucionalismo Digital: Mapeando A Resposta Constitucional Aos Desafios Da Tecnologia Digital**. Direitos Fundamentais & Justiça, Belo Horizonte, ano 15, n. 45, p. 63-91, jul./dez. 2021.

CHUY, José Fernando Moraes. **O sistema de Investigação Brasileiro, a “LDGP Penal” e a Efetiva Garantia de Direitos Fundamentais.** p. 1. Disponível em: https://web.adpf.org.br/wp-content/uploads/2021/03/2-Artigo_JOSE-FERNANDO-MORAES-CHUY.pdf. Acesso em 2 de jul. 2025.

DAGUER, Beatriz; BORRI, Luiz Antonio; SOARES, Rafael Junior. **O reconhecimento facial na segurança pública e a proteção de dados pessoais como garantia fundamental.** Revista de Direito e as Novas Tecnologias. São Paulo: RT. v. 16, jul.-set. 2022.

DONEDA, Danilo. **Panorama histórico da proteção de dados pessoais.** In: DONEDA, Danilo; MENDES, Laura Schertel; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz (coord.). Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021. p. 3–20.

FARIA, Ana Cláudia Rodrigues de; FONSECA, Reynaldo Soares da. **Os desafios do constitucionalismo digital.** In: NEVES, Luciana Sabbatine; FARIA, Ana Cláudia Rodrigues de (Orgs.). Estudos sobre as aplicações jurídicas da fraternidade: uma homenagem aos Professores Reynaldo Soares da Fonseca e Marcelo Navarro Ribeiro Dantas. Porto Alegre: Fundação Fênix, 2024. p. 29-52.

FERNANDES, Sérgio Ricardo Aquino; PELLENZ, Mayara; BASTIANI, Ana Cristina Bacega de. **Fraternidade como Alternativa à Seletividade do Direito Penal.** Florianópolis, n. 76, p. 155-182, ago. 2017.

FERREIRA, André da Rocha. **Tratamento de dados pessoais em investigações criminais: o direito fundamental à autodeterminação informativa como limite constitucional.** Revista Brasileira de Ciências Criminais, v. 185. ano 29. p. 115-159. São Paulo: RT, nov. 2021. p. 141.

FONSECA, Reynaldo Soares da. **A Democracia Fraternal na Era Digital.**

FONSECA, Reynaldo Soares da. **O Princípio Constitucional da Fraternidade: Seu Resgate no Sistema de Justiça.** Belo Horizonte: D'Plácido, 2019.

FONSECA, Reynaldo Soares da; PAULA, Bruno Fernandes de. **Da privacidade à proteção de dados pessoais: fundamentos teóricos e evolução histórica.** Ver-o-Direito: revista de direito público com ênfase na competência da justiça federal, v. 4, n. 1, jul. 2021.

FONSECA, Reynaldo Soares da; ROSSETTO, Geralda Magella de Faria. **Dívida Fraternal E Política Compensatória: O Dilema Da Proteção, Promoção E Defesa Dos Direitos Humanos Na Civilização Tecnológica.**

FUX, Luiz; FONSECA, Gabriel Campos Soares da. **Segurança da informação e proteção de dados como pressupostos para o Poder Judiciário na era digital: uma análise da Resolução CNJ 361/2020 e da Resolução STF 724/2020.** In: BARATA, Bruno; ALMEIDA, Laryssa; FROTA, Leandro. (Coord.). **Ensaio sobre a transformação digital no direito: estudos em homenagem ao Ministro Kássio Nunes Marques.** Brasília: OAB Editora, 2021.

GARCIA, Rafael de Deus. **Um velho direito à privacidade para um novo tipo de policiamento: algoritmos e inteligência artificial no processo penal e na segurança pública.** 2021.

HECK, Ralph Leal. **Algoritmos que nos governam: reflexões filosóficas sobre propriedades críticas da atual estrutura da revolução informacional.** *Philosophos - Revista de Filosofia*, Goiânia, v. 29, n. 1, 2024. DOI: 10.5216/phi.v29i1.78173. Disponível em: <https://revistas.ufg.br/philosophos/article/view/78173>. Acesso em: 17 jul. 2025.

JONAS, Hans. **O Princípio Responsabilidade: ensaio de uma ética para a civilização tecnológica.** (Trad.: Marijane Lisboa; Luiz Barros Montez). Rio de Janeiro: Contraponto, PUC-Rio, 2006.

LANGOSKI, Deisemara Turatti. BRAUN, Helenice da Aparecida Dambrós. **Ressignificação Direitos Humanos Fundamentais sob o prisma do Multiculturalismo e da Fraternidade.** p. 1170.

MAGALHÃES, Alice Azevedo; GOMES, Tércio Spínola. **Regulação de sistemas de reconhecimento facial para fins de segurança pública no Brasil: riscos e desafios.** *Revista Humanidades & Inovação*, v. 8, n. 47, 2021. p. 174.

MENDES, Gilmar; FERNANDES, Victor Oliveira. **Constitucionalismo Digital e Jurisdição Constitucional: uma agenda de pesquisa para o caso brasileiro.** *Revista Justiça do direito*, v. 3, n. 2, p. 6-51, maio-agosto, 2020.

MENDRONI, Marcelo Batlouni. **Curso de investigação criminal.** 3. ed. rev. e amp. São Paulo: Atlas, 2013.

MONTEIRO, Guilherme Ornelas. **Instrumentos de reconhecimento facial e os contornos da lei geral de proteção de dados ante a privacidade nas cidades (in)inteligentes.** *Revista de Direito e Atualidades*, v. 1, n. 1, jan.-mar. 2021. p. 35.

NEVES, Cleuler Barbosa; MATOS, Gisele Gomes. **LGPD Penal e a lacuna regulatória para o tratamento dos dados pessoais para fins de criminais: APL e PL 1515/2022.** *Revista Caderno Pedagógico – Studies Publicações e Editora Ltda., Curitiba*, v. 22, n. 7, p. 1-30. 2025.

PONTE, Amanda Leite de Farias. **Da necessidade de limites ao tratamento e compartilhamento de dados por órgãos de inteligência do Estado à luz da Lei Geral de Proteção de Dados em matéria penal.** *Caderno Virtual*, Brasília, v. 1, n. 54, 2022.

RODRIGUES, Luiz Fernando. **A importância do compartilhamento de dados pessoais para fins de investigação criminal e os possíveis reflexos da LGPD.** In: ARAS, Vladimir B.; MENDONÇA, Andrey B.; CAPANEMA, Walter Aranha; SILVA, Carlos Bruno F. da; COSTA, Marcos Antônio da S. (org.) *Proteção de Dados Pessoais e Investigação Criminal*. Ministério Público Federal. Brasília: ANPR, 2020.

ROSA, Raíssa Roese. **O Anteprojeto da Lgpd Penal e a Necessidade de Cooperação Internacional para o Compartilhamento Extraterritorial de**

Dados Pessoais para Fins Penais. 2022. Monografia (Pós-Graduação) - Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa.

SANTOS, Jéssica Guedes. **Reconhecimento facial entre a criminologia, a mídia e a LGPD penal.** Internet & Sociedade, v. 2, n. 1, jun. 2021.

SARLET, Ingo Wolfgang. **Fundamentos Constitucionais: o Direito Fundamental à Proteção de Dados.** In: DONEDA, Danilo; MENDES, Laura Schertel; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz (coord.). Tratado de proteção de dados pessoais. 2. ed. Rio de Janeiro: Forense, 2023.

SCHWABE, Jürgen; MARTINS, Leonardo. **Cinquenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão.** Decisão do Tribunal Constitucional alemão de 1983 Montevideo: Konrad AdenauerStiftung, 2005, pp. 233-245. Disponível em: http://www.kas.de/wf/doc/kas_7738-544-1-30.pdf. Acesso em: 30 jun. 2025. p. 237

SILVA NETO, Arthur Corrêa da. **Dos impactos do julgamento no STF no RE 1.301.250: caso Marielle Franco.** Consultor Jurídico, São Paulo, 3 abr. 2025. Disponível em: www.conjur.com.br. Acesso em: 3 jul. 2025.

TOSCHI, Aline Seabra; LOPES, Herbert Emílio Araújo. **Dados de Tróia.** Proteção de dados pessoais e investigação criminal. 2020, p. 105.

UNIÃO EUROPEIA. **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.** Jornal Oficial das Comunidades Europeias, L 281, p. 31-50, 23 out. 1995. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046>. Acesso em: 1 jul. 2025.

UNITED STATES. Supreme Court of the United States. **Katz v. United States, 389 U.S. 347 (1967).** Disponível em: <https://supreme.justia.com/cases/federal/us/389/347/>. Acesso em: 1 jul. 2025.

UNITED STATES. Supreme Court of the United States. **Olmstead v. United States, 277 U.S. 438 (1928).** Disponível em: <https://supreme.justia.com/cases/federal/us/277/438/>. Acesso em: 1 jul. 2025.

VIOLA, Mário; HERINGER, Leonardo; CARVALHO, Celina. **O Anteprojeto da LGPD Penal e as regras sobre transferência internacional de dados pessoais.** Instituto de Tecnologia & Sociedade do Rio. Agosto, 2021.

WARREN, Samuel; BRANDEIS, Louis. **The right to privacy.** Harvard Law Review, v. 4, n. 5, p. 193-220, 15 dez. 1890. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/download/127/97>. Acesso em: 1 de jul. de 2025.