Revista Brasileira de **CIÊNCIAS CRIMINAIS**

BRAZILIAN CRIMINAL SCIENCES REVIEW

Ano 33 • vol. 211 • nov./dez. 2025

Dossiê Especial: "Proteção de Dados Pessoais e Ciências Criminais"

Prof. Dr. Rodrigo Oliveira de Camargo (Org.)
Prof. Dr. Carlos Hélder Carvalho Furtado Mendes (Org.)

REVISTA BRASILEIRA DE
CIÊNCIAS CRIMINAIS
Ano 33 • vol. 211 • nov./dez. 2025

Presidência
Antonio Pedro Melchior

Coordenação
André Nicolitt

EQUIPE EDITORIAL DA REVISTA – IBCCRIM

Coordenador editorial: Willians Meneses (Instituto Brasileiro de Ciências Criminais, IBCCRIM, São Paulo/SP)

Editor-científico chefe: Prof. Dr. André Nicolitt (Faculdade de Direito da Universidade Federal Fluminense, UFF, Rio de Janeiro/RJ)

Editores científicos-assistentes: Prof. Dr. Bruno Silveira Rigon, Prof. Dr. Carlos Hélder Carvalho Furtado Mendes (Centro Universitário, UNDB, São Luiz/MA), Profa. Dra. Ana Carolina Filippon Stein (Centro Universitário Metodista, IPA, Porto Alegre/RS) , Prof. Dr. Douglas Borges de Vasconcelos (Universitat Pompeu Fabra, UPF, Espanha), Profa. Dra. Ellen Cristina Carmo Rodrigues Brandão (Universidade Federal de Juiz de Fora, UFJF, Juiz de Fora/MG), Prof. Dr. Gustavo Noronha de Ávila (Pontifícia Universidade Católica do Paraná, PUCPR, Curitiba/PR), Profa. Dra. Junya Rodrigues Barletta (Universidade Federal do Rio de Janeiro, UFRJ, Rio de Janeiro/RJ), Prof. Dr. Luiz Gabriel Batista Neves (Universidade Federal da Bahia, UFBA, Salvador/BA), Profa. Dra. Maria Auxiliadora Minahim (Universidade Federal da Bahia, UFBA, Salvador/BA), Me. Maria Brito Alves (Instituto Brasileiro de Ciências Criminais, IBCCRIM, Brasília/DF) Prof. Dr. Nestor Araruna Santiago (Universidade de Fortaleza, UNIFOR, Fortaleza/CE), Profa. Dra. Renata Almeida da Costa (Univesidade La Salle, Canoas/RS), Dr. Rodrigo Oliveira de Camargo (Pontifícia Universidade Católica do Rio Grande do Sul, PUCRS, Porto Alegre/RS), Prof. Dr. Taiguara Líbano Soares e Souza (Universidade Federal Fluminense, UFF, Rio de Janeiro/RJ) e Prof. Dr. Vitor Stegemann Dieter (Instituto de Criminologia e Política Criminal, ICPC, Curitiba/PR)

Assistente Editorial: Gustavo Marcelino de Souza (Instituto Brasileiro de Ciências Criminais, IBCCRIM, São Paulo/SP)

CONSELHO EDITORIAL

Adolfo Ceretti (Università degli Studi di Milano-Bicocca, Itália)
Afranio da Silva Jardim (UERJ, Rio de Janeiro/RJ)
Alejandro Aponte (Pontificia Universidad Javeriana, Colômbia)
Alessandra Rapacci Mascarenhas Prado (Universidade Federal da Bahia, UFBA, Salvador/BA)
Anabela Miranda Rodrigues (Universidade de Coimbra, Portugal)
Ana Isabel Pérez Cepeda (Universidade de Salamanca, Espanha)
Ana Messuti (Instituto Vasco de Criminologia, Espanha)
Antonio José Teixeira Martins (Universidade Federal do Rio de Janeiro, UFRJ, Rio de Janeiro/RJ)
Antonio Magalhães Gomes Filho (USP, São Paulo/SP)
Antonio Scarance Fernandes (USP, São Paulo/SP)
Antonio Vercher Noguera (Universidade de Salamanca, Espanha)
Aury Lopes Jr. (Pontifícia Universidade Católica do Rio Grande do Sul, PUCRS, Porto Alegre/RS)
Beatriz Corrêa Camargo (Universidade Federal de Uberlândia, UFU, Uberlândia/MG)
Bernardo del Rosal Blasco (Universidade de Alicante, Espanha)
Carlos María Romeo-Casabona (Universidad del País Vasco, Espanha)
Cláudia Maria Cruz Santos (Universidade de Coimbra, Portugal)
Cornelius Prittwitz (Universidade Johann Wolfgang Goethe de Frankfurt, Alemanha)
David Baigún (Universidad de Buenos Aires, Argentina)
Edmundo Hendler (Universidad de Buenos Aires, Argentina)
Emilio Garcia Mendez (Universidad de Buenos Aires, Argentina)
Ernesto Calvanese (Università degli Studi di Milano, Itália)
Esther Gimenez-Salinas I Colomer (Universidad Ramon Llull, ESADE, Espanha)
Eugenio Raúl Zaffaroni (Universidad de Buenos Aires Argentina)
Fernanda Regina Vilares (FGV, FGVSP, São Paulo/SP)
Fernando Acosta (University of Ottawa, Canadá)
Fernando Santa Cecília Garcia (Universidade Complutense de Madrid, Espanha)
Francisco Muñoz Conde (Universidad Pablo de Olavide, Espanha)
Geraldo Prado (UFRJ, Rio de Janeiro/RJ)
Guilherme Francisco Ceolin (Centro Universitário de Brasília, UniCEUB, Brasília/DF)
Helena Regina Lobo da Costa (Universidade de São Paulo, USP, São Paulo/SP)
Heloisa Estellita (Fundação Getulio Vargas, FGVSP, São Paulo/SP)
Iasevoli Clelia (Universita' Degli Studi di Napoli, Itália)
Ignacio Berdugo Gómez de La Torre (Universidad de Salamanca, Espanha)
Iñaki Rivera Beiras (Universidad de Barcelona, Espanha)
Iván Navas Mondaca (Universidad San Sebastián, Chile)
Jésus-María Silva Sánchez (Universidad Pompeu Fabra, Espanha)
João Pedroso (Universidade de Coimbra, Portugal)
Jorge de Figueiredo Dias (Universidade de Coimbra, Portugal)
José Francisco de Faria Costa (Universidade de Coimbra, Portugal)
Juan Felix Marteau (Universidad de Buenos Aires, Argentina)
Juan Pablo Montiel (Universidad de San Andrés, Argentina)
Juarez Cirino dos Santos (UFPR, Curitiba/PR)
Juarez Tavares (UERJ, Rio de Janeiro/RJ)
Kai Ambos (Georg-August-Universität Göttingen, Alemanha)
Leandro Ayres França (Pontifícia Universidade Católica do Rio Grande do Sul, PUCRS, Porto Alegre/RS)
Luis Alberto Arroyo Zapatero (Universidad de Castilla-La Mancha, Espanha)
Luis Fernando Niño (Universidad de Buenos Aires, Argentina)
Luiz Regis Prado (UEM, Maringá/PR)

Maria Paz Arenas Rodrigañez (Universidade Complutense de Madrid, Espanha)
Manuel da Costa Andrade (Universidade de Coimbra, Portugal)
Maria João Antunes (Universidade de Coimbra, Portugal)
Mariângela Gama de Magalhães Gomes (Universidade de São Paulo, USP, São Paulo/SP)
Marina Pinhão Coelho Araujo (Insper Instituto de Ensino e Pesquisa, INSPER, São Paulo/SP)
Mauricio Martínez Sánchez (Universidad Libre, Colômbia)
Máximo Sozzo (Universidad Nacional del Litoral, Argentina)
Miguel Reale Júnior (USP, São Paulo/SP)
Nicolás Rodríguez García (Universidad de Salamanca, Espanha)
Nilo Batista (UERJ, Rio de Janeiro/RS)
Pedro Caeiro (Universidade de Coimbra, Portugal)
Olga Spinoza (Universidade do Chile, Chile)
Pilar Gomes Pavón (Universidade Complutense de Madrid, Espanha)
Raúl Cervini (Universidade da República do Uruguai, Uruguai)
Salo de Carvalho (Universidade Federal do Rio de Janeiro, UFRJ, Rio de Janeiro/RJ)
Sergio Moccia (Università di Napoli Federico II, Itália)
Sérgio Salomão Shecaira (Universidade de São Paulo, USP, São Paulo/SP)
Stella Maris Martinez (Universidad de Buenos Aires, Argentina)
Urs Kindhäuser (Universidad de Bonn, Alemanha)
Vicente Greco Filho (USP, São Paulo/SP)

CORPO DE PARECERISTAS (DESTE NÚMERO)

Bruno Shimizu (Defensoria Pública do Estado de São Paulo, DPESP, São Paulo)
Catiane Steffen (Pontifícia Universidade Católica do Rio Grande do Sul, PUCRS, Rio Grande do Sul)
Fernando Hoffmam (Universidade Federal de Santa Maria, UFSM, Rio Grande do Sul)
José Roberto Wanderley de Castro (Centro Universitário Maurício de Nassau, Uninassau, Pernambuco)
Leonardo Lacerda Alves (Centro Federal de Educação Tecnológica de Minas Gerais, Cefet-MG, Minas Gerais)
Luísa Walter da Rosa (Universidade de São Paulo, USP, São Paulo)
Luiz Eduardo Cani (Fundação Universidade Regional de Blumenau, Furb, Santa Catarina)
Luigi Giuseppe Barbieri Ferrarini (Universidade São Judas Tadeu, USJT, São Paulo)
Rafael Junior Soares (Pontifícia Universidade Católica do Paraná, PUCPR, Paraná)
Ramiro Gomes von Saltiel (Pontifícia Universidade Católica do Rio Grande do Sul, PUCRS, Rio Grande do Sul)

AUTORES(AS) (DESTE NÚMERO)

Anderson Pires Giampaoli (Academia de Polícia "Dr. Coriolano Nogueira Cobra" do Estado de São Paulo, Acadepol, São Paulo)
André Luís Callegari (Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, IDP, Distrito Federal)
Augusto Jobim do Amaral (Pontifícia Universidade Católica do Rio Grande do Sul, PUCRS, Rio Grande do Sul)
Araceli Martins Beliato (Universidade de São Paulo, USP, São Paulo)
Gabriel Saad Travassos (Pontifícia Universidade Católica do Rio Grande do Sul, PUCRS, Rio Grande do Sul)
Jamilla Monteiro Sarkis (Pontifícia Universidade Católica do Rio Grande do Sul, PUCRS, Rio Grande do Sul)
José Guimarães Mendes Neto (Centro Universitário UNDB, Maranhão)
Luiz Eduardo Cani (Fundação Universidade Regional de Blumenau, Furb, Santa Catarina)
Paola Alcântara Lima Dumont (Pontifícia Universidade Católica de Minas Gerais, PUC-MG, Minas Gerais)
Rafael Francisco Marcondes de Moraes (Academia de Polícia "Dr. Coriolano Nogueira Cobra" do Estado de São Paulo, Acadepol, São Paulo)
Roberta de Lima e Silva (Pontifícia Universidade Católica do Rio Grande do Sul, PUCRS, Rio Grande do Sul)
Samuel Andreatta (Pontifícia Universidade Católica do Rio Grande do Sul, PUCRS, Rio Grande do Sul)
Thallita Gabriele Lopes Lima (Pontifícia Universidade Católica do Rio de Janeiro, PUCRJ, Rio de Janeiro)

Indexadores / Indexes



Bases de dados / Data bases







Bibliotecas / Libraries



As opiniões expressas nos artigos são de responsabilidade dos autores.
Revista Brasileira de Ciências Criminais
revista@ibccrim.org.br – www.ibccrim.org.br

ISSN (Impresso): 1415-5400
ISSN (Eletrônico): 2965-3967

Revista Brasileira de CIÊNCIAS CRIMINAIS

Ano 33 • vol. 211 • nov./dez. 2025

Coordenação (editor-chefe)
André Nicolitt

Publicação oficial do
Instituto Brasileiro de Ciências Criminais

IBCCRIM

Revista dos Tribunais

Thomson Reuters™

ISSN (Impresso): 1415-5400
ISSN (Eletrônico): 2965-3967

Revista Brasileira de CIÊNCIAS CRIMINAIS

Ano 33 • vol. 211 • nov./dez. 2025

Presidência
Antonio Pedro Melchior

Coordenação (editor-chefe)
André Nicolitt

Os colaboradores desta Revista gozam da mais ampla liberdade de opinião e de crítica, cabendo-lhes a responsabilidade das ideias e conceitos emitidos em seus trabalhos.

© edição e distribuição da
Thomson Reuters Brasil Conteúdo e Tecnologia Ltda.

Juliana Mayumi Ono
Diretora Responsável

Av. Dra. Ruth Cardoso, 7815 – 6º Andar – Pinheiros
CEP 05425-905, São Paulo, SP, Brasil

TODOS OS DIREITOS RESERVADOS. Proibida a reprodução total ou parcial, por qualquer meio ou processo – Lei 9.610/1998.

CENTRAL DE RELACIONAMENTO THOMSON REUTERS SELO REVISTA DOS TRIBUNAIS
(atendimento, em dias úteis, das 09h às 18h)
Tel. 0800-702-2433

e-mail de atendimento ao consumidor: sacrt@thomsonreuters.com
e-mail para submissão dos originais: revista@ibccrim.org.br

Conheça mais sobre Thomson Reuters: www.thomsonreuters.com.br

Acesse o nosso *eComm*
www.livrariart.com.br

Impresso no Brasil: [11-2025]
Profissional
Fechamento desta edição: [13.10.2025]



Instituto Brasileiro de Ciências Criminais

Diretoria da Gestão 2025/2026

DIRETORIA EXECUTIVA

PRESIDENTE
Antonio Pedro Melchior
1ª Vice-Presidente
Carina Quito
2ª Vice-Presidente
Camila Torres Cesar
1ª Secretária
Julia Baroli Sadalla
2ª Secretária
Claudia Cristina Barrilari
3º Secretário
Bruno Shimizu

1º Tesoureiro
Vinícius de Souza Assumpção
2ª Tesoureira
Raquel Lima Scalcon
1º Diretor Nacional das Coordenadorias Regionais e Estaduais
Luiz Gabriel Batista Neves
2º Diretor Nacional das Coordenadorias Regionais e Estaduais
Marcelo Almeida Ruivo dos Santos
3º Diretor Nacional das Coordenadorias Regionais e Estaduais
Roberto Moura

CONSELHO CONSULTIVO

MEMBROS
Anamaria Prates
Bruno Salles Pereira Ribeiro
Cleifson Dias Pereira
Helena Regina Lobo da Costa
Renato Stanziola Vieira
Silvia Virginia Silva de Souza

OUVIDORA
Fernanda Pascoal Valle Bueno de Castilho

CONSELHO DE DIVERSIDADE

MEMBROS
Andre Pires de Andrade Kehdi
Clarice Beatriz
Débora Viviane
Isadora Brandão
Lúcia Ribeiro
Marcio Romualdo
Maria Sylvia de Oliveira
Michael Mary Nolan
Priscila França
Priscila Pamela C. Santos

DEPARTAMENTOS

ACESSIBILIDADE
Aline Cruz
AMICUS CURIAE
Juliano Breda
BIBLIOTECA
Marcela Diorio
BOLETIM
Ana Cristina Gomes
CONVÊNIOS NACIONAIS
Maria Brito
CONVÊNIOS INTERNACIONAIS
Maria Brito
CURSOS
Fernando Gardinali
ESTUDOS E PROJETOS LEGISLATIVOS
Chiavelli Falavigna
CURSOS IBCCRIM, COIMBRA
Claudia Barrilari
GRUPO DE ESTUDOS AVANÇADOS (GEAS)
Nicole Muffone
INFÂNCIA E JUVENTUDE
Ana Paula Freitas
INICIAÇÃO CIENTÍFICA (LABORATÓRIOS)
Rodrigo Martins
JUSTIÇA E SEGURANÇA PÚBLICA
Roberto Moura
JUSTIÇA RESTAURATIVA
Luiz Gabriel Batista
MONOGRAFIAS
Andrea Cristina D'Angelo
NOVAS TECNOLOGIAS NA JUSTIÇA PENAL
Maíra Fernandes
POLÍTICA DE DROGAS
Julia Sadalla
REVISTA BRASILEIRA DE CIÊNCIAS CRIMINAIS
Andre Nicolitt
SISTEMA PRISIONAL
Mariana Py

COMISSÃO ORGANIZADORA

31º SEMINÁRIO INTERNACIONAL DE CIÊNCIAS CRIMINAIS – PRESIDENTES
PRESIDÊNCIA
Mariângela Gama de Magalhães Gomes
COMISSÃO
Álvaro Roberto Antanavicius Fernandes
Carolina Costa
Chiavelli Facenda Falavigno
Diogo Rudge Malan
Fernanda Prates Fraga
Francisco Alessandro de Oliveira Araújo
Jamilla Monteiro Sarkis
Luis Fernando Niño
Marcus Alan de Melo Gomes
Maria Carolina de Melo Amorim
Marina Pinhão Coelho Araújo
Marta Saad
Vinícius Gomes de Vasconcellos

EQUIPE DO IBCCRIM

NÚCLEOS DE PUBLICAÇÕES

SUPERVISÃO
Willians Meneses
EQUIPE
Gustavo Marcelino de Souza

NÚCLEO DE ADMINISTRAÇÃO, EDUCAÇÃO E BIBLIOTECA

SUPERVISÃO
Fernanda Barreto
EQUIPE
Alexandre Soledade de Oliveira
Ana Paula da Silva
Hegle Borges da Silva
Mariana Xavier
Vanessa dos Santos Lima
Sara Lemos de Oliveira

NÚCLEO FINANCEIRO

SUPERVISÃO
Paulo Márcio
EQUIPE
Andrea Pereira dos Santos

Instituto Brasileiro de Ciências Criminais (IBCCRIM) | www.ibccrim.org.br
Rua Onze de Agosto, 52, 6º andar, São Paulo, SP. CEP 01018-000

Revista Brasileira de
CIÊNCIAS CRIMINAIS

Ano 33 • vol. 211 • nov./dez. 2025

Diretora de Conteúdo e Operações Editoriais
Juliana Mayumi Ono

Gerentes de Conteúdo
Camilla Furegato da Silva
Fernanda Beatriz de Oliveira de Faria Bernardi

Especialistas Editoriais
Angela Bottene Daniel
Juliana Cornacini Ferreira

Editora: Amanda Rodrigues Juvêncio

Analistas de Operações Editoriais: Alexandre da Cruz Teixeira, Ana Carolina Borges, Diogo Travassos Ferreira, Fernanda Lourenço Pinto Bini, Gustavo Capabianco, Igor Taga, John Carlos Farias, Júlia Palhardi Ataide, Juliana Honorato, Natalia Andrade dos Anjos Munhoz, Sabrinny Nogueira Vieira, Stella Correa da Cunha Martins e Tuani Menezes

Analista de Qualidade Editorial: Ariene Cristina Almeida do Nascimento

Analista de Projetos: Bruna Galdino

Estagiárias: Camila Morais, Giovanna Massavelli, Luana Simplicio e Mariana Campos

Capa: Andréa Cristina Pinto Zanardi

Adaptação de Capa: Linotec

Gerente de Operações e Produção Gráfica
Mauricio Alves Monte

Analistas de Produção Gráfica: Jéssica Maria Ferreira Bueno e Victória Menezes Pereira

Sua opinião é importante para nós!

Prezado(a) Cliente,

Como assinante das nossas Revistas, você faz parte de uma comunidade que valoriza a tradição e a qualidade que imprimimos em cada edição.

Para continuarmos aprimorando nossos serviços e garantindo que nossas Revistas atendam às suas expectativas, gostaríamos de convidá-lo(a) a participar de uma breve pesquisa. Sua opinião é fundamental para nós, e suas respostas nos ajudarão a entender melhor suas preferências e necessidades.

A pesquisa é rápida e fácil de responder, e suas respostas serão tratadas com total confidencialidade. Agradecemos antecipadamente por dedicar um pouco do seu tempo para nos ajudar a melhorar ainda mais nossas publicações.

Acesse o *QR code* abaixo para iniciar a pesquisa:

Thomson Reuters – Revista dos Tribunais

Sumário

Editorial

Dossiê "Proteção de dados pessoais e Ciências Criminais": prólogo de uma formação jurídico-penal

Dossier "Personal data protection and criminal sciences": prologue to a legal-criminal education

Prof. Dr. Rodrigo Oliveira de Camargo (Org.) e Prof. Dr. Carlos Hélder Carvalho Furtado Mendes (Org.) 17

Dossiê "Proteção de Dados Pessoais e Ciências Criminais"

Da nuvem à corte: o julgamento constitucional da prova penal invisível

From the cloud to the courtroom: the constitutional review of invisible criminal evidence

José Guimarães Mendes Neto e André Luís Callegari 25

Compartilhamento de dados financeiros na persecução penal

Financial data sharing in criminal prosecution

Luiz Eduardo Cani 51

Faces make cases: o caso *Clearview AI* e os desafios do uso de tecnologias algorítmicas no sistema de justiça criminal brasileiro

"Faces make cases": the Clearview AI case and the challenges of using algorithmic technologies in the Brazilian criminal justice system

Thallita Gabriele Lopes Lima 85

Devida investigação criminal: compromissos epistêmicos e probatórios na extração de dados pessoais em fontes abertas

Due criminal investigation: epistemic and evidential commitments in the extraction of personal data from open sources

Anderson Pires Giampaoli, Rafael Francisco Marcondes de Moraes e Roberta de Lima e Silva 115

Reconhecimento facial: biopolítica granular e controle customizado no Brasil

Facial recognition: granular biopolitics and customized control in Brazil

Gabriel Saad Travassos e Augusto Jobim do Amaral 143

O uso da inteligência artificial na predição do feminicídio e o direito à explicabilidade e à autodeterminação informativa

The use of artificial intelligence in the prediction of femicide and the right to explainability and informational self-determination

Araceli Martins Beliato 169

A coleta de dados em larga escala e as possibilidades críticas de direito comparado: sistema de dupla proteção

Bulk data collection and critical possibilities in compared law: double lock system

Samuel Andreatta 203

Técnicas antiforenses: obstrução da justiça ou garantia da defesa?

Antiforensic techniques: obstruction of justice or guarantee of defense?

Jamilla Monteiro Sarkis e Paola Alcântara Lima Dumont 227

Entrevistas

Entrevista com a Professora Dra. Heloisa Estellita

Interview with Professor Dr. Heloisa Estellita

Rodrigo Oliveira de Camargo e Carlos Helder Furtado Mendes 261

Entrevista com o Professor Dr. Geraldo Prado

Interview with Professor Dr. Geraldo Prado

Rodrigo Oliveira de Camargo e Carlos Helder Furtado Mendes 267

Direito Por Quem o Faz

Análise jurisprudencial dos Tribunais Superiores no campo da proteção de dados pessoais em âmbito penal

Case law analysis of the Superior Courts in the field of personal data protection in criminal matters

Raissa de Cavassin Milanezi 277

Índice Alfabético-remissivo

Autores 307

Temas 309

Normas de Publicação – *Revista Brasileira de Ciências Criminais* 313

Diretrizes ao Corpo de Avaliadores – *Revista Brasileira de Ciências Criminais* 325

Condições para Submissão (*Checklist*) 331

Editorial

Dossiê "Proteção de dados pessoais e Ciências Criminais": prólogo de uma formação jurídico-penal

Dossier "Personal data protection and criminal sciences": prologue to a legal-criminal education

DOI: [doi.org/10.5281/zenodo.17058439].

Resumo: O dossiê "Proteção de Dados Pessoais e Ciências Criminais" da Revista Brasileira de Ciências Criminais analisa os impactos da era digital sobre direitos fundamentais e o sistema penal. A crescente coleta e processamento de dados pessoais por meio de tecnologias avançadas suscitam dilemas relacionados à privacidade, à proporcionalidade e ao devido processo legal. O editorial destaca os riscos da hipervigilância algorítmica, da mercantilização da informação e do uso de métodos ocultos de investigação, apontando a necessidade de maior controle, transparência e garantias no tratamento de provas digitais. Também evidencia lacunas normativas e a urgência de regulamentação específica em matéria penal, capaz de conciliar efetividade investigativa e proteção da autodeterminação informacional. Defende-se, ainda, a incorporação transversal da proteção de dados na formação jurídica e o fortalecimento da atuação judicial para limitar abusos. O dossiê busca estimular o debate e consolidar uma cultura penal comprometida com a dignidade humana e o Estado de Direito.

Palavras-chave: Vigilância algorítmica; Autodeterminação informacional; Processo penal; Cibercriminalidade; Formação jurídica.

Abstract: The dossier "Personal Data Protection and Criminal Sciences" of the Revista Brasileira de Ciências Criminais explores the impact of the digital era on fundamental rights and the criminal justice system. The increasing collection and processing of personal data through advanced technologies raise challenges concerning privacy, proportionality, and due process of law. The editorial highlights the risks of algorithmic surveillance, data commodification, and covert investigative methods, emphasizing the need for stronger oversight, transparency, and safeguards in handling digital evidence. It also points to regulatory gaps and the urgency of specific criminal law provisions capable of balancing investigative effectiveness with the protection of informational self-determination. Furthermore, it calls for the transversal incorporation of data protection into legal education and for a more active judicial role in curbing abuses. The dossier seeks to foster debate and promote a criminal law culture committed to human dignity and the rule of law.

Keywords: Algorithmic surveillance; Informational self-determination; Criminal procedure; Cybercrime; Legal education.

A era digital trouxe consigo avanços tecnológicos sem precedentes, mas também complexos desafios para a proteção de direitos fundamentais, especialmente

no âmbito das ciências criminais. A crescente capacidade de coleta, armazenamento e processamento de dados pessoais, impulsionada por algoritmos e inteligência artificial, levanta questões cruciais sobre privacidade, liberdade e o próprio devido processo legal.

O reconhecimento da proteção de dados pessoais como garantia fundamental pela Emenda Constitucional 115/2022 e as obrigações assumidas pelo Brasil na Convenção de Budapeste por meio do Decreto 11.491/2023 direcionarão práticas e processos legislativos em matéria penal pelos próximos anos, já que o instrumento internacional orienta os países signatários a que adotem medidas legislativas em seus ordenamentos jurídicos internos voltadas (i) à criminalização de condutas que atentem contra o bem jurídico dado pessoal; (ii) à regulamentação de atividades de tratamento de dados pessoais para fins de prevenção, investigação, detecção e repressão de infrações penais ou para execução penal; e (iii) ao compartilhamento de dados para o combate à cibercriminalidade.

O pensamento crítico e a perspectiva acadêmica não podem estar alheios a essa realidade e é por isto que *Revista Brasileira de Ciências Criminais* (*RBCCrim*) dedica um dossiê temático à "Proteção de Dados Pessoais e Ciências Criminais", buscando aprofundar o debate sobre as tensões e intersecções entre esses campos. Para enriquecer essa discussão, foram realizadas entrevistas com dois proeminentes juristas brasileiros: o Professor Dr. Geraldo Prado e a Professora Dra. Heloisa Estellita.

Pelas lentes do *Poder, Vigilância e Garantismo*, o Professor Dr. Geraldo Prado registra que a concentração e o processamento massivo de dados e o emprego de inteligência artificial potencializam os poderes de controle social a níveis nunca antes experimentados. Aborda temas como a mercantilização dos dados pessoais, classificando-a como "algo bastante perigoso, quase uma transmissão onerosa dos órgãos alheios", e alerta para o incremento de erros judiciários devido à manipulação maliciosa de dados de terceiros. Com relação aos métodos ocultos de investigação, como a infiltração digital e o uso de *softwares* espiões, ele destaca o elevado risco de manipulação maliciosa do ambiente digital, propondo a necessidade de um terceiro controlador, idealmente um perito nomeado pelo juiz criminal, para garantir a integridade dessas atividades. O professor ressalta a investigação defensiva como prática voltada à redução de danos, contraponto legítimo à extração unilateral de dados pelas forças estatais e mecanismo necessário de verificação e controle de atividades probatórias sofisticadas, que exige conhecimento multidisciplinar para discutir temas da ciência da computação. Em sua visão, a defesa penal deve dispor de recursos técnicos para entender a prova digital em todas as suas etapas e explicá-la ao julgador.

Por derradeiro, Prado enfatiza a urgência de incorporar a proteção de dados pessoais como um direito fundamental de forma transversal na formação jurídica,

desde o ensino médio, reiterando o papel das Ciências Criminais como limite aos "poderes selvagens estatais e não estatais" no nível da dogmática jurídica e na prática do sistema penal, em compromisso com o Estado de Direito, a proteção da liberdade e o respeito à dignidade humana.

Já sob a perspectiva de *Regulamentação, Desafios e Lacunas*, a Professora Dra. Heloisa Estellita traz uma visão complementar e igualmente crítica sobre a proteção de dados pessoais no contexto penal, destacando a urgência de o Brasil se alinhar aos padrões da Diretiva UE 2016/680 como um modelo para reequilibrar a proteção de direitos fundamentais com o avanço do acesso das autoridades de persecução penal a dados pessoais. No plano internacional, a professora aponta para a ausência de marcos normativos no Estatuto de Roma como um dos principais desafios para a harmonização entre o combate à criminalidade transnacional e a proteção de dados em tribunais internacionais; por outro lado, registra que o Tribunal Penal Internacional tem demonstrado robustez na proteção de dados de investigados, acusados, vítimas e testemunhas, contrastando com a publicidade processual brasileira.

No âmbito do Direito Penal Econômico, que lida com a gestão e a análise massiva de dados, Estellita enfatiza que a garantia da proteção de dados sem comprometer a efetividade das investigações reside na construção de medidas proporcionais e tecnicamente adequadas, as quais incluem autorização legal, finalidades legítimas, transparência, minimização, descarte de material impertinente, análise de risco e, crucialmente, limitações robustas ao compartilhamento.

Com relação à produção probatória em crimes econômicos complexos, pondera que o uso de fontes abertas e dados estruturados obtidos via sistemas automatizados pode ser útil, mas sua validade depende de critérios rigorosos de transparência, autenticidade, integridade e contextualização. O risco, segundo ela, reside na opacidade dos *outputs* gerados por algoritmos e na ausência de contraditório sobre os critérios de busca, seleção e classificação dos dados.

Para uma regulamentação legítima e proporcional, a Professora Dra. Estellita propõe duas medidas urgentes: a) legislar de forma clara e exaustiva por meio de uma lei geral de proteção de dados em matéria penal; e b) atualizar toda a legislação autorizativa de intervenções nesse direito, incluindo dispositivos específicos para a proteção da autodeterminação informacional e regulando novas formas de intervenção, como a infiltração *online*. Ela destaca, ainda, a necessidade de incorporar a proteção de dados pessoais como uma dimensão transversal na formação jurídica, desde a graduação até a pós-graduação, abordando a matéria a partir da teoria constitucional dos direitos fundamentais. Ela também aponta lacunas na tutela penal brasileira, como a ausência de tipos penais para o compartilhamento ilegal de dados pessoais e violações graves de segurança cibernética, sugerindo a necessidade de legislação nessa matéria.

Dossiê "Proteção de dados pessoais e Ciências Criminais": prólogo de uma formação jurídico-penal. *Revista Brasileira de Ciências Criminais*. vol. 211. ano 33. p. 17-21. São Paulo: Ed. RT, nov./dez. 2025.
DOI: [doi.org/10.5281/zenodo.17058439].

As entrevistas com o Professor Dr. Geraldo Prado e a Professora Dra. Heloisa Estellita oferecem um panorama abrangente e aprofundado sobre os desafios e as perspectivas da proteção de dados pessoais no âmbito das ciências criminais brasileiras. Ambos os especialistas convergem na necessidade urgente de uma regulamentação mais eficaz e de uma mudança de paradigma na cultura jurídica para enfrentar os impactos da revolução digital. A hipervigilância algorítmica, a mercantilização de dados e os métodos ocultos de investigação representam ameaças significativas aos direitos fundamentais, exigindo respostas legislativas, judiciais e educacionais coordenadas. Concluem ser imperativo que o Brasil avance na criação de uma LGPD Penal que estabeleça parâmetros claros para o tratamento de dados em investigações criminais, garantindo a proteção da autodeterminação informacional sem comprometer a efetividade da persecução penal.

Na opinião dos professores, a formação jurídica também deve ser reformulada para incorporar criticamente o tema da proteção de dados, capacitando os profissionais do direito a lidar com as complexidades do ambiente digital. Além disso, reputam como fundamental a atuação do Poder Judiciário para coibir abusos e garantir que as práticas investigativas estejam em conformidade com os princípios do devido processo legal e da proporcionalidade. O diálogo entre as diferentes vertentes do pensamento jurídico, como demonstrado pelas entrevistas, é fundamental para a construção de soluções.

O destaque dado por este editorial para as entrevistas não desprestigia os artigos que compõem o dossiê. Ao contrário, trata-se de um conjunto que, a partir da problemática apresentada, trabalha diversas abordagens no campo das Ciências Criminais. Os textos reunidos, agora à disposição do leitor, não apenas apontam para a construção de argumentos sólidos do ponto de vista teórico, mas também expõem situações práticas que revelam a pertinência temática, sobretudo quanto aos desafios evidenciados em perspectiva aos casos de interesse dos órgãos da persecução penal.

Ao leitor, o dossiê também apresenta uma pesquisa de jurisprudências sobre proteção de dados pessoais no âmbito penal, junto às Cortes Superiores. A partir da análise, pôde-se perceber que algumas decisões esvaziam o conteúdo do direito fundamental consagrado na Emenda Constitucional 115/2022, sob o argumento de que a LGPD Cível não se aplica em âmbito penal, além de se observar que as Cortes apresentam entendimentos divergentes sobre a extensão da proteção de dados, sem que tenha se operado, até o momento, um debate profundo sobre a temática no STF e no STJ. A análise identifica que os Tribunais confundem normas autorizativas com normas de competência e ressalta a necessidade de ampliar teoria e legislação, na linha do que constataram os entrevistados desta edição especial, para garantir uma interpretação penal harmônica com o direito à proteção de dados.

Dossiê "Proteção de dados pessoais e Ciências Criminais": prólogo de uma formação jurídico-penal. *Revista Brasileira de Ciências Criminais*. vol. 211. ano 33. p. 17-21. São Paulo: Ed. RT, nov./dez. 2025.
DOI: [doi.org/10.5281/zenodo.17058439].

O encerramento deste dossiê não é um fim. Para nós, ficou muito claro que é preciso assumir um compromisso sério com a formação de uma cultura jurídico-penal comprometida com a pesquisa e o ensino voltados ao desenvolvimento adequado da garantia da proteção de dados pessoais junto ao sistema de justiça criminal. E, no que depender de nós, a *RBCCrim*, diante de sua posição, não se furtará da sua enorme responsabilidade.

Nosso muito obrigado a todos os envolvidos na construção deste projeto. Editores, pareceristas e, sobretudo, aos autores que enviaram suas investigações para o *dossiê*. Foram contribuições excepcionais e altamente reflexivas. Esperamos que o presente trabalho alcance seus objetivos e desperte o interesse sobre o tema, construindo e fomentando esse movimento reflexivo em torno da nova garantia fundamental: "proteção de dados pessoais".

Boa leitura a todos.

Prof. Dr. Rodrigo Oliveira de Camargo (Org.)
Prof. Dr. Carlos Hélder Carvalho Furtado Mendes (Org.)

Dossiê "Proteção de dados pessoais e Ciências Criminais": prólogo de uma formação jurídico-penal. *Revista Brasileira de Ciências Criminais*. vol. 211. ano 33. p. 17-21. São Paulo: Ed. RT, nov./dez. 2025. DOI: [doi.org/10.5281/zenodo.17058439].

Dossiê "Proteção de Dados Pessoais e Ciências Criminais"

Da nuvem à corte: o julgamento constitucional da prova penal invisível

From the cloud to the courtroom: the constitutional review of invisible criminal evidence

José Guimarães Mendes Neto[1]
Universidade Estadual do Maranhão, Uema-MA, Brasil.
guimaraesmneto@hotmail.com

André Luís Callegari[2]
Instituto Brasiliense de Direito Público, IBDP, Brasil.
callegari@callegariadvogados.com.br

DOI: [doi.org/10.5281/zenodo.17058310].

1. Doutor e Mestre em Direito Constitucional pelo Instituto Brasiliense de Direito Público (IDP/DF). Especialista em Direito Penal Econômico pelo Instituto Brasileiro de Ciências Criminais (IBCCRIM) e Instituto de Direito Penal Econômico e Europeu (IDPEE), da Faculdade de Direito da Universidade de Coimbra. Especialista em Direito Eleitoral pela Pontifícia Universidade Católica de Minas Gerais (PUC Minas). Bacharel em Direito pela Unidade de Ensino Superior Dom Bosco (UNDB-MA). Professor da Universidade Estadual do Maranhão (UEMA-MA) e do Centro Universitário Dom Bosco (UNDB-MA). Advogado.
   Currículo Lattes: [http://lattes.cnpq.br/3665653914918095].
   ORCID: [https://orcid.org/0000-0003-1175-3211].
   E-mail: guimaraesmneto@hotmail.com
2. Doutor em *Derecho Publico y Filosofia Juridica* – Universidad Autónoma de Madrid (2001). Doutor *honoris causa* pela Universidad Autónoma de Tlaxcala, México, e pelo Centro Univesitário del Valle del Teotihuacan, México. Graduado em Ciências Jurídicas e Sociais pela Pontifícia Universidade Católica do Rio Grande do Sul (1989). Realizou estudos de pós-doutorado na Universidad Autónoma de Madrid sob a direção do Prof. Dr. Manuel Cancio Meliá. Professor do Instituto Brasiliense de Direito Público. Recebeu a medalha Des. Ernesto José Baptista, tendo em vista a prestação de assinalados serviços por atos ou donativos à Escola Superior da Magistratura do Estado do Piauí. Vice-presidente acadêmico do Instituto Iberoamericano de Derecho Penal. Professor visitante do Centro Universitário del Valle de Teotihuacan. Professor visitante – Universidad Externado de

Área do Direito: Processual; Penal; Digital

Resumo: O artigo examina a constitucionalidade da chamada prova penal invisível, caracterizada pela obtenção compulsória e velada de dados em nuvem mediante *backup* forçado. A pesquisa demonstra que tais práticas, embora justificadas sob a ótica da eficiência investigativa, colidem frontalmente com garantias constitucionais como a reserva legal, a vedação à autoincriminação e a proteção de dados pessoais. Defende-se que sua legitimidade somente seria possível mediante consentimento do titular, delimitação temporal rigorosa e vinculação a crimes específicos. Conclui-se que, no formato atual, trata-se de prática inconstitucional e incompatível com o Estado Democrático de Direito.

Palavras-chave: Vigilância digital; Eficiência investigativa; Autodeterminação informacional; Garantias fundamentais; Segurança jurídica.

Abstract: The article examines the constitutionality of the so-called invisible criminal evidence, characterized by the compulsory and covert acquisition of cloud data via forced backups. It shows that such practices, though justified by investigative efficiency, conflict with constitutional guarantees such as the principle of legality, the privilege against self-incrimination, and personal data protection. The paper argues that legitimacy would require the data subject's consent, strict temporal limits, and linkage to specific serious offenses. It concludes that, in its current form, the practice is unconstitutional and incompatible with the Democratic Rule of Law.

Keywords: Digital surveillance; Investigative efficiency; Informational self-determination; Constitutional safeguards; Legal certainty.

Sumário: 1. Introdução. 2. Sincronização, armazenamento em nuvem (*backup*) e poder investigativo: o enquadramento fático das práticas de acesso forçado. 3. (In)observância das garantias processuais à luz dos requisitos constitucionais: reserva legal; direito à não autoincriminação; *fishing expedition*; cadeia de custódia. 4. Limites constitucionais: consentimento, temporalidade e tipificação penal específica. 5. Considerações finais. Referências. Legislação. Jurisprudência.

1. Introdução

O avanço da tecnologia e a onipresença da *internet* têm alterado profundamente os meios de investigação criminal, trazendo consigo novos desafios jurídicos, especialmente no que diz respeito à compatibilidade – ou não – entre os métodos investigativos e os direitos e garantias fundamentais previstos constitucionalmente. No centro desse cenário, destaca-se a prática de coleta forçada e velada de dados armazenados por servidores de *internet* – como ocorre nos serviços de *backup* em

Colombia. Membro do Centro de Estudios de Derecho Penal Económico y de la Empresa, Peru. Advogado. Autor de diversos livros e artigos jurídicos.
ORCID: [https://orcid.org/0000-0002-3440-9758].
E-mail: callegari@callegariadvogados.com.br

Mendes Neto, José Guimarães; Callegari, André Luís. Da nuvem à corte: o julgamento constitucional da prova penal invisível. *Revista Brasileira de Ciências Criminais*. vol. 211. ano 33. p. 25-49. São Paulo: Ed. RT, nov./dez. 2025.
DOI: [doi.org/10.5281/zenodo.17058310].

nuvem – sem ciência do titular das informações, fenômeno que aqui se denomina como prova penal invisível.

Assim, o presente estudo tem como objetivo analisar os contornos constitucionais desse método de obtenção de prova digital, partindo da seguinte indagação central: em que medida a prova penal digital obtida por meio de *backup* forçado e velado pode ser considerada constitucional no contexto do ordenamento jurídico brasileiro, e quais seriam os requisitos e limites necessários para sua admissibilidade?

Isto é, o objetivo (problema) central desse artigo perpassa na análise sobre em que medida a prova penal digital pode ser dotada de fundamentação normativa de natureza constitucional, apta a permitir sua aplicação no ordenamento jurídico brasileiro, especialmente no que se refere à coleta de dados de terceiros armazenados por servidores de *internet* por meio de *backup* forçado e velado ao titular, observando-se os limites e requisitos indispensáveis à sua legitimidade.

Para tanto, o artigo estrutura-se em três frentes principais. No primeiro capítulo, irá se realizar o enquadramento fático sobre as práticas de acesso forçado, abordando a forma como mecanismos como a sincronização automática e o armazenamento e nuvem vêm sendo utilizados por autoridades investigativas, muitas vezes à revelia de qualquer respaldo legal, e com amplo e direto impacto em direitos fundamentais; tais como a privacidade, a proteção de dados pessoais e a integridade dos sistemas informáticos.

Já no segundo capítulo, a abordagem será quanto à relação entre tais práticas e o núcleo essencial das garantias constitucionais e processuais, com destaque para a legalidade estrita (*nulla coactio sine lege*), a vedação ao uso da analogia em prejuízo do acusado, o direito à não autoincriminação e a preservação da cadeia de custódia das provas digitais. Tais elementos revelam a fragilidade jurídica da prova penal invisível quando confrontada com o Estado Democrática de Direito.

Por fim, o terceiro capítulo propõe a delimitação dos limites constitucionais mínimos para que esse tipo de prova possa, eventualmente, ser validada no processo penal. Para tanto, discute-se a necessidade de observância de três critérios fundamentais: o consentimento expresso do titular dos dados, a delimitação temporal da coleta, e a vinculação a tipos penais específicos – elementos estes que visam evitar arbitrariedades e garantir segurança jurídica tanto ao Estado quanto ao investigado.

Por sua vez, a hipótese que se pretende confirmar é a de que, na forma em que vem sendo aplicada, a prática da coleta de dados por meio de *backup* forçado e velado é inconstitucional, por violar frontalmente garantias processuais e direitos fundamentais. Assim, propõe-se não o afastamento da tecnologia no âmbito da persecução penal, mas sua regulação rigorosa e criteriosa, compatível com os princípios constitucionais que regem o processo penal brasileiro.

Trata-se de tema ainda pouco enfrentado pela doutrina nacional, embora cada vez mais presente na prática forense, especialmente diante da crescente atuação de empresas de tecnologia (conhecidas como *big techs*) em colaboração com investigações criminais. O presente trabalho busca, portanto, contribuir de forma crítica e propositiva para a reflexão acadêmica e institucional sobre os riscos da normalização de práticas investigativas que violam a intimidade digital do indivíduo sob o pretexto de eficiência estatal.

Sem pretender esgotar o tema, espera-se com este artigo fomentar o debate acadêmico e jurídico sobre os limites legítimos do poder investigativo estatal na era digital, reafirmando que o uso de novas tecnologias, por mais eficazes que sejam, devem observância aos alicerces legais predispostos no processo penal, bem como aos princípios estruturantes da Constituição Federal de 1988.

2. Sincronização, armazenamento em nuvem (*backup*) e poder investigativo: o enquadramento fático das práticas de acesso forçado

Inicialmente, cumpre-se destacar sobre a possibilidade de representações – por autoridades investigativas (policial e/ou ministerial) – para medidas cautelares de afastamento dos sigilos de dados e comunicações telefônicas e telemáticas, quebra do sigilo bancário e autorização para compartilhamento de dados.

Na referida hipótese de medida cautelar de afastamento do sigilo telefônico e telemático, os fundamentos legais e constitucionais utilizados tem por orientação o artigo 5º, incisos X e XII, da Constituição Federal de 1988[3] e na Lei 9.296/1996, especialmente os artigos 1º e 2º da referida lei[4]. Por sua vez, a quebra de sigilo bancário

3. Art. 5º. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: X – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal (Brasil, 1988).
4. Art. 1º A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça. Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática. Art. 2º Não será admitida a interceptação de comunicações telefônicas quando ocorrer qualquer das seguintes hipóteses: I – não houver indícios razoáveis da autoria ou participação em infração penal; II – a prova puder ser feita por outros meios disponíveis; III – o fato investigado constituir infração penal

tem por base constitucional o próprio artigo 5º, incisos X e XII da Constituição Federal de 1988 (Brasil, 1988) e a Lei Complementar 105/2001 com base no artigo 1º, § 4º, incisos VI e VIII[5].

Portanto, o enquadramento fático do presente artigo diz respeito quanto ao interesse de autoridades investigativas em colherem a existência – ou não – de fontes de provas atinentes a descobrir a existência de organizações criminosas (Brasil, 2013), cometimento de crimes licitatórios (BRASIL, 2021a), peculato (Brasil, 1940), lavagem de dinheiro (BRASIL, 1998) e/ou corrupção ativa e passiva (Brasil, 1940).

Acontece que a questão problemática em si não está nos termos da referida medida (uma vez que há disposição normativa legal para tanto), mas sim no contemporâneo fato em que se observa na prática forense autoridades investigativas representando – com fundamento no artigo 3º, inciso I e artigo 5º da Lei 9.296/1996 c/c artigo 7º, inciso I e III, da Lei 12.965/2014 – pelo afastamento do sigilo das comunicações em sistemas de informática e telemática e consequente monitoramento de aparelho telefônico com sistema operacional IOS identificado, para fins de com isso acionar o servidor de *internet* para que possa: i) ativar/habilitar a sincronização automática da conta alvo, de forma compulsória e velada ao usuário; ii) ativar/habilitar os serviços de armazenamento em "nuvem", de forma compulsória e velada ao usuário, disponibilizando acesso *online* a todo o conteúdo.

O problema de pesquisa deste artigo está nestes pontos: ou seja, dados de terceiros que estejam armazenados por servidores de *internet* podem ser recolhidos a partir de *backup* forçado e velado ao portador, por conta de interesses advindos das autoridades investigativas sob a égide do fundamento eficientista da política de segurança pública[6].

Representações nesse formato tem por finalidade alcançar informações (fontes de provas) através de empresas da área de tecnologia com atuação em diversos

---

punida, no máximo, com pena de detenção. Parágrafo único. Em qualquer hipótese deve ser descrita com clareza a situação objeto da investigação, inclusive com a indicação e qualificação dos investigados, salvo impossibilidade manifesta, devidamente justificada (Brasil, 1996).

5. Art. 1º As instituições financeiras conservarão sigilo em suas operações ativas e passivas e serviços prestados. § 4º A quebra de sigilo poderá ser decretada, quando necessária para apuração de ocorrência de qualquer ilícito, em qualquer fase do inquérito ou do processo judicial, e especialmente nos seguintes crimes: VI – contra a Administração Pública; VIII – lavagem de dinheiro ou ocultação de bens, direitos e valores (Brasil, 2001).
6. Compreende-se segurança pública enquanto àquele direito que regula ações do Estado que "a) visam a proteção da segurança pública; b) contra perigos; c) sendo que essas ações afetam determinados destinatários, geralmente, em âmbito constitucionalmente protegido" (Gleizer; Montenegro; Viana, 2021, p. 81).

países: *big techs*. Como principais exemplos: a *Microsoft* Informática Ltda; o Google Brasil Internet Ltda, a *Apple* Brasil e o *WhatsApp*.

A *Microsoft*, o *Google* e a *Apple* são empresas multinacionais norte-americanas que atuam no setor de tecnologia, com forte presença no desenvolvimento de *softwares*, serviços digitais e soluções em nuvem.

A *Microsoft* destaca-se pelo sistema operacional *Windows* e pelo pacote de escritório *Microsoft Office*, além de atuar nos segmentos de *hardware*, armazenamento em nuvem (Azure) e jogos eletrônicos (Xbox)[7]. O Google LLC, fundado em 1998 em *Menlo Park*, ganhou notoriedade inicialmente por seu mecanismo de busca, expandindo-se posteriormente para as áreas de publicidade *online*, *software*, armazenamento em nuvem e dispositivos móveis, especialmente por meio do sistema operacional Android[8]. A Apple, por sua vez, é uma das maiores empresas de tecnologia do mundo, amplamente reconhecida por seus dispositivos eletrônicos, como *iPhone*, *iPad*, *Mac* e *Apple Watch*, bem como por seus serviços de *software*, armazenamento em nuvem (*iCloud*), mídia digital e entretenimento, incluindo plataformas como *iTunes*, *Apple* TV+ e *Apple Music*[9].

Todavia, a problematização não se exaure apenas nas autoridades investigativas, mas também em outros espaços do sistema de justiça, uma vez que persistem decisões judiciais autorizando o afastamento de dados de endereços eletrônicos (*e-mails*, "nuvem" e serviços associados), bem como das comunicações telefônicas e telemáticas de diversos terminais móveis.

Portanto, embora inexista respaldo normativo legal para tanto, o poder judiciário – ainda assim – pode considerar como necessária a flexibilização dos sigilos telemáticas e telefônicos enquanto método de investigação de fontes de provas para apuração de suposto fato típico.

Assim, o problema jurídico é ainda maior, a partir de decisões judiciais determinando que grandes empresas da área de tecnologia (*big techs*) em determinado prazo, sob pena de multa diária: i) ative/habilite a sincronização automática de conta indicada ou vinculada a determinado *International Mobile Equipment Identity*

7. MICROSOFT. Disponível em: [https://news.microsoft.com/facts-about-microsoft/]. Acesso em: 10.04.2025.
8. GOOGLE. Disponível em: [https://policies.google.com/terms?utm_source=about.google&utm_medium=referral&utm_campaign=footer]. Acesso em: 10.04.2025.
9. OLIARI, Deivi Eduardo; ZAMBON, Cláudia Neli de Souza. Apple: como esta marca se tornou sinônimo de qualidade e hoje é a marca mais valiosa do mundo. In: CONGRESSO DE CIÊNCIAS DA COMUNICAÇÃO NA REGIÃO SUL, 15, 2014, Palhoça. *Anais*... São Paulo: Intercom – Sociedade Brasileira de Estudos Interdisciplinares da Comunicação, 2014. Disponível em: [https://canaltech.com.br/empresa/apple/]. Acesso em: 10.04.2025.

(IMEI)[10] informado pelas autoridades investigativas, de forma compulsória e velada ao usuário; ii) ative/habilite os serviços de armazenamento em "nuvem" *iCloud, Google Drive* e *OneDrive,* de forma compulsória e velada ao usuário, e disponibilize durante todo o prazo de monitoramento, acesso *online* à visualização/*download* de todo o conteúdo. Para tanto, utilizando-se como fundamento legal o artigo 3º, inciso I e artigo 5º da Lei 9.296/1996 c/c artigo 7º, inciso I e III da Lei 12.965/2014.

A *Apple* Brasil, por exemplo, informa que, para cumprir a decisão judicial, seria imprescindível a especificação do *Apple ID* ou a conta de *e-mail* do alvo investigado, nome completo e número de telefone e/ou nome completo e endereço físico relacionado à conta da *Apple* do alvo investigado. Portanto, seriam duas as hipóteses possíveis quando do acometimento de decisões como a supracitada.[11]

Na primeira hipótese, a Apple Brasil não consegue – ativar/habilitar a sincronização automática de conta indicada ou vinculada tão somente com a indicação, pelas autoridades investigativas, de determinado IMEI, de forma compulsória e velada ao usuário; ativar/habilitar os serviços de armazenamento em "nuvem" *iCloud*, de forma compulsória e velada ao usuário, tendo tão somente a indicação, pelas autoridades investigativas, do número do IMEI –, pois a pesquisa tendo por referência tão somente o número do IMEI da conta alvo investigada não permite ao respectivo servidor realizar os atos descritos na decisão judicial.

Já na segunda hipótese, a Apple Brasil tendo acesso a todas as informações (a dizer, número do IMEI, *Apple* ID/conta de *e-mail*, nome completo e número de telefone e/ou nome completo e endereço físico relacionados à conta da *Apple*), disponibiliza por *link* todo o conteúdo da nuvem do proprietário da conta o que, posteriormente, é submetido ao *software Cellebrite Physical Analyzer* para decodificar e categorizar os arquivos da nuvem *Apple*, em especial o conteúdo do *WhatsApp.*

Sendo assim, aparentemente, apenas na segunda hipótese é que então se observaria o problema de pesquisa deste artigo; entretanto, mesmo na primeira hipótese,

10. "Cada celular tem um número de identificação único e global, chamado de IMEI (*International Mobile Equipment Identity*). Fazendo uma analogia, o IMEI equivalei ao número de chassis de um carro, ou seja, é único para cada aparelho celular. O IMEI é formado por quatro grupos de números: 000000-00-000000-0. Para achar o número de IMEI do celular, o consumidor pode: 1) procurar na caixa do celular; 2) procurar em um adesivo que fica por trás da bateria; ou 3) digitar *#06# no celular e apertar a tecla para ligar" (BRASIL. AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES. *Identificação Internacional de Equipamento Móvel – IMEI*. Disponível em: [www.gov.br/anatel/ptbr/assuntos/celularlegal/imei]. Acesso em: 10.04.2025).

11. SAMPAIO, Denis; SANTOS JUNIOR, Antônio. Backup forçado e velado de dados em investigações: um tema delicado. Disponível em: [https://www.conjur.com.br/2024-jun-22/backup-forcado-e-velado-de-dados-em-investigacoes-um-tema-delicado/].

o problema de pesquisa subsiste, pois, embora não haja o *backup* forçado e velado ao portador, todas as informações que estiverem armazenadas na nuvem do ato investigado – por autorização deste para o respectivo armazenamento – poderão ser compartilhadas com as autoridades investigativas; ainda que sem regramento normativo legal para tanto.

Desse modo, surgem questionamentos acessórios: a quem pertence os dados armazenados no serviço de armazenamento de nuvem? Ao servidor de *internet* ou à pessoa detentora dos dados e que se utiliza dos serviços de armazenamento de nuvem?

A partir do enquadramento fático descrito e das duas hipóteses que decorrem, resta inegável que ambas são modalidades de intervenção nos direitos fundamentais, especificamente a privacidade, a proteção de dados pessoais e a confidencialidade e integridade dos sistemas informáticos.

A intervenção no direito fundamental à privacidade é inconteste, pois inexiste limites para a utilização de novas tecnologias com impacto no âmbito do sistema penal colocando em risco a liberdade e o pleno exercício democrático inerente ao Estado de direito instituído. De igual modo, a intervenção no direito fundamental à proteção de dados pessoais, pois sequer é considerado o consentimento dos usuários para a coleta de dados de terceiros armazenados por servidores de *internet* por meio de *backup* forçado e velado ao titular. No mais, o enquadramento fático apresentado também viola o direito fundamental à confidencialidade e a integridade, vez que inexistem limites jurídicos e modelos regulatórios compatíveis com esta referida prática invasiva no ambiente digital.

Ainda que o usuário autorize o *backup* de seus dados e informações junto aos servidores de *internet*, isso, por sua vez, não deve significar uma transferência de propriedade a estes ao ponto de o autorizarem em disponibilizar o conteúdo da "nuvem" junto às autoridades investigativas, ainda que com decisão judicial que a justifique. A razão seria – sobretudo – pela ausência da observância aos requisitos demarcados constitucionalmente, bem como os necessários limites normativos para sua legalidade e constitucionalidade.

Importa esclarecer que a sincronização automática de contas consiste no processo pelo qual dados vinculados a uma conta de usuário – como *e-mails*, agendas, fotos, documentos e contatos – são atualizados de forma contínua e automática entre um dispositivo móvel e o servidor onde tais informações estão armazenadas, usualmente em ambientes de nuvem. O objetivo dessa funcionalidade é assegurar que qualquer alteração realizada em um dos dispositivos conectados se reflita imediatamente nos demais vinculados à mesma conta[12-13].

12. "[...] a sincronização em ambientes móveis pode ser definida como o ato de estabelecer equivalência entre duas coleções de dados, entre cliente e servidor, após a ocorrência de

Por sua vez, a expressão "conta indicada ou vinculada a determinado IMEI" refere-se à associação entre uma conta de usuário e o número de identificação único do dispositivo móvel – o IMEI. Essa vinculação delimita a sincronização a dispositivos previamente autorizados, conferindo uma camada adicional de controle e segurança quanto ao acesso aos dados armazenados[14].

Ocorre, entretanto, que na prática forense contemporânea, autoridades investigativas têm se valido de medidas judiciais que determinam, às empresas de tecnologia, a ativação da sincronização automática de forma compulsória e velada ao usuário. A expressão "compulsória" evidencia a obrigatoriedade da medida, sem possibilidade de recusa ou desativação por parte do titular da conta. Já o termo "velada" revela que essa sincronização ocorre à margem do conhecimento ou consentimento do usuário, sem qualquer notificação prévia ou posterior sobre a sua ativação.

Diante disso, a compreensão adequada dessas práticas exige atenção a três dimensões fundamentais: privacidade, consentimento e legalidade. No que tange à

---

alteração nos registros armazenados. Depois de sincronização de dados cada elemento de dados em uma coleção é mapeado por um elemento de dados em outra, sendo que seus dados são equivalentes, entretanto não necessariamente idênticos" (Manganelli; Romani, 2004, p. 41).

13. Para tanto, destacam-se alguns tipos de sincronização, quais sejam: *One-Way* e *Two-Way*. A One-Way "compreende a transferência de atualizações de dados em sentido único. Após um dispositivo estabelecer conexão com outro ele indica todas as alterações realizadas localmente. Após a transmissão, os dados são aplicados no banco de dados do receptor. O dispositivo receptor não recebe nenhuma mensagem de aceite ou erro na efetivação das requisições ao banco de dados. O plano *One-Way* pode ser aplicado de duas formas: no sentido cliente/servidor ou ao contrário". No tipo de sincronização *One-Way* Cliente/Servidor "o cliente é responsável por iniciá-la e submeter todas as modificações ao servidor, mas o servidor não retorna o resultado final das ações realizadas no banco de dados". No tipo de sincronização *One-Way* Servidor/Cliente o "servidor que inicia a transmissão, que conecta-se com o cliente e submete todos os dados atualizados no banco de dados consolidado. Após terminar a transferência, o cliente possui a versão atualizada de todos os registros do banco de dados do servidor. O servidor não captura nenhuma alteração feita pelo cliente". Já a *Two-Way* significa que a "transmissão das modificações ocorre nos dois sentidos, tanto do cliente como do servidor. A sincronização é iniciada pelo cliente. O servidor identifica e trato os conflitos existentes retornando ao cliente os dados corretos. No final, o cliente e o servidor possuem os mesmos dados" (Manganelli; Romani, 2004, p. 42).
14. "So electronic serial numbers were created to give unique identification to mobile devices known as International Mobile equipment Identity (IMEI) and the MEID (Mobile Equipment ID – a super set of IMEI) of today. IMEI is unique to every ME (mobile equipment) and uniquely identifies an individual mobile station. The IMEI format is given by Telecommunication standardization authorities and structured by the BABT and structure of IMEI is specified in 3GPP TS 23.003" (Kumar; Kaur, 2015, p. 528-529).

privacidade, a sincronização automática compulsória e oculta viola o direito do usuário de controlar quais dados estão sendo transferidos, armazenados ou acessados por terceiros. A vinculação ao IMEI, inclusive, pode agravar a exposição de dados em casos de perda, roubo ou acesso indevido ao dispositivo.

No aspecto do consentimento, é imprescindível que o titular dos dados tenha plena ciência da existência da sincronização, suas consequências diretas e indiretas, e que possa optar livremente por ativá-la ou não. O simples uso de um serviço digital não pode ser presumido como autorização irrestrita para a manipulação de dados pessoais por autoridades públicas ou plataformas tecnológicas.

Por fim, quanto à legalidade, verifica-se que a prática da ativação forçada da sincronização automática – especialmente quando vinculada a determinado IMEI e realizada sem ciência do usuário – carece de fundamento jurídico claro. A ausência de normas específicas que disciplinem esse tipo de intervenção torna a prática juridicamente precária, especialmente diante do direito fundamental à proteção de dados, à intimidade e às garantias processuais estabelecidas na Constituição Federal.

Assim, a utilização de sincronização automática à revelia do titular da conta, ainda que com o intuito de viabilizar a persecução penal e garantir a eficácia da política de segurança pública, configura-se como uma medida altamente questionável sob a óptica dos direitos fundamentais, das garantias processuais constitucionais e dos próprios limites materiais da constitucionalidade.

Ademais, ainda que o usuário eventualmente consinta com a sincronização automática entre seus dispositivos e o servidor de armazenamento em nuvem, tal consentimento não implica transferência de titularidade dos dados nem autoriza, por si só, o fornecimento do conteúdo sincronizado às autoridades investigativas, ainda que mediante decisão judicial. O fornecimento indiscriminado de dados pessoais, sem base legal específica e sem respeito aos direitos fundamentais e garantias processuais constitucionais, compromete gravemente a integridade do devido processo legal.

Defende-se esse posicionamento, sobretudo, por haver inequívoca ausência da observância aos direitos fundamentais, aos requisitos processuais constitucionalmente demarcados, bem como aos necessários limites para sua respectiva constitucionalidade.

Nesse contexto de sincronização automática e do enquadramento fático aqui exposto, cumpre-se destacar – por exemplo – o posicionamento do Supremo Tribunal Federal e do Superior Tribunal de Justiça a respeito do tema espelhamento de mensagens por meio do aplicativo *WhatsApp Web*[15]; qual seja: inconstitucionalidade

15. Considerando o fato de que o subcapítulo trata do tema da sincronização automática, cumpre-se destacar sobre o *WhatsApp Web*. Este, por sua vez, é considerado como uma

e ilegalidade desta referida modalidade de sincronização (Moura; Barbosa, 2021, p. 487).

Quanto ao serviço de armazenamento em nuvem (*backup*), cumpre-se destacar que ele diz respeito a um sistema que permite aos usuários conservarem dados e arquivos em servidores remotos acessíveis pela *internet*; ao invés de armazenar em dispositivos físicos (discos rígidos e/ou *pendrives*).

De tal modo, o serviço de armazenamento em nuvem oferece vantagens como a possibilidade de acesso, pelos usuários, aos arquivos de qualquer lugar que detenha a devida conexão com a internet; facilidade para fins de compartilhamento de documentos; e economia quanto ao espaço para armazenamento em dispositivos locais[16].

A relação para com o termo *backup* é direta, pois significa – exatamente – o processo na qual se fazem cópias de segurança de dados para que impossibilite a eventual perda de informações importantes, haja vista a inequívoca possibilidade de falha no *hardware*, ataques de *hardware*, ou mesmo erros humanos[17-18].

Todavia, a ativação ou habilitação, de forma compulsória e velada, de serviços de armazenamento em nuvem como *iCloud, Google Drive* e *OneDrive*, com a consequente disponibilização de acesso remoto para visualização ou *download* integral de seu conteúdo, levanta sérias e complexas implicações legais e constitucionais (Paese Segundo, 2022).

Por sua vez, as expressões "compulsória" e "velada" revelam aspectos críticos do ponto de vista jurídico, pois: a primeira implica que o *backup* é imposto, não

---

extensão da conta de mensagens instantâneas utilizadas no celular do portador. Assim, as mensagens enviadas e recebidas são automaticamente sincronizadas entre o celular e o computador, o que permite ao usuário deter acesso em ambos (WhatsApp, sem data).

16. "Un cloud computing è un sistema di elaborazione distribuito, basato su Internet. Più chiaramente, può essere paragonato ad un grande e sofisticato personal computer (sistema di elaborazione) non realizzato da un sistema eletrônico fisicamente individuabile in un luogo ma da un insieme di sistemi elettronici connessi tra loro mediante la Rete Internet e quindi mediante una connessione telemática" (Aterno; Mattiucci, 2013, p. 865).
17. "Con questa modalità, ad esempio è possibile avere un PC Windows che opera dentro un Apple Mac. L'hardware è unico, quello del Mac, ma l'utente può lavorare simultaneamente con due computer diversi condividendo tastiere, hard disk, monitor, ecc. Il processo di virtualizzazione è ad oggi talmente spinto che dentro un computer è possibile simulare diversi computer virtuali collegati tra loro in rete; in pratica è possibile avere delle intere reti virtuali soli in un computer di casa" (Aterno; Mattiucci, 2013, p. 867).
18. "Nella prassi il sequestro di dati informatici passa ordinariamente attraverso la copiatura integrale dell´hard disk e la sucessiva restituzione dello stesso al legittimo proprietário. Questa è generalmente ritenuta la soluzione migliore anche dal punto de vista delle buone pratiche di computer forensics" (Murgia, 2017, p. 163).

podendo ser desativado pelo usuário; e a segunda sugere que o procedimento ocorre à sua total revelia, sem ciência ou consentimento.

Assim sendo, a prática de sincronização e *backup* ocorre de maneira invisível ao usuário, nos bastidores da arquitetura digital – envolvendo servidores de *internet* e autoridades investigativas – vinculando-se diretamente ao IMEI do dispositivo móvel. Isto é, o titular da conta permanece alheio à existência, ao alcance e ao conteúdo do que está sendo armazenado ou compartilhado.

As implicações dessa dinâmica podem ser sistematizadas em três dimensões fundamentais: privacidade, consentimento e legalidade.

Do ponto de vista da privacidade, o armazenamento forçado e oculto compromete o controle informacional do usuário sobre seus próprios dados, além de criar vulnerabilidades adicionais quando vinculado ao IMEI. Quanto ao consentimento, observa-se a ausência de escolha livre sobre a ativação dos serviços de *backup*, o que confronta diretamente os princípios constitucionais da autodeterminação informacional e da dignidade da pessoa humana. No plano da legalidade, inexiste base normativa específica que autorize a imposição desse tipo de medida pelas autoridades investigativas, tampouco há modelos regulatórios que legitimem o exercício do *backup* em nuvem de forma compulsória e sem ciência do titular da conta.

Não obstante, os serviços de armazenamento em nuvem – como *Apple*, *Google* e *Microsoft* – manifestam-se no sentido da impossibilidade técnica em efetuar *backup* dos dados do portador/usuário a sua revelia, ou seja, de modo forçado. Para tanto, destacam a inexistência de capacidade técnica para tanto, bem como a dificuldade de que as referidas empresas possam atuar à revelia dos usuários (Aterno; Mattiucci, 2013, p. 870-871).

Contudo, ainda assim, o debate jurídico quanto ao tema é imprescindível, principalmente pela cada vez mais acelerada evolução tecnológica no contexto moderno. Evolução que, por vezes, pode ser impulsionada para fins de persecução penal.

A título de premissa conclusiva inicial, destaca-se que o exame do panorama fático revela um preocupante deslocamento das práticas investigativas digitais no Brasil, em que medidas cautelares formalmente embasadas vêm sendo instrumentalizadas para legitimar o acesso forçado e velado a dados armazenados em servidores de nuvem, por meio de sincronização automática ativada à revelia do usuário.

Essa atuação demonstra uma crescente naturalização de práticas invasivas que ocorrem nos bastidores digitais, com base em fundamentos normativos insuficientes e sem o controle efetivo do titular dos dados.

Ainda que amparadas em decisões judiciais e justificadas pela busca de eficiência na persecução penal, tais medidas não podem se sobrepor aos limites constitucionais impostos ao poder investigativo do Estado. A possibilidade de acionamento de servidores para a extração integral de dados sincronizados, sem ciência do titular,

reconfigura o paradigma da prova penal, aproximando-se de um modelo de vigilância permanente incompatível com o Estado Democrático de Direito.

Sendo assim, este primeiro capítulo evidencia que, na prática atual, a chamada *prova penal invisível* – obtida a partir de sincronizações e *backup*s compulsórios – representa uma modalidade de intervenção estatal que exige urgente rediscussão quanto à sua constitucionalidade jurídica.

Lembrando que a ausência de marco normativo adequado – aliada à crescente pressão tecnológica por respostas eficazes à criminalidade – não pode justificar a erosão silenciosa de direitos fundamentais e garantias processuais constitucionais.

3. (In)observância das garantias processuais à luz dos requisitos constitucionais: reserva legal; direito à não autoincriminação; *fishing expedition*; cadeia de custódia

A consolidação do processo penal democrático exige a rigorosa observância das garantias constitucionais no tratamento da prova digital. A prática da recolha de dados armazenados em nuvem mediante *backup* forçado e sem ciência do titular, embora invocada com fins de eficácia investigativa, afronta pilares essenciais da ordem constitucional, como a reserva legal, a vedação à autoincriminação, *fishing expedition* e a preservação da cadeia de custódia da prova penal.

A primeira violação manifesta-se na ausência de norma específica que autorize a obtenção de dados digitais por meio de procedimentos ocultos e compulsórios. O princípio *nulla coactio sine lege,* consagrado no art. 5º, II, da Constituição Federal, veda a intervenção estatal sem respaldo normativo expresso.

A exigência de respaldo normativo é reforçada ainda pelos princípios da segurança jurídica e da legalidade administrativa (CF/1988, art. 37, *caput*)[19], os quais vedam atuações estatais arbitrárias, especialmente em contextos de restrição de direitos fundamentais, como a privacidade e a proteção de dados pessoais.

No contexto da prova penal digital, a necessidade de previsão legal específica torna-se ainda mais evidente em razão das características particulares desses elementos probatórios: imaterialidade, volatilidade, fragilidade, invisibilidade e dispersão geográfica (Murgia, 2017, p. 207).

Por sua vez, a tentativa de suprir esse vazio legal mediante analogia com normas destinadas à interceptação de comunicações (Lei 9.296/1996) ou ao Marco Civil da Internet (Lei 12.965/2014) revela grave desvio hermenêutico (Brasil, 1996, 2014).

19. Art. 37. A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência [...] (Brasil, 1988).

A primeira trata exclusivamente da interceptação de comunicações em trânsito, exigindo requisitos estritos como autorização judicial fundamentada, indícios de autoria e subsidiariedade do meio probatório (Gleizer; Montenegro, 2021, p. 121; Moura; Barbosa, 2021, p. 485). Já o Marco Civil da Internet limita-se à regulamentação do fornecimento de registros de conexão e acesso mediante ordem judicial[20], não havendo previsão sobre a extração unilateral de conteúdo armazenado (Brasil, 2011).

A jurisprudência do Supremo Tribunal Federal inicialmente rejeitou a utilização da interceptação telefônica sem lei específica, reconhecendo sua licitude apenas após a edição da Lei 9.296/1996. A Corte reforçou que a proporcionalidade, a adequação e a necessidade da medida devem ser observadas de forma estrita, não podendo tais critérios serem elididos por analogias não previstas no texto legal (Mendes; Branco, 2022, p. 637).

A aplicação desses precedentes às hipóteses de *backup* forçado mostra-se inadmissível, sob pena de grave comprometimento das garantias processuais. É dizer, na medida que novas tecnologias avançam no contexto comunicacional do mundo mais difícil fica a proteção do investigado/imputado de se defender contra as intromissões indevidas das informações outrora trocadas. Piora mais ainda com a possibilidade de que interlocutores possam estar monitorados a um indefinido tempo (Gleizer; Montenegro; Viana, 2021, p. 123).

Em igual sentido, a Corte Constitucional Italiana oferece importante parâmetro comparativo ao afirmar que a utilização de softwares espiões (*spywares*) para coleta de dados armazenados não configura interceptação de comunicação, mas sim acesso autônomo e unilateral, exigindo legislação específica[21].

---

20. Cumpre-se destacar o entendimento firmado pelo Supremo Tribunal Federal sobre a atuação das *bigs techs* e a ausência de norma que autorize coleta compulsória e velada de dados armazenados em nuvem por empresas com sede no exterior. Na oportunidade, foi reconhecida a constitucionalidade da aplicação do art. 11 do Marco Civil da Internet e do art. 18 da Convenção de Budapeste, permitindo requisições diretas de dados a empresas com representação no Brasil, quando o dado for coletado, tratado ou armazenado em território nacional. Isto é, reforça que o acesso a dados deve observar base normativa específica, sendo inadequado extrapolar o supracitado marco para justificar medidas como *backup* forçado e velado sem previsão legal expressa (Brasil, 2023).

21. "Quanto ai giudici di merito, posto che il citato decreto della Procura della Repubblica si è limitato a disporre che, da parte della Polizia Giudiziaria, siano estrapolati dati, sia già formati che contenuti nella memoria del personal computer in uso al BA., e quelle che in futuro sarebbero state archiviate, chiarirono correttamente che 'per flusso di comunicazioni deve intendersi la trasmissione, il trasferimento, di persona o a distanza, di informazioni da una fonte trasmittente a un destinatario, da un soggetto a un altro, cioè il dialogo delle comunicazioni in corso all'interno di un sistema o tra più sistemi informatici o telematici

Tal compreensão tem por premissa central a legalidade estrita e a cadeia de custódia como elemento imprescindível para a validade das provas digitais no âmbito do processo penal (Kerr, 2005, p. 280; Murgia, 2017, p. 194-211).

Em síntese, a adoção de práticas de obtenção de provas digitais à revelia do titular, sem respaldo legal específico e por meio de analogias indevidas, viola frontalmente o princípio *nulla coactio sine lege*. A superação dessa lacuna normativa não deve ocorrer pela via judicial ou por práticas consuetudinárias, mas sim por meio de legislação específica aprovada pelo Poder Legislativo, garantindo controle democrático e respeito às garantias fundamentais (Kerr, 2005, p. 281).

Dessa forma, reforça-se a necessidade de regulamentação clara dos métodos de investigação digital, assegurando, nos termos constitucionais, a efetividade do devido processo legal, a inviolabilidade da intimidade, a proteção dos dados e a higidez da atividade probatória. A ausência dessa normatização compromete não apenas o equilíbrio entre persecução penal e liberdades civis, mas também a legitimidade da própria atuação estatal no ambiente digital.

Ademais, a exigência de entrega de senhas ou a extração forçada de dados digitais colide com a garantia da não autoincriminação (art. 5º, LXIII, CF, Brasil, 1988). Isto é, o ato de obrigar o investigado – ainda que veladamente – a cooperar ativamente na produção da prova contra si afronta o núcleo da presunção de inocência e inverte a lógica acusatória do processo penal.

Sabe-se que o avanço das tecnologias digitais e a crescente criptografia de dados impuseram novos desafios ao processo penal, especialmente no tocante à garantia constitucional da vedação à autoincriminação (*nemo tenetur se detegere*)[22].

Assim, a exigência de fornecimento de senhas ou cooperação ativa do investigado na produção de prova penal digital acaba por ferir frontalmente essa garantia; prevista implicitamente no art. 5º, LXIII, da CF/1988, expressamente no art. 186 do CPP e reafirmada em tratados internacionais como o Pacto Internacional sobre Direitos Civis e Políticos (artigo 14, § 3º) e a Convenção Americana sobre Direitos Humanos (artigo 8, 2) (Brasil, 1992).

(Cass. SS.UU. 23.2.2000 n. 6), non potendo ritenersi sufficiente l'elaborazione e l'esternalizzazione del pensiero, e non attraverso simboli grafici apposti su supporto cartaceo, in un documento informatico realizzato mediante un sistema di elaborazione video e così conservato'. In questo caso, l'attività autorizzata dal PM, consistente nella 'rimozione e copia di documenti conservati sul 'disco rigido' del dispositivo utilizzato dalla BA., non aveva ad oggetto un 'flusso di comunicazioni', richiedendo un dialogo con altri soggetti, ma 'un rapporto operativo tra il microprocessore e il sistema elettronico video', cioè 'un flusso unidirezionale di dati' confinato entro i circuiti del personal computer'" (Itália, 2010).

22. "In light of these realities, applying the traditional Fourth and Fifth Amendment rules to the new network crimes leaves the first stage of network crime investigations almost entirely unregulated" (Kerr, 2005, p. 292-294).

A doutrina norte-americana do *act of production* – originada no caso *Fisher v. United States* – sustenta que, para haver violação ao direito de não autoincriminação, é necessário que o investigado seja coagido, que seu ato tenha conteúdo testemunhal e que tal conteúdo seja incriminador. Em consonância, a teoria da *foregone conclusion* permite a exigência de colaboração apenas quando o Estado já detém, de forma independente, conhecimento sobre o conteúdo e titularidade da prova (Kerr, 2019).

Porém, no Brasil, tal flexibilidade não se aplica. O Superior Tribunal de Justiça (Brasil, 2021b) e o Supremo Tribunal Federal (Brasil, 2015) têm afirmado que o fornecimento de senhas não pode ser compelido nem autorizado por decisão judicial, sob pena de violação ao direito fundamental do investigado.

Paralelamente, a prática do chamado *fishing expedition*, caracterizada por buscas genéricas e sem delimitação objetiva, viola o devido processo legal e os direitos à intimidade e à proteção de dados. No ambiente digital, o risco é intensificado pela imensa capacidade de armazenamento dos dispositivos eletrônicos e pela existência de verdadeiros "domicílios virtuais" (Murgia, 2017, p. 2018). A apreensão de um único aparelho pode permitir acesso irrestrito a dados pessoais sem pertinência com o objeto da investigação[23].

Portanto, a ausência de normas específicas que regulem a coleta, análise e uso de provas digitais gera insegurança jurídica e propicia violações sistemáticas às garantias processuais. Isto é, os dispositivos eletrônicos não podem ser tratados como simples gavetas físicas – o potencial invasivo do acesso irrestrito impõe a necessidade de regras que limitem o escopo das buscas e assegurem proteção proporcional aos dados (Kerr, 2005, p. 304).

Assim sendo, o respeito ao direito à não autoincriminação e à proibição de *fishing expedition* constitui pilar da legitimidade democrática da persecução penal na era digital. A defesa dessas garantias é condição para que o processo penal não se converta em instrumento de arbítrio sob o pretexto de eficiência investigativa[24].

---

23. "At the final stage of the investigation, investigators look through the copy for evidence of the crime. This raises a threat to privacy that I call the needle-in-a-haystack problem. Because computers can store an extraordinary amount of information, the evidence of crime is akin to a needle hidden in na enormous electronic haystack. If no rules regulate how investigators look through the haystack to find the needle, any justification for a search may justify an invasive look through computer files that represent a small city's worth of private information" (Kerr, 2005, p. 299-301).

24. Importa-se destacar o entendimento da 2ª Turma do Supremo Tribunal Federal reconhecendo a inconstitucionalidade do congelamento de dados sem autorização judicial, reforçando a centralidade do direito à privacidade e da autodeterminação informacional como cláusula de contenção do poder investigativo. A decisão reforça o argumento de que

Por último, a cadeia de custódia – de suma relevância para as provas digitais, dado seu caráter volátil e sua suscetibilidade a manipulações – constitui salvaguarda indispensável da fidedignidade probatória. A ausência de documentação rigorosa quanto à origem e integridade dos dados compromete sua validade jurídica e pode ensejar nulidades processuais.

Há quem defenda que por meio da cadeia de custódia das provas digitais seriam protegidos os direitos fundamentais à confidencialidade e integridade dos sistemas informáticos (Prado, 2021). Contudo, a garantia processual da cadeia de custódia tem por fundamento não só a proteção quanto à segurança dos sistemas informáticos por parte do Estado, mas também o dever de proteção contra intervenção estatal à revelia de qualquer respaldo legal e autorização judicial (Gleizer; Montenegro; Viana, 2021, p. 130).

Diante do cenário em que se debate a legitimidade da obtenção de dados de terceiros, armazenados em servidores de terceiro, mediante procedimentos de *backup* forçado e à revelia do titular, impõe-se a aplicação rigorosa do princípio da desconfiança processual.

Nesse contexto, a cadeia de custódia das provas digitais desempenha papel essencial ao registrar, de forma cronológica e documentada, todos os atos que integram a trajetória do vestígio probatório, desde sua origem até sua apresentação em juízo. Tal controle visa não apenas a preservação da autenticidade e da integridade do conteúdo digital, mas também a contenção de eventuais abusos por parte do poder estatal, assegurando que qualquer intervenção nos sistemas informáticos respeite os limites legais e constitucionais, inclusiva a necessária autorização judicial (Simarro Pedreira, 2020, p. 235).

No caso específico da obtenção de dados armazenados por terceiros em nuvem, especialmente quando realizada por meio de *backup* oculto e compulsório, o respeito à cadeia de custódia deve ser compreendido como imperativo constitucional. Tal instituto não é mera formalidade técnica, mas sim uma salvaguarda processual que assegura à parte acusada o controle da origem, da autenticidade e da manipulação da prova digital. Ignorar essa exigência significativa tolerar um processo penal vulnerável a falsificações, ocultações seletivas e práticas inquisitivas incompatíveis com o modelo acusatório (Massena, 2023, p. 21).

Em síntese, diante das especificidades da prova digital – marcadas por sua imaterialidade, fragilidade e elevada capacidade de invasão à intimidade – a preservação das garantias constitucionais torna-se ainda mais urgente e indispensável no processo penal; especificamente: reserva legal; direito à não autoincriminação; *fishing expedition* e cadeia de custódia.

---

a coleta de dados digitais exige rigor procedimental à legalidade, sob pena de invalidade da prova (Brasil, 2024).

4. Limites constitucionais: consentimento, temporalidade e tipificação penal específica

Cumpre-se destacar que a distinção entre segurança pública e persecução penal – para o Direito Processual Penal – é de suma importância para melhor compreensão sobre os limites de atuação do Estado. Isto é, enquanto a segurança pública tem por visão a prevenção da criminalidade e a manutenção da ordem social, a persecução penal, por sua vez, restringe-se à apuração e punição de delitos já cometidos, com a devida submissão a regras rígidas e a garantias constitucionais próprias.

Nesse contexto, a prática de obtenção de dados armazenados por terceiros em nuvem, especialmente quando realizada por meio de *backup* oculto e compulsório insere-se em zona de risco à luz da Constituição Federal, haja vista a inobservância de limites constitucionais próprios.

O Supremo Tribunal Federal, por sua vez, na Arguição de Descumprimento de Preceito Fundamental 444 veio a reforçar sobre a necessidade de que o acusado não possa ser constrangido a produzir provas contra si. Logo, deduz-se que, se é ilegítima a condução coercitiva para fins de interrogatório, de igual modo seria o acesso forçado a conteúdos digitais sem autorização válida, por configurar meio indireto de autoincriminação.

Para fins do presente artigo, três limites constitucionais – ao mínimo – precisariam ser observados para a supracitada medida pudesse vir a ter alguma perspectiva jurídica constitucional e legal de aceitabilidade por parte do sistema de justiça; quais sejam: a) consentimento; b) temporalidade e c) tipificação penal específica.

O consentimento, no presente cenário, aparece como primeiro balizador da licitude da medida. Significa, portanto, a manifestação de vontade informada e livre, cujo respeito assegura a autodeterminação informacional; este enquanto princípio estruturante do direito à proteção de dados pessoais (Brasil, 2024).

Todavia, no caso da prática de persecução penal atinente à obtenção de dados armazenados por terceiros em nuvem, realizado por meio de *backup* oculto e compulsório, o referido consentimento é não só suprimido como superado. Isto é, o titular não só desconhece a medida, como, em muitos casos, até chega a se manifestar de modo contrário à realização de *backup* em seus dados móveis. Isso, por sua vez, viola a um só tempo o direito à privacidade e o controle próprio do indivíduo sobre seus próprios dados.

Ainda que se invoque o contraditório diferido ou o elemento-surpresa típico da persecução penal, esses mecanismos, por sua vez, não podem suplantar a exigência do consentimento, pois representam exceções que não afastam a necessidade de proteção dos direitos fundamentais.

A jurisprudência do Superior Tribunal de Justiça sobre a entrada policial em domicílio com consentimento demonstra que, mesmo em espaços físicos, a validade

dessa permissão exige formalidades que garantam a ausência de coação. Essa lógica, por sua vez, deve ser estendida ao chamado "domicílio digital".

Assim como não se admite entrada em residência sem autorização legítima; de igual modo não deve ser admitido acesso a dispositivos ou nuvens privadas sem consentimento, salvo em casos excepcionais previamente autorizados pelo Poder Judiciário e desde que observados os limites constitucionais aqui defendidos.

Em complemento ao consentimento, o segundo critério/limite constitucional essencial que ora se defende é o da temporalidade; ou seja, a delimitação temporal assegura que o Estado só acesse informações relevantes ao fato investigado, evitando devassas indiscriminadas e violações desproporcionais à intimidade.

A título de exemplo, cumpre-se destacar que a interceptação telefônica, regulada pela Lei 9.296/1996, detém um prazo inicial de quinze dias, prorrogável por igual período, desde que justificado e autorizado judicialmente. Isso revela que, mesmo em casos de comunicação "ao vivo", há clara delimitação temporal, para fins de impedir abusos e violações a preceitos fundamentais.

Nessa medida, a ausência de limites temporais para a prática de obtenção de dados armazenados por terceiros em nuvem, especialmente quando realizada por meio de *backup* oculto e compulsório, é medida que compromete a proporcionalidade da medida. Isto é, sem delimitação temporal clara para a medida, o Estado pode acessar o histórico completo da vida digital de uma pessoa, inclusive quanto a períodos irrelevantes para a investigação (apesar de poder vir a servir para outras investigações), violando garantias e preceitos fundamentais.

Para tanto, a proposição que se propõe – enquanto parâmetro razoável – o limite de 90 dias antes e 90 dias depois do fato investigado, com possibilidade de uma única renovação. Esse marco busca equilibrar efetividade investigativa e proteção dos direitos do investigado.

Aliás, o próprio Superior Tribunal de Justiça, sobre relatórios genéricos do Coaf, reforça essa necessidade de delimitações, uma vez que informações sem recorte temporal claro constitui, verdadeiramente, na prática de *fishing expedition* e devem ser consideradas ilegais e inconstitucionais.

A experiência internacional confirma essa tendência. Espanha, Estados Unidos e França, por exemplo, já estabelecem prazos curtos e rigorosos para uso de ferramentas de monitoramento digital, exatamente para limitar excessos e proteger os direitos fundamentais individuais frente à tecnologia estatal.[25]

25. CORRÊA, Isadora Donza; MONTEIRO NETO, João Araújo A adesão do Brasil à convenção de Budapeste e o enfrentamento do cibercrime: entre a cooperação internacional e a expansão do direito penal. *Revista Eletrônica Direito & TI,* Porto Alegre, v. 1, n. 16, maio-ago. 2023. RAMALHO, David Silva. *Métodos ocultos de investigação criminal em*

Por fim, o terceiro e último critério é a vinculação a tipos penais específicos. Significa dizer que a prática de obtenção de dados armazenados por terceiros em nuvem, especialmente quando realizada por meio de *backup* oculto e compulsório, devem ser autorizadas apenas para investigar crimes de gravidade elevada, com potencial de ameaça significativa a bens jurídicos fundamentais.

A autorização genérica é insuficiente, ou seja, necessário um rol taxativo e legal claro definindo quais crimes justificam a adoção dessa medida extrema, para fins de garantir proporcionalidade e mínima previsibilidade da medida. Essa proposta, por sua vez, inspira-se no modelo português de ações encobertas, que delimita com precisão os delitos que podem justificar medidas invasivas no ambiente digital.

Nesse sentido, a sugestão que aqui se defende é a de que apenas crimes como: homicídio, sequestro, tráfico de pessoas, corrupção, terrorismo, exploração sexual infantil e crimes cibernéticos autorizem o uso da técnica, mediante decisão judicial fundamenta e rigoroso controle da medida.

Em síntese, o respeito aos critérios de consentimento, temporalidade e vinculação a tipos penais específicos é condição indispensável para que a prática de obtenção de dados armazenados por terceiros em nuvem – especialmente quando realizada por meio de *backup* oculto e compulsório – possa ser considerada constitucional. Do contrário, a medida configura grave violação ao Estado Democrático de Direito.

5. Considerações finais

A partir da análise desenvolvida nos três capítulos que compõem este estudo, constata-se que a prática da coleta de dados armazenados em nuvem por meio de *backup* forçado e velado ao titular – prática aqui denominada prova penal invisível – apresenta severos conflitos com o ordenamento jurídico-constitucional brasileiro. Ainda que o avanço tecnológico ofereça novos instrumentos de persecução penal, sua adoção não pode prescindir dos limites jurídicos impostos pelo Estado Democrático de Direito.

No primeiro capítulo, demonstrou-se que a ativação compulsória de sincronizações e *backup*s em sistemas de nuvem, realizada à margem do conhecimento do usuário, constitui forma de intervenção estatal sem respaldo legal específico. Tais práticas ocorrem, muitas vezes, por meio de decisões judiciais lastreadas em fundamentos normativos imprecisos, o que acarreta violação direta aos direitos

ambiente digital. Coimbra: Editora Almedina, 2019, p. 69. FONSECA, Marcos de Lucca; GENNARINI, Juliana Caramigo. A adesão do Brasil à convenção de Budapeste e os impactos para a produção de provas digitais. *Revista de Direito Penal e Processo Penal,* v. 4, n. 1, jan.-jun. 2012

fundamentais à privacidade, proteção de dados e autodeterminação informacional. A ausência de transparência e de controle por parte do titular revela um deslocamento preocupante do devido processo legal para uma lógica de vigilância digital não regulada.

Já no segundo capítulo, identificou-se que a obtenção forçada e velada de provas digitais afronta o núcleo duro das garantias constitucionais do processo penal, com destaque para a reserva legal, a vedação à autoincriminação, a proibição de *fishing expeditions* e a imprescindível observância da cadeia de custódia. A ausência de norma específica e a tentativa de suprir esse vazio com analogias legislativas indevidas comprometem a integridade do modelo acusatório e colocam em risco a confiabilidade do material probatório. O processo penal democrático não admite medidas excepcionais sustentadas em interpretações extensivas que ampliem, sem respaldo legislativo, o poder investigativo do Estado.

Por fim, o terceiro capítulo propôs três critérios mínimos e inafastáveis para que a eventual obtenção de dados em nuvem por meio de *backup* possa ser compatibilizada com o texto constitucional: (i) o consentimento livre e informado do titular dos dados; (ii) a delimitação temporal estrita da medida; e (iii) sua vinculação a tipos penais específicos, de elevada gravidade. Esses parâmetros visam assegurar a proporcionalidade e a previsibilidade na adoção de técnicas invasivas de coleta digital, evitando abusos e garantindo a preservação da dignidade e da liberdade individual.

Diante de todo o exposto, conclui-se que a prova penal invisível, tal como atualmente empregada, é inconstitucional e ilegal, por violar de forma sistemática os direitos fundamentais e as garantias processuais do investigado. A utilização da tecnologia na persecução penal não pode ser descolada dos marcos normativos que asseguram a legitimidade da atuação estatal. Longe de se opor à modernização dos instrumentos investigativos, este artigo defende sua regulamentação rigorosa, que respeite os princípios constitucionais e evite a erosão silenciosa das liberdades civis.

A efetividade da justiça penal não pode ser alcançada à custa da legalidade e da dignidade da pessoa humana. É preciso reafirmar que, mesmo diante de avanços tecnológicos e de demandas crescentes por eficiência, o processo penal deve continuar sendo um instrumento de contenção do poder punitivo e não de sua amplificação arbitrária.

Referências

ATERNO, Stefano; MATTIUCCI, Marco. Cloud forensics e nuove frontiere dele indagini informatiche nel processo penale. *Archivio Penale*, Pisa, v. LXV, n. 3, p. 865-878, 2013. Disponível em: [https://archiviopenale.it/File/DownloadArchivio?codice=2e337569-30a3-4165-9fc1-631594d49dac]. Acesso em: 10.04.2025.

BRASIL. Agência Nacional de Telecomunicações. *Identificação Internacional de Equipamento Móvel – IMEI*. Brasília: Disponível em: [www.gov.br/anatel/pt-br/assuntos/celularlegal/imei]. Acesso em: 10.04.2025.

GLEIZER, Orlandino; MONTENEGRO, Lucas; VIANA, Eduardo. *O direito de proteção de dados no processo penal e na segurança pública*. Rio de Janeiro: Marcial Pons, 2021.

GOOGLE. Disponível em: [https://policies.google.com/terms?utm_source=about.google&utm_medium=referral&utm_campaign=footer]. Acesso em: 10.04.2025.

ITÁLIA. Cass. Pen., sez. V. 29 abril 2010. n. 16556. Virruso. Disponível em: [www.penale.it/stampa.asp?idpag=1228]. Acesso em: 12.05.2025.

KERR, Orin S. Digital evidence and the new criminal procedure. *Columbia Law Review*, v. 105, p. 279-318, jan. 2005. Disponível em: [https://papers.ssrn.com/sol3/papers.cfm?abstract_id=594101]. Acesso em: 15.04.2025.

KUMAR, Krishan; KAUR, Prabhpreet. Vulnerability detection of international mobile equipment identity number of smartphone and automated reporting of changed IMEI number. *International Journal of Computer Science and Mobile Computing*, v. 4, n. 5, p. 527-533, 2015. Disponível em: [https://ijcsmc.com/docs/papers/May2015/V4I5201553.pdf]. Acesso em: 15.04.2025.

MANGANELLI, Elenice Colle; ROMANI, Juliano. *Protocolos de sincronização de dados em ambientes wireless*: um estudo de caso. 2004. Trabalho de Conclusão de Curso – Universidade Federal de Santa Catarina, Florianópolis, 2004. Disponível em: [https://repositorio.ufsc.br/bitstream/handle/123456789/183816/tcc.pdf?sequence=-1&isAllowed=y]. Acesso em: 15.04.2025.

MASSENA, Caio Badaró. A propósito da cadeia de custódia das provas digitais no processo penal: breves notas sobre lógica da desconfiança, assimetria informacional e direito de defesa. *Boletim IBCCRIM*, São Paulo, v. 31, n. 368, p. 19-21, jul. 2023. Disponível em: [https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/506]. Acesso em: 15.04.2025.

MENDES, Gilmar Ferreira; BRANCO Paulo Gustavo Gonet. *Curso de direito constitucional*. 17. ed. São Paulo: SaraivaJur, 2022 (Série IDP – Linha Doutrina).

MICROSOFT. Disponível em: [https://news.microsoft.com/facts-about-microsoft/]. Acesso em: 10.04.2025.

MOURA, Maria Thereza Rocha de Assis; BARBOSA, Daniel Marchionatti. Dados digitais: interceptação, busca e apreensão e requisição. In: LUCON, Paulo Henrique dos Santos et al. (Coord.). *Direito, processo e tecnologia*. 2. ed. rev. atual. e ampl. São Paulo: Thomson Reuters Brasil, 2021. p. 485-487.

MURGIA, Severino. *Prova informatica e processo penale*. 2017. Tesi (Dottorato in Diritto Pubblico, Giustizia Penale e Internazionale XXIX

Ciclo) – Università degli Studi di Pavia, Pavia, Itália, 2017. Disponível em: [https://iris.unipv.it/retrieve/e1f104fb-9b34-8c6e-e053-1005fe0aa0dd/Severino%20Murgia%20-%20Prova%20informatica%20e%20processo%20penale.pdf]. Acesso em: 15.04.2025.

OLIARI, Deivi Eduardo; ZAMBON, Cláudia Neli de Souza. Apple: como esta marca se tornou sinônimo de qualidade e hoje é a marca mais valiosa do mundo. In: CONGRESSO DE CIÊNCIAS DA COMUNICAÇÃO NA REGIÃO SUL, 15, 2014, Palhoça. *Anais...* São Paulo: Intercom – Sociedade Brasileira de Estudos Interdisciplinares da Comunicação, 2014. Disponível em: [https://canaltech.com.br/empresa/apple/]. Acesso em: 10.04.2025.

PAESE SEGUNDO, Wilson Antonio. Aquisição de provas criminais eletrônicas no Brasil à luz da convenção de Budapeste, do cloud act dos Estados Unidos da América e do direito da União Europeia. *Galileu*: *Revista de Direito e Economia*, Lisboa, v. XXII, p. 63-79, jan.-dez. 2022. Disponível em: [https://journals.ual.pt/galileu/wp-content/uploads/2023/02/Galileu_XXIII_1-2_Aquisicao.pdf]. Acesso em: 15.04.2025.

PRADO, Geraldo. Breves notas sobre o fundamento constitucional da cadeia de custódia da prova digital. *Geraldo Prado*, 22 jan. 2021. Disponível em: [https://geraldoprado.com.br/artigos/breves-notas-sobre-o-fundamento-constitucional-da-cadeia-de-custodia-da-prova-digital/]. Acesso em: 09.02.2024.

SIMARRO PEDREIRA, Margarita. La cadena de custodia em la prueba digital: España vs. EEUU. In: COLMENAREJO, Maria Jesús Ariza; RÍOS, Eva Isabel Sanjurjo (Coords.). *Exclusiones probatórias en el entorno de la investigación y prueba electrónica*. Madrid: Editorial Reus, 2020. p. 225-237.

WHATSAPP. *Sobre o WhatsApp Web e WhatsApp para computador*. [S.l.] [s.d.]. Disponível em: [https://faq.whatsapp.com/668538004658079/]. Acesso em: 11.04.2025.

Legislação

BRASIL. Constituição (1988). *Constituição da República Federativa do Brasil*. Brasília: Congresso Nacional, 1988. Disponível em: [www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm]. Acesso em: 25.11.2023.

BRASIL. *Decreto 678/1992*. Promulga a Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica), de 22 de novembro de 1969. Brasília: Presidência da República, 1992. Disponível em: [www.planalto.gov.br/ccivil_03/decreto/d0678.htm]. Acesso em: 10.04.2025.

BRASIL. *Decreto-lei 2.848, de 7 de dezembro de 1940*. Código Penal. Rio de Janeiro: Presidência da República, 1940. Disponível em: [www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm]. Acesso em: 10.04.2025.

BRASIL. *Projeto de Lei 2126/2011*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília: Câmara dos Deputados, 2011. Disponível em: [www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=517255]. Acesso em: 12.05.2025.

BRASIL. *Lei Complementar 105, de 10 de janeiro de 2001*. Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências. Brasília: Presidência da República, 2001. Disponível em: [https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm]. Acesso em: 10.04.2024.

BRASIL. *Lei 9.296, de 24 de julho de 1996*. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Brasília: Presidência da República, 1996. Disponível em: [https://www.planalto.gov.br/ccivil_03/leis/l9296.htm]. Acesso em: 10.04.2025.

BRASIL. *Lei 9.613, de 3 de março de 1998*. Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras – COAF, e dá outras providências. Brasília: Presidência da República, 1998. Disponível em: [www.planalto.gov.br/ccivil_03/leis/l9613.htm]. Acesso em: 10.04.2025.

BRASIL. *Lei 12.850, de 2 de agosto de 2013*. Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei 9.034, de 3 de maio de 1995; e dá outras providências. Brasília: Presidência da República, 2013. Disponível em: [www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm]. Acesso em: 10.04.2025.

BRASIL. *Lei 12.965/2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília: Presidência da República, 2014. Disponível em: [www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm]. Acesso em: 10.04.2025.

BRASIL. *Lei 14.133, de 1º de abril de 2021*. Lei de Licitações e Contratos Administrativos. Brasília: Presidência da República, 2021a. Disponível em: [www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14133.htm]. Acesso em: 10.04.2025.

Jurisprudência

BRASIL. Superior Tribunal de Justiça, Recurso Especial 1.875.514/MS, rel. Min. Laurita Vaz. j. 30.08.2021b. Disponível em: [https://processo.stj.jus.br/processo/dj/documento/mediado/?tipo_documento=documento&componente=MON&sequencial=133376782&tipo_documento=documento&num_registro=202001201736&data=20210901&formato=PDF]. Acesso em: 22.04.2025.

BRASIL. Supremo Tribunal Federal, Plenário, Ação Declaratória de Constitucionalidade 51/DF, rel. Min. Gilmar Mendes, j. 23.02.2023. Disponível em: [https://portal.stf.jus.br/processos/detalhe.asp?incidente=5320379]. Acesso em: 22.04.2025.

BRASIL. Supremo Tribunal Federal, 2ª T., Agravo Regimental no Habeas Corpus 222.141/PR, rel. Min. Ricardo Lewandowski, Redator do Acórdão: Min. Gilmar Mendes, j. 06.02.2024.

BRASIL. Supremo Tribunal Federal, Habeas Corpus 131.946/MG, rel. Min. Edson Fachin, j. 16.12.2015. Disponível em: [https://portal.stf.jus.br/processos/detalhe.asp?incidente=4899543]. Acesso em: 15.04.2025.

Autores convidados

PESQUISA DO EDITORIAL

Área do Direito: Processual; Penal; Digital

Veja também Doutrina relacionada ao tema

- Busca e apreensão de dados em telefones celulares: novos desafios diante dos avanços tecnológicos, de Ricardo Jacobsen Gloeckner e Daniela Dora Eilber – *RBCCrim* 156/353-393;
- O *malware* enquanto meio de prova: um estudo transdisciplinar entre os processos trabalhista e penal, de Cláudio Iannotti da Rocha e João Victor Loss de Souza – *RT* 1067/245-266;
- Prova penal: da semiótica à importância da cadeia de custódia, de Ana Luisa Zago de Moraes – *RBCCrim* 132/117-138;
- Prova penal: STJ rejeita arquivo digital parcialmente corrompido, de Luiz Antonio Borri, Gustavo Noronha de Ávila e Rafael Junior Soares – *BRTO* 60; e
- Valoração da prova digital: entre a desconfiança e a crença, de Luíza Guimarães Campos Batista Gomes e André Ricardo Godoy de Souza – *RePro* 359/175-207.

Veja também Jurisprudência relacionada ao tema

- STJ, EDcl no AgRg no RHC 184003/SP, j. 10.04.2025, *DJe* 14.04.2025; e
- STJ, RHC 184003, j. 10.12.2024, *DJe* 26.12.2024.

Compartilhamento de dados financeiros na persecução penal

Financial data sharing in criminal prosecution

Luiz Eduardo Cani[1]
Universidade Regional de Blumenau, FURB, Brasil.
luizeduardocani@gmail.com

DOI: [doi.org/10.5281/zenodo.17058237].

Área do Direito: Processual; Penal

Resumo: O compartilhamento de dados financeiros é um problema central do direito processual penal contemporâneo. Neste artigo, analisa-se as atividades de inteligência financeira, destacando (a) as transformações que resultaram no indevido acoplamento das atividades de inteligência à persecução penal, (b) o surgimento da inteligência financeira e suas consequências na persecução penal, (c) os critérios legais e jurisprudenciais de compartilhamento dos dados financeiros, e (d) o aproveitamento de dados ilicitamente obtidos na persecução penal (lavagem de dados ilícitos). A pesquisa revela a persistente divergência jurisprudencial sobre os limites do compartilhamento dos dados financeiros. Os métodos adotados são o dedutivo (abordagem) e o monográfico (procedimento) com consulta a fontes secundárias de ordem bibliográfica (livros e artigos) e documental (legislação e jurisprudência).

Abstract: The financial data sharing is a central problem in contemporary criminal procedural law. In this article, it is analyzed the financial intelligence activities, highlighting (a) the transformations that resulted in the improper coupling of intelligence activities to criminal prosecution, (b) the emergence of financial intelligence and its consequences for criminal prosecution, (c) the legal and jurisprudential criteria for sharing financial data, and (d) the use of illicitly obtained data in criminal prosecution (illicit data laundering). The research reveals the persistent divergence in jurisprudence on the limits of sharing financial data. The methods adopted are deductive (approach) and monographic (procedure) with consultation of secondary sources of bibliographic (books and articles) and documentary (legislation and jurisprudence) order.

1. Pós-Doutor e Doutor (com voto de louvor) em Ciências Criminais (PUCRS). Professor de Direito Penal e Processo Penal (FURB). Consultor jurídico e parecerista.
Currículo Lattes: [http://lattes.cnpq.br/8283452898258709].
ORCID: [https://orcid.org/0000-0003-4016-5945].
E-mail: luizeduardocani@gmail.com

Palavras-chave: Relatório de inteligência financeira – Representação fiscal para fins penais – Proteção de dados – Compartilhamento de provas – Processo penal.

Keywords: Financial intelligence report – Tax representation for criminal purposes – Data protection – Evidence sharing – Criminal procedure.

Sumário: 1. Introdução. 2. Redefinição da persecução penal: do procedimento bifásico ao trifásico. 3. Da inteligência de guerra à inteligência financeira: terceirização da persecução penal e atribuição de funções atípicas de segurança pública a órgãos financeiros. 4. Compartilhamento de dados financeiros no processo penal. 5. Lavagem de dados financeiros ilícitos no processo penal. 6. Considerações finais. Referências. Legislação. Jurisprudência.

1. Introdução

As[2] discussões sobre os limites, requisitos e efeitos do compartilhamento de dados financeiros receberam maior destaque apenas com o julgamento de algumas ações de impugnação em 2024. Contudo, são mais antigas as preocupações com temas correlatos, como separação informacional, autodeterminação informativa, proteção de dados pessoais, inteligência de segurança pública, sigilos bancário e fiscal. A relevância do tema se deve à concepção de que os regimes de governo adotados pelos Estados podem ser analisados pelas intervenções processuais penais autorizadas[3].

Os Relatórios de Inteligência Financeira (RIF) do Conselho de Controle de Atividade Financeira (Coaf) e as Representações Fiscais para Fins Penais da Fazenda Pública (RFPP) são os dois principais arquivos com dados financeiros compartilhados na persecução penal. O aproveitamento desses arquivos na persecução penal gera problemas semelhantes, apesar de possuírem sujeitos ativos e finalidades distintas.

Destaca-se que arquivos não são provas documentais. Arquivos são produzidos depois da prática da infração penal. Documentos são elaborados antes do crime para praticá-lo, como a nota fiscal com valor inferior ao da operação para sonegar

2. Agradeço a Rodrigo Oliveira de Camargo, Carlos Hélder Carvalho Furtado Mendes, Marcelo Almeida Ruivo, Carlo Velho Masi, Fernanda Osório e Virgínia Lessa pela discussão prévia de várias ideias que compõem este pequeno texto.
3. Daí a afirmação de que "Los princípios de la política procesal de uma nación no son outra cosa que segmentos de su política estatal em general. Se puede decir que la estrutura del proceso penal de uma nación no es sino el termómetro de los elementos corporativos o autoritários de su Constitución" (Goldschmidt, 1935, p. 67).

tributos, ou se constituem durante a prática da infração, como o registro de acesso não autorizado a sistema informático[4].

O problema mais relevante nessa matéria é a delimitação do âmbito de proteção formado no encontro entre os sigilos bancário e fiscal, a proteção de dados pessoais e a legalidade. Portanto, pergunta-se: Como os dados financeiros são compartilhados na persecução penal? O objetivo geral é analisar o compartilhamento de dados financeiros na persecução penal. Os objetivos específicos são: (a) destacar as transformações que resultaram no indevido acoplamento das atividades de inteligência à persecução penal, (b) explicar o surgimento da inteligência financeira e suas consequências na persecução penal, (c) analisar os critérios legais e jurisprudenciais de compartilhamento dos dados financeiros, e (d) explicitar o aproveitamento de dados ilicitamente obtidos na persecução penal, caracterizando ilícita lavagem de dados.

A relevância do tema decorre da existência de situações de intervenção estatal indevida nos direitos fundamentais, sobretudo justificadas a pretexto da persecução dos crimes de lavagem de dinheiro, financiamento ao terrorismo, organizações criminosas e tributários.

O método de abordagem empregado é o dedutivo, na medida em que a conclusão se segue das premissas analisadas ao longo do texto. O método de procedimento é o monográfico. A técnica de pesquisa é a bibliográfica, com consulta a fontes secundárias, de ordem bibliográfica (livros e artigos) e documental (legislação e jurisprudência).

2. Redefinição da persecução penal: do procedimento bifásico ao trifásico

A concepção tradicional de persecução penal estrutura-se em duas atividades complementares no tempo e no objeto. O início da persecução se dá com a obtenção, de ofício ou mediante comunicação de terceiros, da informação acerca da suposta prática de um crime (notícia-crime)[5]. A partir de então deve ser instaurado o procedimento investigatório com a finalidade de produzir elementos que confirmem ou refutem a notícia-crime. Produzidos elementos suficientes de materialidade e autoria (justa causa) e presentes as demais condições da ação penal[6], pode

4. "O documento forma-se em geral na presença do fato documentado e na ausência do destinatário da representação, ao passo que a testemunha depõe em presença deste e na ausência daquele" (Carnelutti, 2004, p. 298).

5. Daí a referência do art. 5º, *caput* e §§ 4º e 5º, do CPP à preexistência de crimes.

6. Não se desconsidera a defesa majoritária da aplicação da teoria geral do processo ao processo penal. Apenas discorda-se do cabimento do interesse de agir, caracterizado pela necessidade e utilidade da tutela jurisdicional. Se o direito civil é autoexecutável e a tutela

ser desencadeada a segunda fase da persecução penal com a acusação (denúncia ou queixa-crime) e seu processamento[7].

A distinção entre investigação e processo existe também nos países de *common law*, embora os institutos sejam outros. A estrutura bifásica, nos países de *civil law*, remonta ao procedimento misto[8], estruturado a partir da junção de dois procedimentos antagônicos: a Ordenança Criminal (*Ordonnance Criminelle*) francesa de 1670 e o Tribunal do Júri (*Trial by Jury*) inglês. Eis a origem da primeira fase, de investigação criminal, com características inquisitórias e da segunda fase, processual, com características acusatórias. O modelo foi estabelecido no Código de Instrução Criminal (*Code d'Instruction Criminelle*) francês de 1808[9] (Código Napoleônico), "em vigor desde 1º de janeiro de 1811" (Coutinho, 2001, p. 37).

---

jurisdicional é invocável somente diante da inércia (pretensão insatisfeita) ou oposição (pretensão resistida) do legitimado passivo, o direito penal não pode, por si só, ver aplicada a pena cominada a um tipo penal. Daí que ao processo penal não servem nem a lide como conteúdo, nem as condições da ação civil (cf.: Coutinho, 1989, p. 129-148), inclusive porque a aplicação de uma pena pressupõe o processo penal (princípio da necessidade) até mesmo para a homologação de um acordo (*vide* Lopes Jr., 2024, p. 2-3).

7. "É para *acusar* que o Estado *investiga* o delito e sua autoria e propõe, ulteriormente, a ação penal. Donde inferir-se que a *persecutio criminis* tem por objeto: a) preparar a acusação; b) invocar a tutela jurisdicional do Estado-Juiz para julgar a acusação. [...] No genitivo *criminis* ou *delicti* da designação jurídica de vários institutos da persecução penal está cristalizado o princípio de que não pode haver atuação persecutória do Estado sem tipicidade. Assim é que, para a existência de investigação (que é uma *informatio delicti*), torna-se imprescindível a *notitia criminis*, isto é, a comunicação ou o conhecimento de conduta configurada como fato típico. A suspeita de crime, ou *opinio delicti*, base e fundamento da acusação, consiste sobretudo na possibilidade de existência de crime decorrente da prática presumível de fato típico" (Marques, 1997, p. 129-130 – grifos nossos).
8. Muitas vezes indevidamente chamado de sistema misto: "não há mais sistema processual puro, razão pela qual tem-se, todos, como sistemas mistos. Não obstante, não é preciso grande esforço para entender que não há – e nem pode haver – um princípio misto, o que, por evidente, desconfigura o dito sistema. Assim, para entendê-lo, faz-se mister observar o fato de que, ser misto significa ser, na essência, inquisitório ou acusatório, recebendo a referida adjetivação por conta dos elementos (todos secundários), que de um sistema são emprestados ao outro" (Coutinho, 1998, p. 167).
9. "E assim, da Lei de 17 de novembro de 1808, nasce o processo chamado misto, monstro de duas cabeças: no labirinto escuro da instrução, reina Louis XIV; segue uma cena disputada diante do povo. Para alguns, parece uma obra prima: segundo os eufemistas, *l'information préliminaire* como aparece na *Ordonnance* de 1670, 'é uma das mais preciosas conquistas da legislação'; habilmente conduzida, 'protege os direitos dos cidadãos contra as medidas imprudentes; prepara o julgamento; assegura a sabedoria'; em suma, é o legado 'mais fecundo' do século XV aos modernos" (Cordero, 1986, p. 73, tradução livre).

Esse procedimento misto foi esboçado por Philippe-Antoine Merlin e Jean-Jacques Régis de Cambacérès no (Código dos Delitos e das Penas (*Code des Délits et des Peines*) de 1795 e aprimorado por Jean-Jacques Régis de Cambacérès no *Code d'Instruction Criminelle*. As suas duas principais características são o início da persecução com uma investigação inquisitória inspirada na *Ordonnance Criminelle* de 1670 e a admissão no processo de documentos produzidos na investigação (cf.: Esmein, 1882, p. 440-455).

O *Code d'Instruction Criminelle* inspirou os redatores do Código de Processo Penal (*Codice di Procedura Penale*) italiano fascista de 1930 (Código Rocco), que posteriormente inspirou o Código de Processo Penal brasileiro de 1941. O processo penal brasileiro também admite o conhecimento dos elementos de investigação, mas não permite uma condenação fundada exclusivamente nos elementos informativos (art. 155 do CPP).

Até a década de 2010, o principal problema do procedimento misto era a frequente redução da fase processual à fase de investigação com a mera repetição dos elementos investigatórios por meio da sua leitura em audiência[10]. A máxima amplitude dessa distorção ainda pode ser percebida em muitos casos penais no plenário do Júri nos quais sequer há inquirição de testemunhas.

A situação foi substancialmente alterada com a soma das diversas transformações jurídicas e tecnológicas em curso, o que não é devido a uma única mudança ou mesmo a uma invenção da década de 2020 ou do século XXI.

As transformações tecnológicas são produtos da "Revolução 4.0", que se acelerou com a elaboração do primeiro modelo funcional de rede neural profunda, vencedor do desafio ImageNet (2012). Destacam-se três alterações principais: (a) aumento da capacidade de armazenamento e processamento de dados, (b) distribuição de sinal de internet por fibra ótica e (c) otimização da internet móvel que permitiram a efetivação da inteligência artificial, a elaboração de aparelhos *smart* e a implementação da internet das coisas (Assange, 2015; Harcourt, 2015).

As principais transformações jurídicas foram desenvolvidas a partir da década de 1980, na Itália e nos Estados Unidos da América (EUA), países com sistemas jurídicos e motivações distintos. Essas medidas posteriormente foram integradas

10. "No fundo, toda a prova produzida na primeira fase da persecução, de regra por um *juiz instrutor*, na investigação preliminar puramente inquisitorial, era usada na fase processual, por exemplo, por sua leitura no chamado *Jugement*. A sessão virava, como era sintomático, teatro, não raro pantomima; puro embuste; e os discursos, pomposos e longos, inflação fonética. As cartas do jogo já estavam marcadas e para desdizer isso era preciso desacreditar na figura democrática do *juiz instrutor*, tão inquisidor quanto qualquer outro que, na história, ocupou aquele *lugar*" (Coutinho, 2010, p. 10 – grifos nossos).

e difundidas globalmente por meio da elaboração e ratificação de tratados internacionais, especialmente a Convenção Contra o Tráfico Ilícito de Entorpecentes e Substâncias Psicotrópicas de 1988 (Convenção de Viena sobre Tráfico) e a Convenção das Nações Unidas contra o Crime Organizado Transnacional de 2000 (Convenção de Palermo).

Nos EUA, as mudanças foram fortemente influenciadas pela política criminal de "combate à lavagem de dinheiro" desenvolvida a partir da "guerra às drogas"[11]. Em reação do comércio de drogas criminalizadas, os EUA reforçaram o *Bank Secrecy Act* de 1970 por meio da edição do *US Money Laundering Control Act* de 1986, que criminalizou pós-fatos anteriormente não punidos, estabeleceu estruturas de fiscalização e deveres de comunicação de suspeitas que resultaram na terceirização de atos de persecução penal.

Na Itália, as mudanças começaram com o maxiprocesso de Palermo contra a *Cosa Nostra*, um dos capítulos mais conhecidos da chamada luta antimáfia, iniciado em 1986 e concluído em 1992. Poucos meses depois da sentença foi editado o *Decreto-legge* 306, de 8 de junho de 1992, a Lei Antimáfia, em que foram criados órgãos especializados na persecução penal da máfia e estabelecidas técnicas especiais de investigação e obtenção de provas (Orlandi, 2021). A inovação mais relevante dessa lei foi a criação de uma fase prévia à investigação criminal oficial, chama investigação preparatória (*inchieste preparatorie*), resultando na agregação de uma fase de inteligência à persecução penal que visa obter a notícia-crime para instaurar a investigação criminal (*indagine preliminare*)[12].

O encontro dessas transformações se deu em nível internacional com a ratificação das convenções que estipularam medidas inspiradas nas legislações nacionais dos EUA e da Itália.

A Convenção de Viena sobre Tráfico[13] estipulou o compromisso dos países signatários de criminalizar as drogas ilícitas e estabelecer medidas para a persecução

11. "A lavagem de dinheiro passou a ser objeto de maior atenção da comunidade internacional ao final dos anos 80 do século XX, quando se percebeu a força e a capacidade de articulação de alguns setores do crime organizado, em especial daquele voltado para o tráfico de drogas. [...] Notou-se que o *dinheiro* é a alma da organização criminosa e seu combate passa pelo *confisco* dos valores que mantém operante sua estrutura. [...] Como boa parte desse capital é *mascarada*, ocultada por atividades aparentemente lícitas, o combate à *lavagem de dinheiro* passou a ser o foco da política criminal de combate ao crime organizado" (Badaró; Bottini, 2019, p. 26 – grifos nossos).
12. A medida é considerada uma repristinação da *inquisitio generalis*, um procedimento investigatório da por meio do qual o Santo Ofício da Inquisição buscava ativamente comunicações de crimes: cf.: Orlandi (2021, p. 371-391).
13. "As Partes nesta Convenção, [...] Reconhecendo os vínculos que existem entre o tráfico ilícito e outras atividades criminosas organizadas, a ele relacionadas, que minam as

do tráfico de drogas e da ocultação e encobrimento da origem ilícita de bens (art. 3). A Convenção de Palermo (Brasil, 2004) estipulou o compromisso internacional de criminalizar as organizações criminosas (art. 5), a lavagem de dinheiro (art. 6), a corrupção (art. 8) e a obstrução à justiça (art. 23) e a estabelecer medidas de persecução desses crimes, como as medidas especiais de prevenção à lavagem de dinheiro (art. 7), programas anticorrupção (art. 9), responsabilização de pessoas jurídicas (art. 10), ajuste dos ordenamentos jurídicos internos para a persecução das organizações criminosas, lavagem de dinheiro, corrupção e obstrução à justiça (art. 11), confisco e apreensão com cooperação internacional (arts. 12-14), extradição e transferência de presos (arts. 16-17), assistência judiciária recíproca (art. 18), investigações conjuntas entre Estados Partes (art. 19), técnicas especiais de investigação (art. 20), transferência de processos penais (art. 21), medidas de proteção e assistência às testemunhas (arts. 24-25), cooperação jurídica internacional (arts. 26-27 e 30), coleta, análise e compartilhamento de informações sobre o crime organizado (art. 28), formação e assistência técnica dos agentes do sistema penal (art. 29) e estabelecimento de medidas preventivas (art. 31).

As Convenções de Viena sobre o Tráfico e de Palermo estabeleceram as bases atuais de duas transformações penais: (a) a criminalização autônoma de atos preparatórios[14] e do exaurimento[15] e (b) a atuação transnacional do sistema penal e cooperação entre Estados Partes.

As atividades de inteligência foram inseridas pouco a pouco na persecução penal, embora essas convenções não prevejam um procedimento parecido com a *inchieste preparatorie*. Com isso, o procedimento bifásico foi transformado em procedimento trifásico. De uma fase de investigação inquisitória seguida de uma fase processual acusatória, passou-se a uma fase de inteligência inquisitória seguida de uma fase de investigação inquisitória concluída com uma fase processual acusatória (Morais da Rosa; Cani, 2023). A inserção de uma etapa pré-processual adicional, exauriente nos planos horizontal e vertical[16], reduz a importância da instrução

economias lícitas de ameaçam a estabilidade, a segurança e a soberania dos Estados, [...] Convêm o que segue" (Brasil, 1991).

14. P. ex., art. 3, 1, da Convenção de Viena sobre Tráfico estabelece diversos comportamentos prévios ao comércio de drogas, como produzir, extrair, preparar, distribuir, cultivar, ter, adquirir etc. Do mesmo modo, o art. 5, 1, a, da Convenção de Palermo estabelece como criminosos o entendimento, o envolvimento e a participação de grupo criminoso.

15. P. ex., art. 3, 1, b, da Convenção de Viena sobre Tráfico considera penalmente relevante a ocultação ou encobrimento de bens oriundos do tráfico de drogas. O art. 6, 1, a, i, da Convenção de Palermo trata da conversão ou transferência de bens produto de crime com o propósito de ocultar ou dissimular a origem ilícita.

16. "Uma das maiores críticas que se faz ao IP é a repetição na produção da prova. O inquérito policial é normativamente sumário, inclusive com limitação quantitativa ou temporal, mas

processual, agravando o tradicional desequilíbrio entre as fases de investigação e processo (cf.: Lopes Jr., 2024, p. 167-168).

A junção da antecipação da consumação, por meio da criminalização de atos preparatórios, com e antecipação da persecução penal, através da inserção de atividades de inteligência, produz um efeito de estrangulamento dos imputados.

Frequentemente, as atividades de inteligência incorporadas nos procedimentos investigatórios são confundidas com atos de investigação e posteriormente aproveitadas como prova na fase processual. De acordo com Luís Greco, a inserção de atividades de inteligência resultou na criação de quatro institutos na Alemanha. Primeiro, as investigações no campo prévio são conduzidas em ambientes considerados problemáticos antes da existência de qualquer suspeita ou perigo. Segundo, as pré-investigações são exceções legais que dispensam a suspeita prévia e trabalham com suspeitas de suspeitas. Terceiro, as investigações proativas deslocam o centro de gravidade da persecução penal, passando da reação para a busca ativa do que, no Brasil, chama-se notícia-crime. Quarto, a preparação para a persecução penal é uma atividade prévia desencadeada com a constatação de uma situação de perigo (Greco, 2018, p. 52 e 57-58).

A questão central dessas mudanças é consequência direta da distinção entre investigação e atividades de inteligência, independente da criação de institutos autônomos e dos nomes atribuídos. As atividades de inteligência podem ser definidas a partir de dois critérios: (a) a atuação antecipada a qualquer evento potencialmente perigoso e (b) informar a tomada de decisões com caráter preditivo[17]. Portanto, diferente da investigação, desencadeada a partir do momento em que as agências do sistema penal obtêm notícias-crime, a atividade de inteligência é sempre preventiva. A atividade de inteligência sempre visa decidir, antecipar um movimento para neutralizar um risco ou um perigo. O pressuposto geral é, portanto, a suspeita.

---

o que sucede na prática é que ele se transforma de fato em plenário. Essa conversão – de normativamente sumário em efetivamente plenário – é uma gravíssima degeneração. A polícia demora excessivamente a investigar, investiga mal e, por atuar mal, acaba por alongar excessivamente a investigação. O resultado final é um inquérito inchado, com atos que somente deveriam ser produzidos em juízo, e que por isso desborda os limites que o justificam" (Lopes Jr., 2024, p. 136-137). Esse comentário é generalizável para todos os procedimentos investigatórios, pois as disposições do inquérito policial se aplicam subsidiariamente também ao procedimento investigatório criminal do MP, nos termos das ADI 2.943, 3.309 e 3.318.

17. "Serviços de inteligência são agências governamentais responsáveis pela coleta, análise e disseminação de informações consideradas relevantes para o processo de tomada de decisões e de implementação de políticas públicas nas áreas de política externa, defesa nacional e provimento de ordem pública" (Cepik, 2023, p. 34).

A falta de notícia-crime a apurar e a necessidade de obtê-la para desencadear uma investigação resulta na generalização de suspeitas. Não suspeitas determinadas, senão suspeitas generalizadas: todos podem ter praticado infrações penais que precisam ser descobertas. Não por acaso, o pressuposto da atividade de inteligência é a existência de conflitos, conforme reconhecido por Marco Cepik, ex-diretor-adjunto da Agência Brasileira de Inteligência (Abin)[18].

Essa concepção altera profundamente tanto a persecução penal quanto o sistema penal, esboroando e confundindo os limites das atividades de cada uma de suas agências. Consequentemente, a persecução passa a ser ininterrupta e predominantemente preventiva. Isso pode ser percebido sobretudo nas operações que não cessam de continuar e ser continuadas em novas operações instauradas a partir de elementos produzidos muitos anos antes, parecendo nunca ter fim.

3. Da inteligência de guerra à inteligência financeira: terceirização da persecução penal e atribuição de funções atípicas de segurança pública a órgãos financeiros

A inteligência tem uma relação íntima com a espionagem: utiliza uma ampla gama de técnicas, inclusive da espionagem, mas se aplica a contextos mais restritos[19]. A atividade parece ter surgido concomitantemente em diversos países durante a antiguidade (Cepik, 2023, p. 34). A atribuição da sua emergência na antiguidade se deve a vários elementos, como a menção ao uso de espiões na Ilíada de Homero[20] e a figura mítica do gigante Argos Panoptes, que podia ver tudo com os olhos que recobriam seu corpo. Contudo, talvez a espionagem seja tão antiga quanto à civilização minoica[21].

18. "Diferentemente de institutos de geografia e estatística ou de centros de pesquisa econômica aplicada, serviços de inteligência estão voltados para a compreensão de relações adversariais e por isso a maioria de seus alvos e/ou problemas são principalmente internacionais e 'difíceis'. Inteligência lida com o estudo do 'outro' e procura elucidar situações nas quais as informações mais relevantes são potencialmente manipuladas ou escondidas [...] Os chamados serviços de inteligência de segurança (*security intelligence*) têm muitos alvos puramente domésticos, mas mesmo esses compartilham a condição de 'outro' aos olhos do arcabouço constitucional e da ordem política constituída" (Cepik, 2023, p. 59).
19. "As atividades dos serviços de inteligência são mais amplas do que a espionagem e também são mais restritas do que o provimento de informações em geral sobre quaisquer temas relevantes para a decisão governamental" (Cepik, 2023, p. 57).
20. No canto X, Agamemnon envia espiões para o acampamento troiano e Heitor envia um espião para o acampamento aqueu (Homero, 1996, p. 169-180).
21. Sobre os minoicos, micênicos e a formação da antiguidade clássica: Vernant (1992).

As atividades de inteligência contemporâneas foram desenvolvidas a partir dos Estados modernos europeus que integraram três matrizes de atividades: "a diplomacia, o fazer a guerra e o policiamento" (Cepik, 2023, p. 46).

O desenvolvimento da atividade de inteligência da modernidade à contemporaneidade pode ser dividido em três gerações.

Na primeira, as atividades de inteligência foram desempenhadas pelas forças armadas e pelas agências especializadas, como a CIA e a Abin, para coletar, analisar e disseminar informações para a tomada de decisão em matéria de política externa e defesa nacional[22]. Essas atividades de inteligência foram aprimoradas e amplamente utilizadas nas guerras não convencionais (guerra modernas) travadas depois da segunda guerra mundial. A estratégia de contrainsurgência implementada na guerra não convencional é orientada por três princípios: (a) luta pelo apoio da população, (b) separação da minoria revolucionária da maioria passiva para obter o apoio da população e (c) coleta de informação total sobre a população envolvida na guerra para "distinguir adequadamente o amigo do inimigo e depois suprimir a minoria revolucionária" (Harcourt, 2021, p. 44).

Na segunda, desenvolvida após a Guerra Fria, as atividades de inteligência foram adaptadas e passaram a ser amplamente utilizadas pelos Estados contra os próprios cidadãos. O momento decisivo para o desenvolvimento da inteligência de segurança pública é, sem dúvida, 11 de setembro de 2001. As medidas de combate ao terrorismo propostas em reação aos atentados foram estruturadas em três eixos: (a) vigilância em massa e coleta de total dados de cada indivíduo da população, (b) identificação e erradicação da minoria revolucionária e (c) pacificação das massas com o direcionamento de conteúdo adequado, garantia apenas do mínimo de bem-estar e assistência humanitária e demonstração de poder e controle sobre o território pelo Estado (Harcourt, 2021, p. 65-67).

Na terceira, órgãos fiscais recebem atribuições atípicas de apuração preliminar de infrações penais tributárias, são criadas obrigações de comunicações de operações suspeitas para particulares como parte da política de prevenção à lavagem de dinheiro e é estabelecida uma UIF em nível nacional para receber as comunicações das operações suspeitas financeiras e fazer a apuração preliminar da lavagem de dinheiro. Embora os órgãos fiscais tenham atribuições tributárias, a apuração do (não) pagamento de tributos se dá também a partir da análise de movimentações financeiras. Consequentemente, tanto os órgãos fiscais quanto as UIFs podem realizar atividades de inteligência financeira.

22. *Vide* Cepik (2023, p. 34). A garantia da ordem pública, referida no trecho, é atribuição da inteligência de segurança pública.

A chegada das gerações ao Brasil pode ser consultada na legislação. A primeira geração, amplamente utilizada pelas forças armadas e de segurança pública na ditadura de 1964-1985, atualmente está prevista na Lei 9.883/1999, que criou o Sistema Brasileiro de Inteligência (SISBIN) com os objetivos de preservar a soberania nacional e defender o Estado Democrático de Direito e os direitos fundamentais (art. 1º). A segunda, por meio da inserção expressa da inteligência de segurança pública no rol de atividades típicas das polícias por meio da Lei 13.675/2018, que determinou o uso da inteligência para atingir os objetivos da Política Nacional de Segurança Pública (art. 6º, I e IX), autorizou[23] o compartilhamento de informações e a combinação de operações (art. 10, IV e § 2º), atribuiu ao Ministério da Segurança Pública a coordenação das atividades integradas ao Sistema Brasileiro de Inteligência e o desenvolvimento da doutrina de inteligência policial (art. 13, VII e VIII). A terceira foi estabelecida antes das demais, originalmente prevista no art. 83 da Lei 9.430/1996 e nos arts. 9, 10, 11 e 15 da Lei 9.613/1996.

A legislação brasileira instituidora das atividades de inteligência de segunda e terceira gerações causa duas violações básicas à legalidade. A primeira é a usurpação de atribuições constitucionais dos órgãos de segurança pública. Nesse sentido, a inteligência de segurança pública e a inteligência financeira frequentemente são conduzidas por Guardas Municipais, pelas Polícias Militares, pela Fazenda Pública ou pelo Coaf, usurpando atribuições das Polícias Civis e Federal. A segunda é a condução das atividades sem a instauração de um procedimento investigatório oficial[24], frequentemente a pretexto das indevidas autorizações legais para diligências paralelas na investigação de organizações criminosas (art. 23, parágrafo único, da Lei 12.850/2013) ou no processamento de tráfico de drogas (art. 52, parágrafo único, I, da Lei 11.343/2006) ou de crimes do rito do Júri (art. 479 do CPP).

A inteligência financeira no Brasil é desempenhada concomitantemente pela Fazenda Pública dos Municípios, Estados, Distrito Federal e da União (art. 199 do

23. Vale referir a distinção entre autorização e regulamentação: "no Brasil [...] não se pergunta por lei fundamentadora ou autorizadora da intervenção em direito fundamental, e sim por lei *regulamentadora* – como se apenas se tratasse de legislar sobre o como, e não sobre o se" (Greco, 2018, p. 40 – grifos nossos).

24. "Com fundamento na usurpação de atribuições de forças de defesa e da introdução de atribuições de guerra em face de cidadãos no interior do território nacional, em pleno estado de paz, questiona-se, inclusive, a constitucionalidade material de atribuições de inteligência para órgãos de segurança pública, assim como a própria licitude do resultado da inteligência como prova, já que sua produção se dá de forma alheia às disposições da investigação preliminar. Informações produzidas em atividades de inteligência acostados em relatórios não se prestam à produção probatória, restando restritas a representação de '*notitia criminis* para que a polícia investigue fatos criminosos'" (Camargo, 2022, 95-96).

CTN) e pelo Coaf vinculado ao Banco Central do Brasil (art. 2º da Lei 13.974/2020). Daí que um olhar apressado ou pouco atento aos detalhes pode provocar a sensação de que as atividades de inteligência são bastante distintas entre si, ou até mesmo que têm em comum somente o nome. Além das agências estatais distintas realizando a atividade, a terceira geração parece destoar tanto no conteúdo (dados financeiros) quanto no objetivo (avaliação prévia de potenciais crimes financeiros e de lavagem de dinheiro). Sequer parece haver um conflito subjacente na atividade de inteligência financeira ou, quando muito, parece ter-se mera oposição ao pagamento de tributos.

Os elementos unificadores das atividades, todavia, são exatamente os mesmos que definem a atividade de inteligência: a atuação preventiva a um evento potencialmente perigoso e a elaboração de informações para subsidiar a tomada de uma decisão preditiva. A inteligência financeira não é alheia à lógica conflituosa, pois está assentada no objetivo declarado de combate à lavagem de dinheiro e ao financiamento do terrorismo. A lógica militarizada das inteligências de defesa e de segurança pública é adaptada para a Fazenda Pública e o Coaf, resultando na implementação de táticas de vigilância em massa e ampla coleta de dados a pretexto de prevenir os crimes tributários e a lavagem de dinheiro.

A generalização da suspeita de envolvimento com sonegação tributária, lavagem de dinheiro e terrorismo é a mais gravosa entre todas as consequências estabelecidas na legislação de inteligência. As duas principais normativas são a Lei 9.613/1996 e o Convênio ICMS 134/2016 do Confaz. A Lei 9.613/1996 criou uma lista de pessoas obrigadas a colaborar (art. 9º) e estabeleceu deveres de (a) registro de clientes e operações (art. 10) e (b) comunicação de operações financeiras suspeitas (art. 11). O Convênio 134/2016 obrigou as instituições financeiras e intermediárias a comunicar transações com cartões de crédito, débito, de loja e quaisquer transações eletrônicas a fim de apurar eventual sonegação de ICMS[25].

Em suma, a terceira geração de inteligência é caracterizada por (a) terceirizar as atividades de inteligência dos órgãos estatais para particulares e (b) atribuir funções preliminares de apuração a agências que têm o dever de comunicar suspeitas de crimes à polícia e ao Ministério Público (MP), mas não integram o sistema penal.

Consta no *site* do Coaf que a inteligência financeira é executada em três etapas: (a) recepção de comunicações, (b) análise de informações e (c) disseminação de RIF (Brasil, 2021). A etapa de análise é fundamental, pois é nesse momento que os analistas de inteligência financeira produzem as informações e avaliam a necessidade de compartilhamento. Constatada a possível prática de crime, a Fazenda Pública e o Coaf agem de modos distintos.

25. O STF declarou a constitucionalidade do convênio no julgamento da ADI 7.276.

A Fazenda Pública elabora uma RFPP (art. 83 da Lei 9.430/1996), composta apenas por dados fiscais do contribuinte cruzados com dados de outros contribuintes, e compartilhada mediante ofício. O Coaf elabora um RIF, composto por dados fiscais e não fiscais obtidos das comunicações de operações suspeitas por qualquer das pessoas obrigadas acerca de transações suspeitas e de pessoas relacionadas (art. 9º da Lei 9.613/1996), e compartilhado diretamente no Sistema Eletrônico de Intercâmbio de Informações (SEI) do Coaf.

Os analistas do Coaf recebem as comunicações das operações financeiras, alimentam uma matriz de risco que estabelece níveis automaticamente a partir da soma dos pontos atribuídos aos fatores das operações financeiras (forma de movimentação, pessoas envolvidas, regiões geográficas, investigações em curso etc.). Se o cálculo de risco atingir a pontuação mínima, é registrado um processo eletrônico e distribuído para um terceiro analista elaborar o RIF (Brasil, 2022), podendo consultar bases de dados do Siscoaf, da Rede Infoseg, do Cadastro de Pessoas Físicas (CPF), do Cadastro Nacional de Pessoas Jurídicas (CNPJ), da Declaração de Operações Imobiliárias (DOI), do Sistema Integrado de Administração de Recursos Humanos (Siape), do Sistema de Informações Rurais (SIR), do Cadastro Nacional de Informações Sociais (CNIS), do Cadastro nacional de Empresas (CNE), da Análise de Informações de Comércio Exterior (Alice *Web*), da Base de Grandes Devedores de União, das Bases do TSE e da Declaração de Porte de Valores (e-DPV) (Brasil, 2020).

Como se pode notar, os dados inseridos em um RIF são muito mais abrangentes do que os dados de uma RFPP, pois incluem dados fiscais, dados bancários, operações imobiliárias, seguros, ações, registros públicos em geral, registros de profissionais liberais e outros. Tais dados nunca dizem respeito exclusivamente ao titular da operação suspeita, pois as operações comunicadas e inseridas nos RIFs sempre envolvem várias pessoas. As comunicações de transações bancárias suspeitas, por exemplo, sempre envolvem as seguintes categorias de pessoas: (a) titulares de contas, (b) beneficiários das transferências, (c) remetentes e (d) diretores ou gerentes de pessoas jurídicas.

Percebe-se que os serviços de inteligência financeira intervêm, de maneira incontornável, em direitos de terceiros, caracterizando um tipo de devassa equivalente ao cumprimento de mandados de busca coletivos.

4. Compartilhamento de dados financeiros no processo penal

O alcance da intervenção das atividades de inteligência é melhor compreendido com a análise do seu ciclo. Embora a atividade de inteligência do Coaf seja apresentada oficialmente em apenas três etapas (recepção, análise e disseminação), o

ciclo completo da inteligência é um complexo e formado por dez etapas[26]: (a) requerimento de informações, (b) planejamento, (c) gerenciamento dos meios de coleta de dados, (d) coleta dos dados, (e) processamento, (f) análise, (g) produção de informações (relatórios, informes ou estudos), (h) disseminação das informações, (i) uso das informações e (j) avaliação das informações (Cepik, 2023, p. 65).

Este ciclo abrange as quatro etapas do processamento de dados pessoais (obtenção, armazenamento, utilização e transferência) que pressupõem normas autorizativas por caracterizarem intervenções em direitos fundamentais distintos[27].

A necessidade de autorização legal específica para cada etapa do processamento de dados se justifica especialmente pela matéria e grau de intervenção das informações produzidas pelos serviços de inteligência nos direitos de personalidade. A inteligência financeira é especialmente delicada, pois é produzida a partir de dados a respeito da intimidade, privacidade, autodeterminação informativa, proteção de dados e sigilos bancário, fiscal, de comunicações telefônicas e de dados. Daí que a justificação da intervenção nesses direitos deve se dar nos estritos limites da autorização constitucional de para que não configure indevida violação[28].

Embora a Constituição brasileira não contenha uma expressa proibição de violação à essência de direitos fundamentais, como ocorre na Constituição alemã[29], tal proibição pode ser deduzida da localização topográfica da dignidade humana no rol de fundamentos da República Federativa do Brasil (art. 1º, III). Entendida como conteúdo implícito da dignidade humana, sem manipular o texto constitucional, pode-se conceber essa proibição como núcleo dos direitos fundamentais[30]

---

26. Percebe-se que as explicações constantes no *site* do Coaf agrupam as etapas para simplificar a explicação.
27. "Se o indivíduo tem de ser protegido de condutas estatais como a *obtenção*, o *armazenamento*, a *utilização* e a *transferência* de dados, as quais têm de encontrar limites, isso significa que essas quatro fases do processamento de informações são intervenções e, principalmente, que elas são intervenções de natureza autônoma: uma norma que autoriza a obtenção de um dado não autoriza já automaticamente a utilização ou o armazenamento, muito menos a transferência. Necessita-se de uma norma para cada uma das quatro fases" (Greco, 2018, p. 44 – grifos nossos).
28. "Intervenção é o que carece de justificação. Uma intervenção não-justificada é o que se chama de *lesão* ou *violação* (*Verletzung*) a direito fundamental. E há uma categoria especial de direitos fundamentais, a daqueles em que as intervenções são impassíveis de qualquer justificação, em que são *intocáveis* (*unantastbar*)" (Greco, 2018, p. 32 – grifos nossos).
29. Como é o caso da Alemanha (2022, p. 27): "Art. 19(2). Em nenhum caso, um direito fundamental poderá ser violado em sua essência".
30. Apesar da opacidade e do racismo da filosofia moderna (*vide* Andrade, 2017), a concepção kantiana de dignidade tinha a humanidade como seu conteúdo e fim em si mesmo, o que implica que não poderia ser convertida em mero instrumento para atingir fins:

e atribuir-lhe a mesma consequência jurídica: considerar intocável o conteúdo de dignidade de qualquer direito fundamental, tal como ocorre na Alemanha (*vide* Greco, 2018, p. 34-35).

Desse modo, considera-se violação qualquer atividade de inteligência que (a) intervenha em direito fundamental sem autorização constitucional (o art. 5º, X e XII, da CRFB considera invioláveis a intimidade, a privacidade, a honra, a imagem, o sigilo das correspondências, das comunicações telegráficas e dos dados, sem autorizar o estabelecimento de exceções legais) ou (b) exceda os limites da autorização constitucional, afetando a dignidade humana durante a intervenção (o art. 5º, XI, XII e LXXIX, da CRFB autoriza a criação de leis para excepcionar a inviolabilidade à casa, ao sigilo das comunicações telefônicas e à proteção de dados).

Merecem destaque os dois pontos mais sensíveis das atividades de inteligência, os quais ligam o tratamento de dados[31]: (a) o desencadeamento da atividade e (b) o compartilhamento das informações produzidas.

É certo que a etapa de coleta de dados fundamental pode ser considerada o centro da atividade de inteligência, mas não se pode ignorar que a coleta é sempre consequência de algo. Isto é, de uma suspeita que desencadeia a coleta, mas, por ser infundada, sequer chega a ser um ensejo[32]. Ou, melhor, uma suspeita fundada na

"No reino dos fins tudo tem ou um preço ou uma dignidade. Quando uma coisa tem um preço, pode-se pôr em vez dela qualquer outra como *equivalente*; mas quando uma coisa está acima de todo o preço, e portanto não permite equivalente, então tem ela dignidade. [...] aquilo [...] que constitui a condição só graças à qual qualquer outra coisa pode ser um fim em si mesma, não tem somente um valor relativo, isto é um prelo, mas um valor íntimo, isto é *dignidade*. A moralidade, e a humanidade enquanto capaz de moralidade, são as únicas coisas que têm dignidade" (Kant, 2008, p. 81 – grifos nossos).

31. Enquanto não é editada lei específica sobre o tratamento de dados para as atividades de inteligência e segurança pública (âmbito de incidência expressamente excluído da LGPD no art. 4º, III e § 1º), deve-se ter em conta os limites da autorização fixados com frequência nos regulamentos de proteção de dados: "de regra, regulamentos de proteção de dados definem as hipóteses em que tais dados podem ser legitimamente utilizados por terceiros e estabelecem mecanismos para proteger os titulares dos dados contra usos inadequados. A licitude do tratamento desse tipo de dado estará vinculada ao consentimento do interessado ou à outra base jurídica que o legitime, princípio estabelecido no Considerando 40 do RGPD, dentre os quais encontra-se o exercício de poderes públicos (Considerando 45 do RGPD), arrolado dentre as condições gerais para a licitude do tratamento (art. 6º RGPD)" (Camargo, 2022, p. 43-44).

32. "A atividade de inteligência dispensa, assim, um ensejo. Ela se move no chamado *estágio ou campo prévio* (Vorfeld), não apenas em relação a delitos, como também a perigos. O conceito fundamental, aqui, é Vorsorge [...] que se poderia traduzir por *precaução*" (Greco, 2018, p. 52 – grifos nossos).

mera possibilidade de ocorrência de uma infração penal que torna esse o momento mais sensível, pois as inviolabilidades podem ser respeitadas ou ignoradas[33]. Trata-se tanto das discussões acerca dos métodos adequados de obtenção[34] e preservação[35] de provas digitais quanto dos requisitos para que os dados sejam coletados[36].

Daí se seguem as etapas que resultam na elaboração do relatório de inteligência que pode ser disseminado se eventual infração penal for apurada. Nessa etapa, de disseminação, as informações produzidas são compartilhadas com outros órgãos públicos para que sejam utilizadas na tomada de decisões nas mais variadas matérias. A inteligência de segurança pública e a inteligência financeira fornecem informações para a polícia e o MP decidirem se haverá investigação e processo penal.

O compartilhamento está previsto no art. 83 da Lei 9.430/1996 (Fazenda Pública) e no art. 15 da Lei 9.613/1996 (Coaf). O requisito do compartilhamento, em ambos os casos, é a apuração da suspeita de uma infração penal. Os destinatários do compartilhamento são a polícia e o MP. Essas duas modalidades de compartilhamento de informações não se confundem com o compartilhamento de provas (art. 372 do CPC). São distintos os (a) objetos (informação ou prova), (b) requisitos (indícios de infração penal ou contraditório e identidade de partes[37]) e (c) destinatários (polícia e MP ou Juízos). Apesar de não se confundirem, não raro os relatórios compartilhados pelos serviços de inteligência financeira são posteriormente compartilhados como provas documentais de outros processos, engrossando o caldo da confusão dos institutos.

Em todo caso, a existência da etapa de compartilhamento é consequência da necessária separação das (a) atribuições e (b) informações disponíveis aos órgãos de inteligência e de persecução penal[38].

---

33. Vale destacar que a suspeita só é obtida depois da apuração preliminar efetuada pelo serviço de inteligência, como é o caso do RIF elaborado pelo Coaf após a conclusão da apuração: "O RIF *não supõe* um juízo de valor sobre a *legalidade* ou *ilegalidade* da operação. Apenas relata uma suspeita, um estranhamento, a partir do qual será *iniciada* uma investigação pela autoridade com *competência* para tal" (Bottini, 2021 – grifos nossos).
34. Tema de diversos trabalhos relevantes. Por todos: Mendes (2024); Saad Gimenes; Rossi; Partata (2024).
35. Sobre: Machado (2023).
36. P. ex., a participação ativa da defesa e paridade de armas na investigação, licitude dos elementos produzidos, *e-discovery*, coleta de elementos de informação pela defesa, e tratamento de dados pela defesa: Camargo (2022, p. 142-181).
37. A Corte Especial do STJ entende que a identidade de partes é desnecessária (EREsp 617.428, j. 04.06.2014), embora seja impossível exercer contraditório sem ser parte originalmente.
38. Daí a relevante separação do direito alemão: "O direito alemão parte de um *imperativo* ou *mandato de separação* (*Trennungsgebot*) entre direito processual penal, direito de polícia

Na etapa de compartilhamento, os âmbitos de incidência das normas de inteligência e de proteção de dados se justapõem, tornando a matéria extremamente complexa. Isso porque a etapa de compartilhamento pode mitigar ou até mesmo esvaziar a separação informacional. A mitigação ocorre nas hipóteses de estabelecimento de critérios demasiado genéricos, pouco rigorosos ou contraditórios que autorizam o compartilhamento facilitado das informações. O esvaziamento se dá quando a separação é meramente formal ou há meio para contornar a separação, especialmente na inteligência de segurança pública cujo compartilhamento de informações pode ser feito facilmente mediante a oitiva dos policiais ou a juntada dos arquivos com relatórios aos autos do processo como se provas documentais fossem (Carnelutti, 2004, p. 298), também comumente aproveitando-se das disposições do art. 479 do CPP, do art. 52, parágrafo único, I, da Lei 11.343/2006 ou do art. 23, parágrafo único, da Lei 12.850/2013.

A jurisprudência acerca do compartilhamento das informações produzidas em inteligência foi desenvolvida de modo variável, dependendo das agências públicas envolvidas e do seu contexto de atuação. A ABIN enfrentou restrições mais severas na sua atuação, enquanto entendimento sobre a inteligência financeira foi marcado por oscilações e divergências entre as Turmas do STF e do STJ.

No julgamento da ADI 6.529, oposta contra a determinação legal de compartilhamento de ofício com a Abin de todos os dados obtidos pelos órgãos componentes do Sisbin (art. 4º, parágrafo único, da Lei 9.883/1999), o STF aplicou a técnica da interpretação conforme a Constituição para estabelecer quatro condições de constitucionalidade do compartilhamento: (a) comprovação de interesse público para o fornecimento dos dados, (b) obrigatoriedade de motivação do ato administrativo de solicitação dos dados de inteligência aos órgãos do Sisbin para apreciada da legalidade pelo Judiciário, (c) dados sujeitos à reserva de jurisdição, como comunicações telefônicas, não podem ser compartilhados sem autorização judicial e (d) imprescindibilidade de procedimento formalmente instaurado, sistemas eletrônicos de segurança e registro para fornecer os dados à Abin. Na apreciação da medida cautelar, o Min. Edson Fachin consignou expressamente sua preocupação com o compartilhamento de dados que "ativa inúmeras sensibilidades democráticas, incluindo o risco de construção de mecanismos típicos de um Estado policialesco" (Brasil, 2020, voto do Min. Edson Fachin, p. 7).

e de inteligência. [...] O imperativo se dirige, em primeira linha, ao objeto de cada um desses setores [...], e tem implicações relativas às faculdades interventivas previstas em cada um deles [...], ademais implicações organizacionais e informacionais" (Greco, 2018, p. 51 – grifos nossos).

A jurisprudência acerca da inteligência financeira teve um caminho mais longo e substancialmente distinto. Isso se deve, em parte, ao tratamento vacilante do afastamento dos sigilos fiscal e bancário, inicialmente como inerente à reserva de jurisdição e agora sem necessidade de autorização judicial[39].

A RFPP foi questionada perante o STF em três ocasiões e perante o STJ em outra.

Primeira, a arguição de inconstitucionalidade do art. 6º da LC 105/2001 que autoriza agentes da Fazenda Pública Municipal, Estadual, Distrital ou Federal a examinar documentação dos contribuintes diretamente nas instituições financeiras, sem autorização judicial, desde que exista procedimento administrativo instaurado. No julgamento do Tema 225[40], o STF considerou que a medida simplesmente repassa o dever de sigilo bancário das instituições financeiras ao fisco, sem violar o sigilo.

Segunda, a arguição de inconstitucionalidade da autorização legal para que a Receita Federal e a UIF compartilhassem com o MP, sem autorização judicial, os dados bancários e fiscais legitimamente obtidos no exercício do dever de fiscalização. Ao julgar o Tema 990[41], ratificou a autorização legal, condicionando-a a existência de um meio de comunicações formais para garantir o sigilo, certificar o destinatário e estabelecer instrumentos de apuração de eventuais desvios. O entendimento firmado pelo STF partiu do pressuposto de que a incidência do sigilo bancário no RIF seria reduzida por não conter movimentações globais dos correntistas, ensejando um tratamento "com menos rigor a proteção do sigilo bancário, comparativamente ao fiscal" (Oliver; Mendes Jr; Luz, 2024). Em consequência, esvaziou a eficácia vertical do direito aos sigilos bancário e fiscal. Afinal, independente do menor detalhamento em relação ao afastamento de sigilo bancário, "não se pode ignorar que há informações sensíveis que ali são incluídas" (Mascarenhas; Vasconcellos, 2025).

Terceira, a constitucionalidade da própria RFPP (art. 83 da Lei 9.430/1996, com a redação da Lei 12.350/2010) foi questionada na ADI 4.980 com alegação de violações aos arts. 3º; 62, *caput* e § 1º, I, "b"; 150, II; 194, *caput;* 195 da CRFB. No julgamento, o STF entendeu que (a) a disposição não é matéria de direito penal ou

39. "embora a Constituição Federal não tenha indicado reserva de jurisdição para essa finalidade, demandando, especificamente, autorização judicial apenas para os casos de expedição de mandados de prisão, de mandados de busca e apreensão e interceptação telefônica [...], o Poder Judiciário, por vezes, já estendeu a exigência de autorização judicial também para acesso aos dados bancários e fiscais, tendo, entretanto, atualmente, se posicionado no sentido de que isso não seria necessário" (Testoni, 2023).

40. RE 601.314, j. 24.02.2016.

41. RE 1.055.941, j. 28.11.2019.

processo penal, a exigência de exaurimento do processo administrativo fiscal privilegia os princípios da ordem constitucional, mantendo o direito penal como *ultima ratio* e (c) a extensão do tratamento dos crimes tributários à apropriação indébita previdenciária e à sonegação tributária maximiza a isonomia tributária.

Quarta, a atuação da Receita Federal do Brasil na apuração de possível sonegação tributária foi questionada perante o STJ. A 5ª Turma reconheceu que o fisco deve observar dois limites nos procedimentos apuratórios: (a) atuação estritamente associada à relação jurídica tributária ou aduaneira e (b) atividade de apuração exclusivamente de ilícitos tributários. Os elementos produzidos foram declarados ilícitos em decorrência dos desvios da pertinência temática tributário-aduaneira e da finalidade fiscal do procedimento[42].

Diferentemente da jurisprudência acerca da RFPP que foi consolidada sem ensejar grandes divergências, os entendimentos acerca do RIF parecem estar muito distantes de uma definição. A ratificação da autorização legal para compartilhamento dos RIFs no julgamento do Tema 990 não tratou de um ponto fundamental: a motivação da passagem do tratamento dos dados para o compartilhamento. O art. 15 da Lei 9.613/1996 trata expressamente do compartilhamento de ofício pelo Coaf se constatada a existência de lavagem de dinheiro. O art. 17-B da Lei 9.613/1996 delimita os dados aos quais terão acesso a autoridade policial e o MP. Nenhuma das disposições legais autoriza que dados sejam requeridos ou requisitados ao Coaf[43].

Essa ausência de autorização legal motivou a instauração de uma duradoura controvérsia entre as Turmas do STF e do STJ acerca da (in)admissibilidade do compartilhamento de RIF também a requerimento ou requisição.

No STF, as duas turmas divergem acerca dos limites do entendimento firmado pelo Pleno no Tema 990.

Por um lado, a 2ª Turma do STF passou a entender que o RIF só pode ser produzido e compartilhado de ofício. Primeiro, foi rechaçada a produção de RIF a pedido e a execução de diligências do Coaf em instituições bancárias[44]. Em seguida, declarou ilícita a iniciativa do MP de requisitar diretamente ao Coaf dados bancários ou fiscais de imputados[45].

42. AgRg no RHC 167.539, j. 12.12.2023.
43. Também nesse sentido: "Os dois diplomas legais que regulam a atividade do Coaf não parecem lhe impor um dever de compartilhar dados pessoais *a pedido de autoridades públicas*" (Estellita, 2021, p. 627).
44. HC 201.965, j. 30.11.2021.
45. RE 1.393.219 AgR, j. 11.07.2024.

Por outro lado, a 1ª Turma do STF, contudo, abriu divergência, entendendo que o julgamento do Tema 990 autorizou a elaboração de RIF de ofício ou mediante solicitação. Inicialmente, a Turma traçou uma indevida distinção entre requisição e solicitação para declarar a licitude de RIF solicitado, entendendo que a solicitação poderia não ser atendida pelo Coaf[46]. A seguir, condicionou a requisição de RIF ao Coaf à prévia instauração de procedimento investigatório com objetivo certo e fundado em elementos indiciários[47].

No contexto dessa divergência, o STJ firmou entendimentos diversos. Primeiramente, a 6ª Turma considerou lícito o acesso a movimentações obtido mediante autorização judicial, ainda que inexistentes movimentações atípicas, o que parece dissociado de qualquer fundamento legítimo para a formulação do pedido de autorização judicial[48]. Em seguida, a Terceira Seção concluiu que o Tema 990 autoriza apenas o compartilhamento de ofício, não sendo possível sua requisição direta[49]. Esse entendimento foi reafirmado em três julgamentos subsequentes[50].

Os acórdãos do RHC 147.707 e do AgRg no RHC 187.335 do STJ foram cassados pelo STF nos julgamentos da Rcl 61.944 e Rcl 70.191 do STF, respectivamente. Em razão disso, o STJ alterou a jurisprudência, passando a adotar o entendimento da 1ª Turma do STF. Seguindo esse entendimento, a 5ª Turma considerou ilícita a requisição do RIF por ausência de prévia instauração de procedimento investigatório formal[51].

Em reação à insegurança jurídica decorrente das oscilações de entendimento, o Conselho Federal da Ordem dos Advogados do Brasil ajuizou a ADI 7.624 para questionar a constitucionalidade do art. 15 da Lei 9.613/1998 à luz da intimidade, privacidade e sigilo e proteção de dados (art. 5º, X, XII e LXXIX, da CRFB), justificando que o Tema 990 foi julgado em 2019, antes da inserção do direito à proteção de dados pessoais no rol de direitos fundamentais.

A 3ª Seção do STJ julgou o REsp 2.150.571, na pendência de julgamento dos limites do Tema 990 pelo STF, concluindo pela necessidade de prévia autorização judicial para a requisição de RIF pela polícia e MP. Prevaleceu o voto do Min. Messod Azulay para quem o STF não abordou o tema do RIF por encomenda no julgamento do *leading case* do Tema 990.

---

46. Rcl 61.944 AgR, j. 02.04.2024.
47. Rcl 70.191 AgR, j. 12.11.2024.
48. RMS 42.120, j. 25.05.2021.
49. RHC 83.233, j. 09.02.2022.
50. RHC 147.707, j. 15.08.2023, *HC* 816.944, j. 23.10.2023 e AgRg no RHC 187.335, j. 18.06.2024.
51. ED no AgRg no RHC 188.838, j. 24.09.2024.

5. Lavagem de dados financeiros ilícitos no processo penal

O encontro com as novas tecnologias atualiza e torna a matéria mais sensível que as já complexas atividades de inteligência inseridas na persecução penal. A multiplicação exponencial dos aparelhos eletrônicos – e, de consequência, dos rastros nos sistemas informáticos –, e o potencial de vigilância em massa das companhias gigantes do setor de tecnologia culminam em uma persecução penal ilimitada. De um lado, os aparelhos eletrônicos são cada vez mais visados pelas agências de persecução penal. Do outro, sociedades empresárias ofertam informações produzidas pelos serviços de inteligência e até mesmo competem com as agências oficiais[52].

No ponto de encontro entre inteligência e informatização emergem as técnicas e os métodos de vigilância digital individual e em massa (Bachmaier Winter, 2025). Essas técnicas são tratadas de maneira distinta. Algumas das técnicas de vigilância digital são majoritariamente consideradas medidas ilícitas e abusivas, especialmente a espionagem e a pescaria probatória (*fishing expedition*[53]), pois a desvinculação de qualquer justificativa legal para a sua implementação caracteriza indevida estratégia militarizada[54]. Outras, contudo, são pontualmente declaradas ilícitas, como ocorreu com o uso de agentes da Abin em investigação criminal oficial da Polícia Federal na Operação Satiagraha[55], ou frequentemente consideradas

52. "A emergência e o crescimento vertiginoso das novas tecnologias de comunicação e informação (TIC's) possibilitou o surgimento de empresas privadas que ofertam informações sobre temas de segurança em escala global, competindo em muitas áreas com os próprios serviços de inteligência pela atenção e os recursos orçamentários dos governantes" (Cepik, 2023, p. 35).

53. "Pode-se invadir silenciosamente as bases de dados público-privadas e se 'pescar' os dados. Isso porque como a invasão acontece à sorrelfa, no que se pode chamar de *Deep Investigation*, depois de encontrado/pescado o dado apto a sustentar acusações, promove-se a sua aparente descoberta" (Ghizoni da Silva; Melo e Silva; Morais da Rosa, 2019, p. 82).

54. Declarada ilícita em decisão monocrática do Min. Gilmar Mendes no julgamento da Rcl 56.510.

55. "1. Uma análise detida dos 11 (onze) volumes que compõem o HC demonstra que existe uma grande quantidade de provas aptas a confirmar, cabalmente, a participação indevida, flagrantemente ilegal e abusiva, da ABIN e do investigador particular contratado pelo Delegado responsável pela chefia da Operação Satiagraha. 2. Não há se falar em compartilhamento de dados entre a ABIN e a Polícia Federal, haja vista que a hipótese dos autos não se enquadra nas exceções previstas na Lei 9.883/99. [...] 4. No caso em exame, é inquestionável o prejuízo acarretado pelas investigações realizadas em desconformidade com as normas legais, e não convalescem, sob qualquer ângulo que seja analisada a questão, porquanto é manifesta a nulidade das diligências perpetradas pelos agentes da ABIN e um ex-agente do SNI, ao arrepio da lei. [...] 6. Portanto, inexistem dúvidas de

medidas lícitas de obtenção (de fontes) de provas[56], tais como o *malware*[57] e as atividades de inteligência financeira.

O STF e o STJ frequentemente mencionam os riscos de pescaria probatória nos casos mencionados anteriormente, seja para vetar a requisição direta pela polícia e MP (posição da 2ª Turma do STF), seja para admitir a requisição desde que preexista a instauração formal de procedimento investigatório (posição da 1ª Turma do STF). Apesar disso, geralmente declaram lícito o uso de relatórios elaborados por serviços de inteligência financeira.

A preocupação com a pescaria probatória é tema recorrente na jurisprudência[58]. Entretanto, as atividades de inteligência não recebem a mesma atenção, apesar das semelhanças entre ambas. As atividades de inteligência são conduzidas ininterruptamente em busca de indícios de possíveis infrações penais a comunicar

---

que tais provas estão irremediavelmente maculadas, devendo ser consideradas ilícitas e inadmissíveis, circunstâncias que as tornam destituídas de qualquer eficácia jurídica, consoante entendimento já cristalizado pela doutrina pacífica e lastreado na torrencial jurisprudência dos nossos tribunais" HC 149.250, j. 07.06.2011.

56. Pode tratar-se de meios de prova ou de métodos de investigação de fontes de prova: "o *meio de prova* [ou *método de produção de determinada prova em espécie*] não deve ser confundido com a própria prova em espécie. A prova em espécie é a informação de valor probatório – ou *elemento probatório* – extraída da *fonte de prova* pelo *método de produção típico* ou *atípico*. [...] *métodos de investigação de fontes de prova* não se prestam à obtenção das provas encartadas no Artigo 155 do Código de Processo Penal, quais sejam as provas cautelares, irrepetíveis e antecipadas, ou ainda as denominadas doutrinariamente de provas pré-constituídas, mas tão somente a elementos informativos que formam o caderno de investigação preliminar. Neste sentido, permite-se concluir que tais elementos informativos não possuem valor probatório" (Mendes, 2024, p. 200-201 e 213 – grifos nossos).
57. "Tanto o recurso *hacking* como a utilização de *malware* nas investigações permitem ao centro de comando um posicionamento à distância do dispositivo alvo, um controle remoto capaz de realizar de maneira oculta o monitoramento em tempo real, do áudio, vídeo, das funções de microfone e câmeras, do fluxo de dados e comunicações, da memória e armazenamento, da geolocalização do dispositivo móvel alvo dentre outras funcionalidades por vezes disponíveis" (Mendes, 2020, p. 164). No Brasil, é indevidamente utilizado como agente infiltrado virtual do art. 10-A da Lei 12.850/2013, apesar da falta de autorização legal expressa.
58. Por exemplo: "A hipótese dos autos, consubstanciada em investigação iniciada para apurar a existência de milícias digitais atentatórias ao Estado Democrático de Direito e à independência das Instituições, não se confunde com a chamada pesca probatória, que somente se caracteriza quando se pretende investigar genericamente algumas pessoas e não fatos, de maneira especulativa, ou seja, obter qualquer dado aleatório, independentemente da investigação instaurada ou infração penal existente" (STF, Reconsideração de despacho na Pet 12.100, j. 26.03.2025).

para a polícia e o MP. A suspeita de possível infração penal recai indistintamente sobre todos. Do mesmo modo, a pescaria probatória visa obter a notícia-crime para desencadear a persecução penal. Essa semelhança, por si só, deve ter a mesma consequência jurídica: ilicitude probatória de todos os elementos produzidos sem fundada suspeita ou de fundadas razões (art. 5º, LVI, da CRFB e art. 157 do CPP).

Contudo, o entendimento majoritário é bastante distinto, inclusive nos Tribunais Superiores. A situação atinge o ápice da gravidade quando os serviços de inteligência passam a utilizar indevidamente estratégias ilegais de produção de dados para a pescaria probatória. Assim, atualiza-se a estratégia persecutória que adota as precitadas táticas de (a) antecipação da consumação dos crimes (criminalização autônoma dos atos preparatórios) e (b) antecipação da persecução penal (agenciamento da inteligência na persecução penal).

Oportuno observar que independente do momento em que surge a suspeita (antes ou depois de instaurado procedimento investigatório) e o órgão do qual parte (serviço de inteligência, polícia ou MP), a mera suspeita não satisfaz condições mínimas da persecução penal[59], pois não é (a) notícia-crime (art. 5º do CPP), (b) fundada suspeita (art. 240, § 2º, do CPP), (c) fundada razão (art. 240, § 1º, do CPP), (d) justa causa (art. 395, III, do CPC), (e) prova (art. 155 do CPP) e, muito menos, (f) prova suficiente para a condenação (arts. 283 e 386 do CPP). A atividade estatal que intervém em direito fundamental a partir de mera suspeita é desencadeada por possibilidade (p. ex., o mundo pode acabar a qualquer momento). Ou existem elementos informativos da suspeita ou não pode ser legítima a intervenção.

Além das conhecidas estratégias de vigilância em massa, podem ser, indevidamente, utilizadas táticas de *hacking* para obter dados mediante fraude contra os sujeitos indeterminados. Nesses casos, a pescaria probatória (*fishing expedition*) que visa obter a notícia-crime de fato indeterminado envolvendo alvo determinado, antes da existência de qualquer suspeita formalizada em procedimento investigatório, é convertida em pescaria falsa (*phishing*[60] *expedition*) mediante instrumentos tecnológicos para burlar a segurança, a intimidade, a privacidade e o sigilo e a proteção de dados de todos em busca de um alvo indeterminado. A principal diferença entre ambas é o alvo: a percaria probatória visa pessoas determinadas em busca de elementos de materialidade, a pescaria falsa visa qualquer pessoa que seja vítima do golpe a partir de quem pode ser possível obter elementos de materialidade e de autoria de quaisquer crimes.

59. Admitindo o compartilhamento quando há suspeita concomitante dos órgãos de inteligência e de persecução: Leite e Teixeira (2023).

60. Neologismo em inglês formado pela união das palavras pesca (*fishing*) + falso (*phony*).

Essas características podem ser encontradas em diversos escândalos de vigilância em massa ocorridos nos últimos anos. O caso mais preocupante envolve o *spyware* Pegasus do NSO Group. Esse programa, instalado remotamente em *smartphones* utilizando uma armadilha de *phishing*, permite monitorar os usuários, rastrear seu deslocamento e gravar imagens e conversas (Blau, 2022). O Brasil quase adquiriu o Pegasus em 2021 (Brasil, 2021), mas acabou comprando o *spyware* FirsMile da Cognyte. Esse programa foi amplamente usado pela Abin para vigiar a população e opositores políticos (Brasil, 2024). Aparentemente, as principais operadoras de telefonia do país estavam cientes da operação ilegal em curso (Serapião, 2024). Outro serviço violador de direitos fundamentais é a Plataforma Integrada de Operações e Monitoramento de Segurança Pública (Córtex) que unifica mais de 160 bases de dados. O Córtex coleta e trata dados pessoais sem parâmetros legais e sem transparência[61].

Os relatórios de informação produzidos pelos serviços de inteligência são amplamente admitidos na persecução penal, especialmente nos megaprocessos[62], limitam o direito de defesa[63] e dificultam a descoberta da lavagem de dados. Quiçá os processos tenham sido transformados em megaprocessos não só pela substituição de seu centro informativo pela delação premiada (Santoro, 2020), mas também pela amplitude da autorização para a juntada dos relatórios de serviços de inteligência

61. "Desde a Copa do Mundo de 2014, o Brasil vem ampliando a aquisição e uso de softwares de espionagem. As práticas de vigilância e investimentos em sistemas como o Córtex têm crescido desde Dilma e Temer. Foi no governo Bolsonaro que essas contratações se intensificaram e a estrutura de inteligência teria ficado mais opaca, com a ampliação do Sistema Brasileiro de Inteligência (Sisbin), que reúne diferentes órgãos que compartilham informações sensíveis entre si. Em paralelo a isso, o governo Bolsonaro ampliou os casos de dispensa de licitação e de decretação de sigilo para os contratos destes tipos de *software*" (Zanatta; Silva, 2024).

62. Sobre a ampliação do processo nas dimensões horizontal (quantidade de suspeitos), vertical (quantidade de imputações) e temporal (duração excessiva): Malan (2019).

63. Constatadas em estudo empírico realizado a partir de entrevistas com advogados e membros do MP: "mostrou-se que o grande volume probatório presente nos megaprocessos bem como a dificuldade de acesso a determinadas informações, torna praticamente impossível o conhecimento de todos os aspectos relacionados ao caso, representando um limite importante à defesa plena. Outro aspecto abordado diz respeito à quantidade de acusados neste modelo processual, o que dificultaria o trabalho da defesa no sentido de individualizar as condutas para então analisar a responsabilidade penal de seu cliente. A rapidez de alguns procedimentos também foi destacada pelos advogados, que trataram das dificuldades organizacionais e de análise quando da atuação em um processo complexo que se desenrola em um curto lapso temporal" (Prates; Bottino, 2019, p. 166-167).

como se provas documentais fossem. Esse entendimento ignora que os RIFs foram definidos como peças de informação no julgamento do Tema 990 (cf.: destaque de Nascimento, 2025).

A autorização para requisição direta de relatórios de inteligência pela polícia e pelo MP é uma modalidade de pescaria probatória ou, no mínimo, uma via privilegiada para a pescaria. O aproveitamento posterior dos relatórios como provas documentais oportuniza a lavagem de dados obtidos ilicitamente. O método é simples: basta inserir os dados nos relatórios para convertê-los em informações aptas a embasar a tomada de decisões. Essa operação, conhecida pelos profissionais de tecnologia como lavagem de dados (*data laudering*), transforma o sistema penal em lavanderia que tem a persecução penal como máquina de lavar.

As provas repetíveis, principalmente a delação premiada, são centrais para executar as operações de ocultação ou dissimulados de dados acessados ou produzidos ilicitamente com o propósito de atribuir aparência de licitude (lavagem de dados), conforme explicado em outro estudo (Cani, 2023). Aquela análise tratava da inteligência de segurança pública. Neste texto, a análise será complementada com quatro características específicas da inteligência financeira que também se utiliza de dados (financeiros) repetíveis[64].

Primeira, os sistemas informáticos em geral operam com mecanismos de tipos de usuários (administradores e não administradores), permissão dos usuários (visualizar ou editar) e controles de acesso dos usuários (permitido, restrito ou proibido). Assim, um mesmo usuário pode até ter permissão para criar e editar arquivos, mas pode não ter acesso a todos os arquivos, pastas ou sistemas. Nesse caso, determinados sistemas informáticos usados por agentes de inteligência financeira podem permitir acessos a arquivos que, inclusive, não deixam registros (*logs*) em condições preestabelecidas. É o que ocorre com o sistema DW-LEL da Receita Federal do Brasil, cujos auditores com senhas *master* podem efetuar consultas sigilosas a dados para monitorar alvos e posteriormente elaborar comunicações anônimas de infrações em geral[65].

Segunda, os dados podem ser obtidos ilicitamente mediante requisição – ou solicitação – direta, sem fundada suspeita. Depois, sua origem pode ser dissimulada em (a) pedido de autorização judicial para compartilhamento ou (b) compartilhamento de ofício por outro analista de inteligência.

64. "Os dados financeiros são estáticos e estão em poder de órgão público, sem a possibilidade de adulteração pelo investigado" (Mascarenhas; Vasconcellos, 2025).

65. Foi o caso da Ação Civil Pública 0103340-29.2016.4.02.5101, na qual a existência dos usuários master só foi descoberta mediante expedição de ofício ao SERPRO para fornecer cópia integral dos registros de acesso aos dossiês das pessoas envolvidas.

Terceira, antes da conclusão de qualquer apuração pode ser vazada para a polícia ou para o MP a (a) declaração de imposto, (b) comunicação de uso transação bancária para apuração de ICMS ou (c) comunicação da operação suspeita. A partir dos dados inseridos na declaração de imposto ou na comunicação, podem ser obtidos outros dados relevantes.

Quarta, dados recebidos ilicitamente mediante (a) monitoramento indevido, (b) obtenção de relatórios de inteligência fora das hipóteses autorizadas ou (c) vazamentos, podem ser cruzados com outros dados obtidos licitamente, tais como em operações de inteligência em fontes abertas (Osint) mediante consultas em redes sociais para instaurar procedimento investigatório ou juntar relatórios ao processo.

É imprescindível distinguir os dados obtidos em fontes abertas[66] daqueles amplamente fornecidos à polícia e ao MP por outros órgãos públicos e por empresas. O acesso a bancos de dados de acesso restrito viola a separação informacional[67], como alertado pela *Data Privacy* em relação ao Córtex[68]. Embora a inteligência financeira supostamente seja baseada na separação informacional[69], a observância estrita dessa separação só seria obtida se os sigilos bancários e fiscais fossem afastáveis exclusivamente mediante autorização judicial. De nada adianta separar as informações e as atribuições de persecução se o Coaf tem poder para compartilhar os dados de ofício, provocando a polícia e o MP, e se a polícia e o MP têm poderes para requisitar dados ao Coaf.

Daí a centralidade do tema para o direito processual penal contemporâneo.

6. Considerações finais

O compartilhamento de dados financeiros na persecução penal é um fenômeno intensificado pelas transformações jurídicas e tecnológicas, mormente a partir

66. A Osint tem âmbito de incidência bastante restrito: "Trata-se de inteligência baseada nas informações que estão disponíveis livremente a partir de fontes públicas, como jornais, revistas, críticas, rádio, telejornais, e, o que é mais comum nos dias atuais, em redes sociais e internet" (Camargo, 2022, p. 100).

67. "A vinculação à finalidade, conjugada à separação entre inteligência, polícia e justiça, significa também que é *inadmissível uma base de dados comum a todos os órgãos estatais*. [...] Se saber é poder, o Estado não pode saber tudo, porque um Estado que tem conhecimentos ilimitados tem também um poder ilimitado" (Greco, 2018, p. 45 – grifos nossos).

68. "Alertamos que a operação do Córtex seria incompatível com a ideia de separação informacional de poderes" (Zanatta; Silva, 2024).

69. "O órgão de inteligência poderá concluir pela existência de crimes, mas não poderá persegui-los; precisamente por isso – por nada poder, senão comunicar – é que o Coaf pode (quase tudo saber, sem prévia autorização judicial" (Leite; Teixeira, 2023).

do século XXI. Neste texto, analisou-se (a) o surgimento de um procedimento trifásico no qual a persecução penal é iniciada antes da existência da notícia-crime, (b) as transformações da inteligência culminantes no aparecimento da inteligência financeira, (c) os critérios legais e jurisprudenciais de compartilhamento dos relatórios de inteligência e (d) a potencial lavagem de dados ilícitos nas atividades de inteligência financeira.

No primeiro tópico, destacou-se a passagem do procedimento bifásico inspirado no processo penal francês de 1808 para o procedimento trifásico estabelecido a partir do acoplamento de atividades de inteligência como uma etapa prévia à investigação criminal, provocando uma alteração substancial na persecução penal e no sistema penal. As transformações jurídicas e tecnológicas se deram no século XXI, os seus principais fatores surgiram e se intensificaram a partir da década de 1980 nos EUA e na Itália. A influência no Brasil se deve à difusão por meio das Convenções de Viena (1988) e de Palermo (2000). As alterações penais e processuais penais resultaram numa atividade incessantemente preventiva por força da antecipação da consumação de alguns crimes e da antecipação da persecução penal desses mesmos crimes.

No segundo tópico, explicou-se o desenvolvimento das atividades de inteligência que culminaram na sua terceira fase: a inteligência financeira. A inteligência financeira é fruto do deslocamento do âmbito de aplicação da lógica militarizada: da segurança pública para os ambientes bancário, fiscal e de outros setores considerados de risco. A generalização da suspeita infundada, inerente à atividade de inteligência, é justificada a pretexto do possível envolvimento dos alvos com crimes tributários, lavagem de dinheiro, terrorismo e organizações criminosas.

No terceiro tópico, analisou-se os critérios legais e jurisprudenciais de compartilhamento dos relatórios de inteligência, especialmente financeira. Destacou-se o tratamento distinto para a inteligência de segurança pública e a inteligência financeira, bem como as divergências entre as Turmas do STF e seu efeito na alteração do entendimento da 5ª e da 6ª Turmas do STJ acerca da possibilidade de compartilhamento de RIF mediante requisição da polícia ou do MP.

No quarto tópico, explicitou-se os potenciais de lavagem de dados por meio de RIF e de RFPP, destacando a injustificada distinção entre inteligência financeira e *fishing expedition*, a possibilidade de produção de uma *fishing expedition* e as quatro principais distinções em relação às atividades de inteligência de segurança pública: (a) dados armazenados em sistemas de informação próprios, (b) autorização do STF para requisição direta, (c) potencial vazamento de dados antes da conclusão de procedimento apuratório e (d) possibilidade de cruzamento de dados pela polícia e pelo MP, sobretudo utilizando os dados centralizados no Córtex.

O compartilhamento de dados financeiros ainda gera diversos outros problemas que podem e devem ser objeto de outros estudos. Exemplifica-se: (a) falta de definição também dos limites de valoração dos relatórios de inteligência; (b) critérios e condições de rastreabilidade das fontes de dados inseridos nos relatórios de inteligência[70]; (c) estabelecimento de limitações efetivas ao tratamento dos dados pessoais em atividades de inteligência; (d) falta de mecanismos específicos de salvaguarda contra o abuso de técnicas e métodos de prova com potencial de espionagem, vigilância em massa e lavagem de dados; e (e) falta de limites ao atingimento de direitos de terceiros durante a persecução penal.

Referências

ALEMANHA. Parlamento. *Lei fundamental da República Federal da Alemanha*. Trad. Assis Mendonça. Berlim: Deutscher Bundestag, 2022.

ANDRADE, Erico. A opacidade do iluminismo: o racismo na filosofia moderna. *Kriterion*, v. 58, n. 137, p. 291-309, 2017. [https://doi.org/10.1590/0100-512X2017n13704ea].

ASSANGE, Julian. *Quando o Google encontrou o WikiLeaks*. Trad. Cristina Yamagami. São Paulo: Boitempo, 2015.

BACHMAIER WINTER, Lorena. A luta pelas garantias do devido processo e a mudança de paradigma na teoria da prova: do liberalismo à *mass surveillance* no processo penal europeu. Trad. Fernanda Vilares e Luiz Eduardo Cani. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, v. 11, n. 1, e1164, 2025. [https://doi.org/10.22197/rbdp.v11i1.1164].

BADARÓ, Gustavo Henrique; BOTTINI, Pierpaolo Cruz. *Lavagem de dinheiro*: aspectos penais e processuais penais. 4. ed. São Paulo: Ed. RT, 2019.

BLAU, Uri. Pegasus Spyware Maker NSO Is Conducting a Lobbying Campaign to Get Off U.S. Blacklist. *Pro Publica*, 12.07.2022. Disponível em: [www.propublica.org/article/pegasus-spyware-nso-israel-blacklist-lobbying]. Acesso em: 15.03.2025.

BOTTINI, Pierpaolo Cruz. Os limites da atuação do Coaf. *Consultor Jurídico*, São Paulo, 29.03.2021. Disponível em: [www.conjur.com.br/2021-mar-29/direito-defesa-limites-atuacao-coaf]. Acesso em: 30.03.2025.

BRASIL. CONSELHO DE CONTROLE DE ATIVIDADES FINANCEIRAS. *A produção de inteligência financeira*. Brasília: Coaf, [2021]. Disponível em: [www.gov.br/coaf/pt-br/acesso-a-informacao/Institucional/a-producao-de-inteligencia-financeira]. Acesso em: 15.03.2025.

70. Sobre a necessidade de rastreabilidade das fontes de prova: Mendes (2024, p. 343-348).

BRASIL. CONSELHO DE CONTROLE DE ATIVIDADES FINANCEIRAS. *Análise de informações*. Brasília: Coaf, [2022]. Disponível em: [www.gov.br/coaf/pt-br/acesso-a-informacao/Institucional/a-producao-de-inteligencia-financeira/analise-de-informacoes]. Acesso em: 15.03.2025.

BRASIL. MINISTÉRIO DA FAZENDA. *Prevenção à lavagem de dinheiro*. Inteligência financeira. Brasília: Coaf, [2020]. Disponível em: [www.gov.br/fazenda/pt-br/assuntos/prevencao-lavagem-dinheiro/inteligencia-financeira]. Acesso em: 15.03.2025.

BRASIL. PF deflagra Operação Vigilância Aproximada para investigar monitoramento indevido de cidadãos. *Polícia Federal*, 25.01.2024. Disponível em: [www.gov.br/pf/pt-br/assuntos/noticias/2024/01/pf-deflagra-operacao-vigilancia-aproximada-para-investigar-monitoramento-indevido-de-cidadaos]. Acesso em: 15.03.2025.

BRASIL. Senadores pedem que TCU apure compra de software espião pelo Ministério da Justiça. *Senado Federal*, 19.05.2021. Disponível em: [www12.senado.leg.br/noticias/materias/2021/05/19/senadores-pedem-ao-tcu-auditoria-sobre-compra-de-software-espiao-pelo-ministerio-da-justica]. Acesso em: 15.03.2025.

CAMARGO, Rodrigo Oliveira de. *Tratamento de dados, persecução penal e a garantia do direito de defesa*. 2022. 210 f. Tese (Doutorado em Ciências Criminais) – Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2022. Disponível em: [https://tede2.pucrs.br/tede2/handle/tede/10605]. Acesso em: 15.03.2025.

CANI, Luiz Eduardo. Impugnações à lavagem de dados no processo penal. *Boletim IBCCRIM*, v. 31, n. 370, p. 24-28, 2023. Disponível em: [https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/687]. Acesso em: 15.03.2025.

CARNELUTTI, Francesco. *Lições sobre o processo penal*. Trad. Francisco José Galvão Bruno. Campinas: Bookseller, 2004. v. 1.

CEPIK, Marco. *Espionagem e democracia*: agilidade e transparência como dilemas na institucionalização de serviços de inteligência. 2. ed. Belo Horizonte: Parabellum, 2023.

CORDERO, Franco. *Guida alla procedura penale*. Torino: Utet, 1986.

COUTINHO, Jacinto Nelson de Miranda. *A lide e o conteúdo do processo penal*. Curitiba: Juruá, 1989.

COUTINHO, Jacinto Nelson de Miranda. Introdução aos princípios gerais do processo penal brasileiro. *Revista da Faculdade de Direito UFPR*, Curitiba, v. 30, n. 30, p. 163-198, 1998. [https://doi.org/10.5380/rfdufpr.v30i0.1892].

COUTINHO, Jacinto Nelson de Miranda. O papel do novo juiz no processo penal. In: COUTINHO, Jacinto Nelson de Miranda (Coord.). *Crítica à teoria geral do direito processual penal*. Rio de Janeiro: Renovar, 2001. p. 3-55.

COUTINHO, Jacinto Nelson de Miranda. Sistema acusatório: cada parte no lugar constitucionalmente demarcado. In: COUTINHO, Jacinto Nelson de Miranda; CARVALHO, Luis Gustavo Grandinetti Castanho de (Org.). *O novo processo penal à luz da Constituição*: análise crítica do Projeto de Lei 156/2009, do Senado Federal. Rio de Janeiro: Lumen Juris, 2010. v. 1. p. 1-17.

ESMEIN, Adhémar. *Histoire de la procédure criminelle en France et spécialement de la procédure inquisitorie depuis le XIIIe siècle jusqu'a nos jours*. Paris: L. Larose et Forcel, 1882.

ESTADOS UNIDOS DA AMÉRICA. Congress. *Public law 91-508*. Washigton, D.C.: Presidência da República, 26.10.1970. Disponível em: [www.govinfo.gov/content/pkg/STATUTE-84/pdf/STATUTE-84-Pg1114-2.pdf.]. Acesso em: 11.03.2025.

ESTADOS UNIDOS DA AMÉRICA. Congress. *Public law 99-570*. Washigton, D.C.: Presidência da República, 27.10.1986. Disponível em: [www.govinfo.gov/content/pkg/STATUTE-100/pdf/STATUTE-100-Pg3207.pdf]. Acesso em: 11.03.2025.

ESTELLITA, Heloisa. O RE 1.055.941: um pretexto para explorar alguns limites à transmissão, distribuição, comunicação, transferência e difusão de dados pessoais pelo Coaf. *Revista Direito Público*, v. 18, n. 100, p. 606-636, 2021. [https://doi.org/10.11117/rdp.v18i100.5991].

GHIZONI DA SILVA, Viviani; MELO E SILVA, Philipe Benoni; MORAIS DA ROSA, Alexandre. *Fishing expedition e encontro fortuito na busca e na apreensão*: um dilema oculto do processo penal. Florianópolis: EMais, 2019.

GOLDSCHMIDT, James. *Problemas jurídicos y políticos del proceso penal*. Conferencias dadas en la Universidad de Madrid en los meses de diciembre de 1934 y de enero, febrero y marzo de 1935. Barcelona: Bosch, 1935.

GRECO, Luís. Introdução. In: WOLTER, Jürgen. *O inviolável e o intocável no direito processual penal*: reflexões sobre dignidade humana, proibições de prova, proteção de dados (e separação informacional de poderes) diante da persecução penal. Trad. Alaor Leite e Eduardo Viana. São Paulo: Marcial Pons, 2018. p. 21-82.

HARCOURT, Bernard. *Exposed*: desire and disobedience in the digital age. Cambridge: Harvard University Press, 2015.

HARCOURT, Bernard. *A contrarrevolução*: como o governo entrou em guerra contra os próprios cidadãos. Trad. Augusto Jobim do Amaral et al. São Paulo: GLAC, 2021.

HOMERO. *Ilíada*. Trad. Carlos Alberto Nunes. 5. ed. Rio de Janeiro: Ediouro, 1996.

IMAGENET. *Large Scale Visual Recognition Challenge 2012*. [S.l.]: Imagenet, 2012. Disponível em: [https://image-net.org/challenges/LSVRC/2012/index]. Acesso em: 15.03.2025.

KANT, Immanuel. *Fundamentação da metafísica dos costumes*. Trad. Paulo Quintela. Lisboa: 70, 2008.

LEITE, Alaor; TEIXEIRA, Adriano. Gestão do poder informacional no processo penal no RHC 147.707-STJ (parte 2). *Consultor Jurídico*, São Paulo, 15 set. 2023. Disponível em: [www.conjur.com.br/2023-set-15/leite-teixeira-gestao-poder-informacional-processo-penal-2]. Acesso em: 30.03.2025.

LOPES JR., Aury. *Direito processual penal*. 21. ed. São Paulo: Saraiva, 2024.

MACHADO, Vitor Paczek. *Exceção de inutilização*? Por um procedimento incidental de discussão da quebra da cadeia de custódia das provas. 2023. 407 f. Tese (Doutorado em Ciências Criminais) – Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2023.

MALAN, Diogo. Megaprocessos criminais e direito de defesa. *Revista Brasileira de Ciências Criminais*, v. 159, p. 45-67, 2019.

MARQUES, José Frederico. *Elementos de direito processual penal*. Campinas: Bookseller, 1997. v. 1.

MASCARENHAS, Gustavo; VASCONCELLOS, Vinícius. Os RIFs do Coaf e as consequências práticas do Tema 990: é necessário que o STF se pronuncie. *Consultor Jurídico*, São Paulo, 21.01.2025. Disponível em: [www.conjur.com.br/2025-jan-21/os-rifs-do-coaf-e-as-consequencias-praticas-do-tema-990-e-necessario-que-o-stf-se-pronuncie]. Acesso em: 15.03.2025.

MENDES, Carlos Hélder Carvalho Furtado. *Prova penal digital*: direito à não autoincriminação e contraditório na extração de dados armazenados em dispositivos informáticos. São Paulo: Tirant lo Blanch, 2024.

MENDES, Carlos Hélder Carvalho Furtado. *Tecnoinvestigação criminal*. Entre proteção de dados e a infiltração por *software*. Salvador: JusPodivm, 2020.

MORAIS DA ROSA, Alexandre; CANI, Luiz Eduardo. No processo penal combo, o exercício da ampla defesa é brinde. *Consultor Jurídico*, São Paulo, 03.02.2023. Disponível em: [www.conjur.com.br/2023-fev-03/limite-penal-processo-penal-combo-exercicio-ampla-defesa-brinde]. Acesso em: 11.03.2025.

NASCIMENTO, Thiago Cyndier Pereira do. E quanto ao RIF na "gaveta" da autoridade destinatária? *Consultor Jurídico*, São Paulo, 04.02.2025. Disponível em: [www.conjur.com.br/2025-fev-04/e-quanto-ao-rif-na-gaveta-da-autoridade-destinataria]. Acesso em: 30.03.2025.

OLIVER, Luiza; MENDES JR., Neuler; LUZ, Ilana Martins. Sigilo bancário e fiscal: dois pesos e duas medidas. *Consulto Jurídico*, São Paulo, 28.08.2024. Disponível em: [www.conjur.com.br/2024-ago-28/sigilo-bancario-e-fiscal-dois-pesos-e-duas-medidas]. Acesso em: 15.03.2025.

ORLANDI, Renzo. Investigações preparatórias nos procedimentos de criminalidade organizada: uma reedição da *inquisitio generalis*? Trad. Ricardo

Jacobsen Gloeckner e Luiz Eduardo Cani. In: TERRA, Luiza Borges (Org.). *Lições contemporâneas do direito penal e do processo penal*. São Paulo: Tirant lo Blanch, 2021. p. 371-391.

ORLANDI, Renzo. O procedimento penal por fatos de criminalidade organizada: do maxi-processo ao "grande processo". Trad. Luiz Eduardo Cani. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, v. 7, n. 3, p. 2105-2126, 2021. [https://doi.org/10.22197/rbdpp.v7i3.634].

PRATES, Fernanda; BOTTINO, Thiago. Megaprocessos e o exercício do direito de defesa: uma abordagem empírica. *Revista Brasileira de Ciências Criminais*, v. 27, n. 162, p. 145-170, 2019.

SAAD GIMENES, Marta; ROSSI, Helena; PARTATA, Pedro. A obtenção das provas digitais no processo penal demanda uma disciplina jurídica própria? Uma análise do conceito, das características e das peculiaridades das provas digitais. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, v. 10, n. 3, e1071, 2024. [https://doi.org/10.22197/rbdpp.v10i3.1071].

SANTORO, Antonio Eduardo Ramires. A imbricação entre maxiprocessos e colaboração premiada: o deslocamento do centro informativo para a fase investigatória na Operação Lava Jato. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, v. 6, n. 1, p. 81-116, 2020. [https://doi.org/10.22197/rbdpp.v6i1.333].

SERAPIÃO, Fábio. Tim, Vivo e Claro sabiam de ataques por software espião, mas não alertaram Anatel. *Folha de S. Paulo*, Brasília, 31.01.2024. Disponível em: [www1.folha.uol.com.br/poder/2024/01/tim-vivo-e-claro-sabiam-de-ataques-por-software-espiao-mas-nao-alertaram-anatel.shtml]. Acesso em: 15.03.2025.

TESTONI, Pablo Naves. RIFs por requisição no Coaf e os problemas dogmáticos do passado. *Consultor Jurídico*, São Paulo, 20.11.2023. Disponível em: [www.conjur.com.br/2023-nov-20/lavagem-afins-rifs-por-requisicao-no-coaf-e-os-problemas-dogmaticos-do-passado]. Acesso em: 15.03.2025.

VERNANT, Jean-Pierre. *As origens de pensamento grego*. Trad. Ísis Borges B. da Fonseca. São Paulo: Difel, 1992.

ZANATTA, Rafael A. F.; SILVA, Vinicius. Por que precisamos rever o uso do Córtex no Brasil? *Data Privacy Research*, São Paulo, 19.12.2024. Disponível em: [www.dataprivacybr.org/por-que-precisamos-rever-o-uso-do-cortex-no-brasil]. Acesso em: 30.03.2025.

Legislação

BRASIL. *Decreto 154, de 26 de junho de 1991*. Promulga a Convenção Contra o Tráfico Ilícito de Entorpecentes e Substâncias Psicotrópicas. Brasília: Presidência da República, 1991. Disponível em: [www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0154.htm]. Acesso em: 11.03.2025.

BRASIL. *Decreto 5.015, de 12 de março de 2004*. Promulga a Convenção das Nações Unidas contra o Crime Organizado Transnacional. Brasília: Presidência da República, 2004. Disponível em: [www.planalto.gov.br/ccivil_03/_Ato2004-2006/2004/Decreto/D5015.htm]. Acesso em: 11.03.2025.

Jurisprudência

BRASIL. Supremo Tribunal Federal, Pleno, ADI 6.529 / DF – Distrito Federal, rel. Min. Cármen Lúcia, j. 13.08.2020. Disponível em: [https://jurisprudencia.stf.jus.br/pages/search/sjur454781/false]. Acesso em: 15.03.2025.

Autor convidado

PESQUISA DO EDITORIAL

Área do Direito: Processual; Penal

Veja também Doutrina relacionada ao tema

- O relatório de inteligência financeira como meio de obtenção de prova no processo penal, de Ademar Borges – *RBCCrim* 176/69-105;
- *Open banking*: impasse entre a privacidade de dados e a revolução tecnológica?, de Alessandra Pela Sabbag e Lucas de Oliveira Noleto – *RDTec* 3; e
- Regulamentação da lei que disciplina a formação e consulta dos bancos de dados com informações de adimplemento e formação de histórico de crédito comentários ao Dec. 7.829/2012, de Bruno Miragem – *RDC* 84/317-333.

Veja também Jurisprudência relacionada ao tema

- STF, RE 1.055.941, j. 04.12.2019, *DJe* 18.03.2021; e
- TRF-4.ª Reg., RSE 5008658-43.2024.4.04.7208, j. 03.12.2024, *DJFe* 04.12.2024.

Faces make cases: o caso *Clearview AI* e os desafios do uso de tecnologias algorítmicas no sistema de justiça criminal brasileiro

"Faces make cases": the Clearview AI case and the challenges of using algorithmic technologies in the Brazilian criminal justice system

Thallita Gabriele Lopes Lima[1]
Pontifícia Universidade Católica do Rio de Janeiro, PUC-Rio, Brasil.
thallita.gabriele@gmail.com

DOI: [doi.org/10.5281/zenodo.17058344].

Área do Direito: Penal; Digital

Resumo: O uso de tecnologias de reconhecimento facial (TRFs) no campo da segurança pública tem suscitado importantes debates sobre os limites entre uso de tecnologias algorítmicas, legalidade e proteção de direitos fundamentais. Este artigo examina o caso da *Clearview AI* – empresa norte-americana que desenvolveu um sistema de TRF baseado na raspagem massiva de imagens extraídas da *internet* – como ponto de partida para refletir sobre os modos de circulação,

Abstract: Facial recognition technologies (FRT) in public security have sparked important debates about the boundaries between using algorithmic technologies, legality, and protecting fundamental rights. This article examines the case of *Clearview AI* – a US company that developed an FRT system based on the massive scraping of images extracted from the internet–as a starting point for reflecting on the circulation, appropriation, and contestation modes of these technologies in

1. Doutora em Relações Internacionais pela Pontifícia Universidade Católica do Rio de Janeiro, possui mestrado pela mesma instituição e graduação em Relações Internacionais pela Universidade Federal Rural do Rio de Janeiro. Coordenadora de pesquisa do projeto O Panóptico do Centro de Estudos de Segurança e Cidadania (CESeC).
Currículo Lattes: [http://lattes.cnpq.br/4467147688792014].
ORCID: [https://orcid.org/0000-0003-3488-349X].
E-mail: thallita.gabriele@gmail.com

apropriação e contestação dessas tecnologias em regimes jurídicos assimétricos. Interroga-se como esse modelo de coleta e uso de dados desafia garantias processuais e tensiona princípios constitucionais como a legalidade da prova, o contraditório e a proteção de dados pessoais. A análise articula o caso *Clearview* às dinâmicas brasileiras de implementação de TRFs, marcadas por informalidade institucional, fragmentação normativa e seletividade penal estrutural. Metodologicamente, combina-se revisão crítica da literatura, análise documental (registros obtidos via LAI, normativas e materiais institucionais) e observação em eventos setoriais. A partir de uma abordagem ancorada nos Estudos de Ciência e Tecnologia (STS) e na criminologia crítica, argumenta-se que infraestruturas sociotécnicas emergentes estão reconfigurando práticas de policiamento e racionalidades probatórias, com impactos diretos na produção da verdade judicial e na distribuição desigual de incertezas e vulnerabilidades no sistema de justiça criminal.

Palavras-chave: Reconhecimento facial – Dados pessoais – *Clearview AI* – Tecnologias de vigilância – Justiça criminal.

asymmetric legal regimes. It examines how this data collection and use model challenges procedural guarantees and undermines constitutional principles such as the legality of evidence, adversarial proceedings, and the protection of personal data. The analysis links the *Clearview* case to the Brazilian dynamics of implementing FRTs, marked by institutional informality, normative fragmentation, and structural criminal selectivity. Methodologically, it combines a critical review of the literature, documentary analysis (records obtained via the Access to Information Act, regulations, and institutional materials), and observation of sectoral events. Based on an approach anchored in Science and Technology Studies (STS) and critical criminology, it is argued that emerging sociotechnical infrastructures are reconfiguring policing practices and evidentiary rationalities, with direct impacts on the production of judicial truth and the unequal distribution of uncertainties and vulnerabilities in the criminal justice system.

Keywords: Facial recognition – Personal data – Clearview AI – Surveillance technologies – Criminal justice.

Sumário: 1. Introdução. 2. Da raspagem ao reconhecimento: descompactando a *Clearview AI* como infraestrutura algorítmica de vigilância. 3. Expansão, controvérsias e ambiguidades regulatórias: localizando o Brasil na circulação de TRF. 4. Entre rostos e rastros: *Clearview AI* e os limites do devido processo legal no Brasil. 5. Conclusão. Referências. Legislação.

1. Introdução

O[2] avanço das tecnologias de inteligência artificial (IA) de algoritmos de aprendizado de máquina tem gerado transformações nos regimes contemporâneos de segurança pública e da justiça criminal. Ancoradas em promessas de maior previsibilidade, agilidade e objetividade, essas tecnologias vêm sendo incorporadas por

2. A frase *Faces make cases*, em destaque no título deste trabalho, foi utilizada na estratégia de *marketing* da empresa no painel da ISC Brasil 2022 e está presente nas apresentações realizadas ao Ministério da Justiça e Segurança Pública pela Secretaria Nacional de Segurança Pública adquiridas via Lei de Acesso à Informação. Processo 08198.023803/2022-21.

diferentes setores do Estado sob justificativas da modernização institucional, ganho de eficiência e do enfrentamento à criminalidade. Sua aplicação envolve desde sistemas preditivos e bases de dados interoperáveis até sensores biométricos e *softwares* de reconhecimento facial. Pelo menos 75 dos 176 países em todo o mundo utilizam ativamente tecnologias algorítmicas para fins de segurança e vigilância (Feldstein, 2019).

Nesse mesmo cenário, nos últimos anos, a implementação de tecnologias de reconhecimento facial (TRFs) para fins de segurança tem sido apresentada no discurso público como uma promessa e uma oportunidade para otimizar a gestão da segurança (Ferguson, 2017). Essas tecnologias são frequentemente descritas como ferramentas fundamentais para aumentar a eficiência das investigações criminais e fortalecer a segurança pública. As TRFs podem identificar e autenticar as identidades das pessoas detectando, capturando e combinando rostos com imagens de um banco de dados, e são compreendidas como uma "solução" à necessidade crescente de identificação contemporânea (Lyon, 2008, p. 500). Sob a lógica tecnopolítica algorítmica, TRF prometem identificar suspeitos, correlacionar informações de maneira precisa, objetiva e rápida (Lyon, 2008).

Segundo Bichoff (2021), 70% das forças policiais do mundo têm acesso a algum tipo de TRF, e 60% dos países já a utilizam em aeroportos. Essas tecnologias têm sido empregadas em operações de policiamento para identificar suspeitos ou localizar pessoas desaparecidas, além de servirem como ferramentas para verificação de identidade, investigação, categorização e análise estatística (Lyon, 2008). No entanto, o funcionamento dessas tecnologias levanta questões críticas e debates na sociedade civil, envolvendo falhas operacionais e técnicas (Lima, 2024), falta de transparência e ausência de *accountability* (Lima et al., 2024, p. 10), os impactos sob os direitos fundamentais (Nunes; Lima; Cruz, 2023) – em especial, o direito à privacidade, à proteção de dados pessoais e às garantias processuais –, bem como a forma como essas tecnologias podem reforçar padrões discriminatórios e dinâmicas de violência marcadas por raça, classe, nacionalidade e gênero (Amoore, 2020; Buolamwini; Gebru, 2018).

Apesar das críticas e controvérsias, as TRFs têm sido promovidas por um discurso de inovação tecnológica no combate ao crime. Essas ferramentas operam com base em dados biométricos, algoritmos e grandes volumes de imagens, muitas vezes coletadas em plataformas públicas, sem consentimento dos titulares dos dados. Entre essas tecnologias, a *Clearview AI* se destaca como um caso paradigmático, tanto pela radicalidade de seu método de coleta (raspagem de dados públicos da *internet*) quanto pelas controvérsias éticas, jurídicas e políticas que sua atuação vem gerando em diferentes países. Nesse sentido, este artigo examina o caso da utilização do *software* da empresa norte-americana *Clearview AI*, que se enquadra em

uma tendência global de aumento na demanda pela reutilização de dados coletados pelo setor privado para fins de segurança (Ferguson, 2017), por vezes, de modo a permitir que governos contornem salvaguardas legais em torno do acesso da aplicação da lei ao comércio de bases de dados (Brayne, 2017; Brayne; Christin, 2021; Crawford, 2021).

Fundada em 2017 nos Estados Unidos, a *Clearview AI* desenvolveu uma TRF baseada em um banco de dados que ultrapassa 50 bilhões de imagens, extraídas de redes sociais, *sites* de notícias, *blogs*, portais governamentais e outras fontes públicas[3]. Sem firmar acordos com as plataformas e sem solicitar autorização dos usuários. Assim, bastaria uma imagem – captada por câmeras de segurança, celulares ou redes sociais – para que o algoritmo cruzasse com seu repositório e devolvesse uma lista de rostos semelhantes, associando a eles nomes, perfis em redes e outras informações pessoais.

A atuação do algoritmo da *Clearview AI* expõe, de maneira aguda, os limites da regulação contemporânea diante da circulação global de dados biométricos, os riscos da centralização privada de tecnologias sensíveis e os desafios que essas ferramentas impõem aos fundamentos do processo penal, especialmente no que diz respeito à legalidade da prova, à proteção de dados sensíveis e à preservação das garantias fundamentais do contraditório e da ampla defesa. Portanto, partimos, das seguintes perguntas: como o modelo de raspagem de dados e uso da *Clearview AI* por órgãos públicos desafia e flexibiliza garantias processuais e direitos fundamentais no campo penal? Que riscos institucionais e políticos estão em jogo quando tais tecnologias operam em contextos marcados por seletividade penal, desigualdade estrutural e baixa capacidade regulatória?

A fim de explorar criticamente os dilemas levantados, o artigo se estrutura em três eixos analíticos interdependentes. A primeira seção examina o funcionamento técnico e o repertório discursivo da *Clearview AI*, com foco em seu modelo de negócios, na construção de uma suposta neutralidade algorítmica, ancorada em uma disputa técnica e na promessa de eficiência investigativa. Na segunda seção, o foco recai sobre o contexto brasileiro e sua inserção na expansão global das TRFs, evidenciando como a ausência de um marco regulatório específico, aliada à fragmentação das políticas de segurança pública, favorece a experimentação institucional desregulada dessas tecnologias. Mostra-se como a difusão descentralizada das TRFs contribui para consolidar um contexto de plasticidade de implantação, flexibilização dos direitos fundamentais e pouca transparência e responsabilização enquanto política pública.

3. CLEARVIEW AI. *Plataforma de reconhecimento facial para segurança pública e investigações*. Disponível em: [www.clearview.ai/]. Acesso em: 30.05.2025.

A terceira seção investiga a trajetória da *Clearview AI* no Brasil, reconstruindo os caminhos formais e informais de sua inserção nos órgãos de segurança e justiça. Essa dimensão da análise tem como ponto nodal a forma como essas tecnologias circulam e se legitimam no campo da segurança pública brasileira, a partir de um emaranhado entre agentes policiais, operadores do direito, fornecedores privados e estruturas administrativas. Com base na análise dos contratos, reuniões técnicas e testes não supervisionados, argumenta-se que a circulação dessa tecnologia cria desafios significativos e condições de possibilidade que comprometem garantias fundamentais, afetando diretamente o regime de produção de prova, especialmente no que diz respeito à cadeia de custódia digital, à opacidade do funcionamento algorítmico e à reconfiguração da figura do suspeito no processo penal.

O artigo se baseia em análise documental e bibliográfica, examinando relatórios públicos, registros obtidos via Lei de Acesso à Informação (LAI), documentos institucionais da *Clearview AI*, materiais jornalísticos e normativos. Foram também analisadas transcrições de entrevistas públicas concedidas por representantes da empresa em veículos de mídia e conferências abertas, acessadas por meio de fontes institucionais e plataformas digitais. A pesquisa também contou com duas participações em feiras de tecnologias de segurança no Brasil nas quais a empresa norte-americana foi expositora: a ISC Brasil 2022[4] e a LAAD Defense & Security 2023[5].

A abordagem teórica adotada é crítica e interdisciplinar, ancorada nos Estudos de Ciência e Tecnologia (STS, na sigla em inglês) e na criminologia crítica. Combinando aportes de diferentes campos e autoras/es, buscamos evidenciar como a materialidade técnica das TRFs contribui para a construção de verdades criminais, a consolidação de formas específicas de policiamento, e os efeitos que isso pode produzir em termos violências, distribuição desigual de insegurança e flexibilização de direitos fundamentais. Cabe pontuar que não é o objetivo deste trabalho se concentrar em realizar uma análise jurídica, mas sim, alinhando-se aos estudos da STS e compondo com a crítica feminista a tecnociência, explorar as implicações nas

4. A ISC Brasil é a edição brasileira da marca ISC Security Events – International Security Conference & Exhibitions. A feira foi realizada entre 21 de setembro de 2022 e 23 de setembro de 2022 no Expo Center Norte, em São Paulo. Disponível em: [www.iscbrasil.com.br/pt-br/o-evento.html]. Acesso em: 14.03.2025.
5. A LAAD Defense & Security (Feira Internacional de Defesa e Segurança), aconteceu entre os dias 11 e 14 de abril de 2023 no Rio de Janeiro. Essa é considerada a maior e mais importante feira de defesa e segurança da América Latina e reúne fabricantes e fornecedores de armas e tecnologias para as Forças Armadas, Polícias, Forças Especiais; militares das Forças Armadas, forças policiais e autoridades governamentais, além de expositores diversos. Disponível em: [www.laadexpo.com.br/]. Acesso em: 11.03.2025.

matérias discursivas[6] do modo algorítmico de produção de verdade e sua admissibilidade no aparato de justiça criminal.

2. Da raspagem ao reconhecimento: descompactando a *Clearview AI* como infraestrutura algorítmica de vigilância

A *Clearview AI* é uma empresa norte-americana fundada em 2017 por Ton-That e Richard Schwartz,[7] com apoio financeiro de investidores como Peter Thiel (também investidor da Meta e dono da empresa de tecnologia de segurança Palantir) e do fundo de investimento Kirenaga Partners. A empresa atua no ecossistema de TRFs algorítmicas, que vêm se tornando tanto ignição para práticas operacionais dos agentes de segurança (de policiais a militares) quando suporte para a produção de evidências no contexto do processo probatório penal (Lima, 2024, p. 55). As TRFs não apenas impulsionam práticas policiais, mas também reconfiguram os fundamentos da justiça criminal, ao desestabilizarem os limites entre vigilância, identificação e produção de prova, frequentemente à revelia de garantias constitucionais como o devido processo legal, o direito à privacidade e à proteção de dados pessoais.

A promessa de construção de "um mundo mais seguro a partir do uso de IA"[8], é apresentada pela *Clearview AI* em seu *site* e em suas redes sociais. Logo na primeira página de seu *site* oficial, a empresa afirma que sua missão é "simples e impactante": reduzir drasticamente o crime e tornar as comunidades mais seguras. Essa promessa, no entanto, está longe de ser simples como se apresenta, e oferecer uma ferramenta única capaz de torná-la possível é, no mínimo atraente. Como temos observado neste trabalho, o uso de tecnologias tem sido mobilizado por um discurso que as apresenta como soluções eficientes diante da incerteza que caracteriza problemas persistentes de segurança.

A empresa norte-americana ganhou notoriedade pública em janeiro de 2020, quando o *New York Times* publicou a reportagem intitulada "The Secretive

6. Conforme proposto por Karen Barad (2007), o termo material-discursivo expressa a inseparabilidade entre matéria e significação, indicando que os fenômenos não são dados previamente, mas emergem por meio de intra-ações entre elementos humanos e não humanos. Em sua perspectiva ontoepistemológica, práticas discursivas não apenas interpretam o mundo, mas o produzem materialmente, de modo que o social e o técnico, o jurídico e o algorítmico, não podem ser analisados separadamente.
7. Assessor de Rudolph W. Giuliani quando ele foi prefeito de Nova York.
8. CLEARVIEW AI. *Plataforma de reconhecimento facial para segurança pública e investigações*. Disponível em: [www.clearview.ai/]. Acesso em: 30.05.2025.

Company That Might End Privacy as We Know It" (A empresa secreta que pode acabar com a privacidade como a conhecemos) (Hill, 2020). Até então, a *Clearview* operava deliberadamente de forma discreta, oferecendo a sua TRF a agências de segurança pública e empresas privadas em diversos países, sem grande exposição midiática ou escrutínio público. A matéria lançou luz não apenas sobre a empresa, mas sobre o seu modelo de negócios: um sistema baseado não só em um algoritmo de correspondência facial, mas na raspagem massiva de imagens de fontes públicas e na oferta do serviço diretamente a instituições policiais e de segurança. Àquela altura, mais de 600 agências policiais nos Estados Unidos já utilizavam a ferramenta – número que, segundo documentos, poderia ultrapassar 2.900 organizações, incluindo o FBI, o Serviço Secreto, a Interpol, a agência de imigração dos EUA e corporações de segurança privada (Haskins; Mac; McDonald, 2020).

O rápido crescimento e a penetração institucional da *Clearview* não passaram despercebidos: apenas dezoito meses após a publicação da matéria investigativa, a empresa foi listada pela revista *Time* como uma das "100 empresas mais influentes do mundo" (*Clearview AI* named [...], 2021), apresentando-se como detentora da "maior rede de biometria facial do planeta" (Hill, 2020). A capacidade de raspar, capturar e indexar rostos públicos em escala global, aliada à oferta direta a autoridades de segurança, transformou a *Clearview* em um caso emblemático das novas formas de vigilância privada com implicações públicas – um modelo que opera nas fronteiras entre o legal e o extralegal, entre o visível e o opaco, entre a inovação e a erosão de direitos fundamentais.

A ferramenta da *Clearview AI* se diferencia de outras TRFs por dois elementos fundamentais: (i) o método de construção de seu banco de dados; e (ii) e a capacidade de seu algoritmo. O algoritmo da *Clearview* pode escanear mais de um bilhão de rostos em menos de um segundo[9], e a empresa afirma que a ferramenta é precisa "todas as demográficas"[10], ancorando essa alegação em uma patente que sua capacidade de criar algoritmos de reconhecimento facial precisos e "sem viés", a partir de informações publicamente disponíveis[11]. Em seu *site* oficial e no material distribuído na Laad 2023, no Rio de Janeiro, a empresa enfatiza um discurso de superioridade técnica, apresentando seu algoritmo como: "sem preconceitos", "assertivo", "preciso", "fidedigno" e "uma solução única e abrangente para inteligência e investigações, disponível no mercado mundial".

9. Apresentação da última versão do *Clearview* 2.0 ao Copaq/Senasp, via Lei de Acesso Informação.
10. Disponível: [www.clearview.ai/]. Acesso em: 15.03.2025.
11. Disponível em: [www.clearview.ai/patentes]. Acesso em: 15.06.2024.

O discurso da empresa busca neutralizar críticas recorrentes dirigidas às TRFs no contexto da segurança pública, especialmente no que se refere à baixa acurácia e aos vieses algorítmicos. Questões relacionadas a vieses demográficos, raciais e de gênero têm sido amplamente destacadas em propostas de moratórias e proibições do uso dessas tecnologias, geralmente associadas a preocupações com a proteção de direitos fundamentais, como o direito à privacidade (Lima, 2024, p. 62). A empresa, por sua vez, tenta reforçar a confiabilidade, precisão e alegada neutralidade de seu algoritmo, ao mesmo tempo em que enfrenta críticas relacionadas ao banco de dados que sustenta sua operação. No conjunto de documentos analisados nesta pesquisa, os algoritmos da *Clearview AI* são descritos como mais objetivos e eficientes do que o julgamento discricionário humano. A "alta eficiência" em problemas complexos e variados tem tornado a *Clearview* atraente, mas isso não implica que a ferramenta esteja livre de erros e vieses operacionais (Lima, 2024, p. 22).

Embora os recursos do seu algoritmo sejam descritos como "diferente de qualquer coisa já produzida" – uma afirmação respaldada por patentes –, o que de fato diferencia a empresa é o seu método de treinamento e coleta de imagens faciais. Ao invés de operar com bases de dados estatais, como registros criminais, arquivos de identidade civil ou cadastros governamentais, *Clearview* desenvolveu um algoritmo capaz de rastrear e indexar bilhões de imagens disponíveis na internet pública. Essa técnica, conhecida como raspagem de dados (*data scraping*), consiste na extração automatizada de conteúdo, como imagens, nomes e metadados, diretamente de redes sociais, *sites* jornalísticos e outras fontes digitais.

Dessa forma, quer tenhamos consentido ou não, nossos rostos aparecem nas fotos que, em muitos casos, acabam se tornando dados de treinamento e integrado a base de dados da empresa. É importante destacar que muitos de nossos dados estão publicamente disponíveis gratuitamente para serem utilizados quando os postamos *online*, sem as salvaguardas típicas encontradas em infraestruturas físicas. Isso torna profundamente difícil até mesmo discernir quem está usando e para quais finalidades. Esse é o principal diferencial da *Clearview*, e o fator de maior controvérsia. Essa prática tem provocado reações contundentes de defensores dos direitos humanos, pesquisadores e órgãos reguladores de proteção de dados (McSorley, 2021; Rezende, 2021). Tanto a forma de processamento dessas imagens quanto a comercialização da ferramenta têm sido duramente questionadas, sobretudo por comprometerem a privacidade dos indivíduos retratados e por impactarem diretamente as plataformas digitais de onde essas imagens são extraídas.

Em uma audiência de prospecção da empresa junto ao Ministério da Justiça e Segurança Pública (MJSP) do Brasil realizada no dia 09 de fevereiro de 2022 pela Copaq – uma comissão composta por representantes de cada uma das unidades e setores da Secretaria Nacional de Segurança Pública (Senasp) –, da qual tivemos

acesso por meio da Lei de Acesso à Informação[12], o representante comercial da empresa reafirma que "o grande objetivo" da *Clearview AI* é ampliar continuamente sua base de dados. Segundo Lima (2024, p. 85), o que o algoritmo de *Clearview* é capaz de fazer – e sua eficácia – depende diretamente do tamanho e da diversidade da sua base de dados, não apenas para gerar resultados mais específicos nas buscas realizadas por agentes de segurança, mas também para alimentar e refinar o próprio modelo algorítmico.

Por isso, a comparação da tecnologia da *Clearview AI* com o Google é recorrente. Das quinze entrevistas publicamente disponíveis em vídeo ou em áudio utilizadas nesta pesquisa, em seis delas o *CEO* Ton-That explica a sua tecnologia como uma ferramenta de busca, como a Google, mas voltada para rostos, destinada às forças de segurança. A analogia com um dos buscadores de *internet* mais populares do mundo não acontece aleatoriamente. Trata-se de uma estratégia de apresentar a ferramenta da empresa como poderosa e "disruptiva" (como reforçado no material de *marketing*) e, ao mesmo tempo, fácil de compreender utilizar e aparentemente alinhada à legislação vigente, que não enfrenta grandes críticas quanto à metodologia de extração de dados públicos da *internet* indexadas pela Google.

Apesar da tecnologia da *Clearview* ser protegida por sigilo corporativo e seu método estar atualmente resguardado por patentes – enquanto propriedade intelectual –, é importante destacar como os dados públicos, o acesso livre à informação, são centrais tanto para a formação do seu banco de dados quanto para a circulação de conhecimento técnico que possibilitou o desenvolvimento de seu algoritmo e suas inovações no campo do reconhecimento facial. Segundo Thylstrup (2019), a reutilização de dados públicos está profundamente interligada à forma como os algoritmos são recalibrados, reempacotados e reaproveitados. No caso da *Clearview AI*, a análise de seu desenvolvimento técnico permite identificar a incorporação de recursos originalmente disponíveis em *softwares* livres como parte da base metodológica de seu sistema proprietário. Isso evidencia como tecnologias tidas como inovadoras frequentemente se constroem a partir de camadas de conhecimento

12. Essa comissão foi criada em 2019 para instituir parcerias entre empresas ou instituições públicas e privadas com o objetivo de inovações, soluções tecnológicas e boas práticas, para a promoção e fomentação da modernização e reaparelhamento dos órgãos de segurança pública. As reuniões do Copaq do Ministério da Justiça é um meio de apresentação da empresa a diversos órgãos, isso porque a audiência de apresentação é aberta a todos os órgãos que tenham interesse. Contudo, o teste, o modo e a aquisição dos contratos não precisam ser intermediados pelo governo federal. Ou seja, a aquisição ocorre de forma autônoma em cada agência, sem nenhuma forma de padronização e regulação (BRASIL. Ministério da Justiça e Segurança Pública. Processo 08198.023803/2022-21. *Pedido de acesso à informação com base na Lei 12.527, de 18 de novembro de 2011*. Brasília, 2022).

aberto, cuja origem é posteriormente encoberta por patentes e estratégias comerciais[13]. A linguagem das patentes, como argumenta Katz (2020, p. 14), reforça uma reivindicação de conhecimento, produz uma métrica de inovação "e deixa a porta aberta a uma cascata de novas utilizações". Atualmente, a empresa possui três patentes.

Essa retórica de inovação técnica é acompanhada por esforços legais e institucionais de legitimação. O banco da *Clearview* ultrapassa 50 bilhões de imagens e, segundo declarações de seus representantes, a empresa pretende atingir a marca de 100 bilhões em poucos anos (Lima, 2024). Embora o volume, por si só, já seja expressivo, o que torna essa base especialmente controversa é o fato de incluir imagens de pessoas que jamais tiveram qualquer interação com o sistema de justiça – ou mesmo conhecimento de que suas fotos estavam sendo utilizadas em contextos de investigação criminal.

Essa transformação do rosto público em dado policial produz uma ambiguidade fundamental: se, por um lado, as imagens foram disponibilizadas voluntariamente pelos usuários em redes sociais, por outro, a recontextualização dessas imagens em um algoritmo biométrico destinado à segurança pública altera completamente sua finalidade e seus efeitos. Essa transição – do rosto ao dado, do dado à identidade, da identidade à prova – é central para entender como tecnologias como a *Clearview* reconfiguram as fronteiras entre o que é considerado informação pública, evidência penal e material de vigilância.

Os dados biométricos capturados e organizados por sistemas como o da *Clearview* não são meramente coletados: eles são produzidos, performados e transformados por uma série de decisões sociotécnicas. Barad (2007) argumenta que fenômenos científicos e tecnológicos não existem de forma autônoma, mas emergem por meio de intra-ações – relações dinâmicas entre sujeitos, objetos, instituições e dispositivos. O dado não é neutro: carrega consigo a marca do contexto em que foi produzido, extraído e reclassificado. O rosto capturado de uma *selfie*, de um vídeo de protesto ou de uma rede social passa a ser mobilizado em outro campo de significado – o da vigilância e da investigação penal – e adquire, nesse processo, um novo estatuto jurídico e político.

Essa reclassificação, além de técnica, é profundamente epistêmica. Como aponta Seaver (2017), os algoritmos são entidades moldáveis, que respondem a incentivos institucionais, culturais e comerciais. O algoritmo da empresa não opera isoladamente, mas está imerso em uma cadeia de significações que vai desde o

13. Para uma análise mais detalhada sobre o processo de desenvolvimento técnico da *Clearview AI* e sua articulação com *softwares* livres, ver Lima (2024).

design do *software* até os contextos institucionais em que seus resultados são interpretados. O sistema responde à demanda por "eficiência" policial, à pressão por inovações rápidas no setor de segurança e à lógica comercial da vigilância como serviço. Sua autoridade é construída pela fusão entre promessa técnica, infraestrutura privada e delegação institucional.

Nesse sentido, o banco de dados da *Clearview AI* não é apenas um repositório: trata-se também de um aparato de inscrição algorítmica de identidades e reconhecimento, capaz de gerar pistas investigativas a alimentar decisões judiciais. Como demonstrado em diversos estudos (Amoore, 2020; Aradau; Blake, 2021; Lima, 2024; Nunes; Lima; Cruz, 2023), as TRFs operam como um filtro técnico de suspeição, reorganizando as relações entre aparência, identidade e culpabilidade. O risco de erro – amplamente documentado para mulheres, pessoas trans e negras (Buolamwini; Gebru, 2018) – é frequentemente naturalizado por discursos que exaltam a eficiência do algoritmo e minimizam os efeitos políticos e sociais de sua adoção.

As controvérsias em torno da *Clearview AI* emergem justamente da desnaturalização dessa cadeia de produção algorítmica. Embora, a empresa esteja enfrentando um escrutínio cada vez maior, em especial com relação a políticas de segurança dos dados e a privacidade, também há um crescente apoio às políticas de compartilhamento de informações pessoais em nome da segurança. Em fevereiro de 2020, a estratégia da empresa passou a focar seus investimentos nos mercados dos Estados Unidos e no Canadá, mas seguiu promovendo sua ferramenta globalmente por meio de oferta de testes gratuitos para agentes de segurança de diversos países europeus e do "Sul Global", em especial América Latina, com participação ativa em conferências policiais e feiras de segurança (Mac; Haskins; Pequeno, 2021). Nos Estados Unidos, a empresa registrou uma ampliação dos picos de utilização e requerimento de testes após o seu *software* ter sido uma ferramenta "essencial" para o reconhecimento dos invasores do Capitólio no dia 06 de janeiro de 2021 (Hill, 2021).

Como observado, dos debates públicos sobre a *Clearview AI* frequentemente reproduz a dicotomia entre privacidade e segurança, como se estivesse em jogo um suposto equilíbrio entre garantir direitos individuais e promover proteção coletiva, uma tensão que tem marcado os debates públicos convencionais sobre tecnologias de vigilância (Bauman et al., 2015). Contudo, é fundamental refletir sobre os limites dessa oposição simplificadora e insuficiente para compreender as implicações reais dessas tecnologias. Em primeiro lugar, porque sugere que a privacidade seria um obstáculo à segurança, quando, na verdade, são justamente os limites jurídicos e políticos ao uso arbitrário de dados que garantem formas legítimas de proteção coletiva. Em segundo lugar, porque essa dicotomia oculta as camadas sociotécnicas e institucionais que estruturam a produção, a circulação e o uso desses dados.

No caso da *Clearview*, os rostos são extraídos de imagens postadas voluntariamente em redes sociais, convertidos em dados biométricos sem consentimento e reorganizados em um sistema de busca policial, um processo que altera profundamente sua natureza, função e efeitos. O que está em jogo, portanto, não é apenas uma disputa entre dois valores abstratos (privacidade *versus* segurança), mas a constituição de uma nova ecologia sociotécnica na qual a coleta, o processamento e o uso dos dados escapam aos marcos tradicionais de regulação e controle.

Em 2020, a União Americana pelas Liberdades Civis (sigla em inglês, ACLU) processou a *Clearview* por violar a Lei de Privacidade de Informações Biométricas (Bipa), de Illinois, uma lei estadual que proíbe a captura de identificadores biométricos de indivíduos, como rosto e impressões digitais, sem aviso prévio e consentimento. Em decorrência desse processo, a empresa foi impedida de vender a ferramenta a empresas privadas (*Clearview AI* Settles [...], 2022). Ademais, os órgãos reguladores de diversos países europeus baniram o uso da ferramenta sob a avaliação de que a Lei Geral de Proteção de Dados europeu (GDPR) (Ramage, 2022) exige consentimento explícito para o processamento de dados pessoais sensíveis (Rezende, 2020). Além disso, a Austrália e o Reino Unido acusaram a empresa de violar suas leis de privacidade e proteção de dados, e o Escritório do Comissário de Privacidade do Canadá segue investigando as atividades da empresa no Canadá (McSorley, 2021).

Apesar dessas ações, a circulação da ferramenta não foi interrompida. Alguns especialistas em privacidade descrevessem que o acordo entre a ACLU e a *Clearview AI* como um "divisor de águas" para avanço da proteção de dados e privacidade, e o banimento em países europeus como um "fechar de portas". No entanto, esses litígios não estancaram nem paralisaram a circulação e uso da tecnologia, que continuou a se expandir e ser remodelada em novos contextos, como na guerra da Ucrânia, onde foi empregada para identificação de corpos e reconhecimento em zonas de conflito (Lima, 2024).

É justamente nesse contexto que o sistema da *Clearview* deixa de ser apenas uma ferramenta técnica e se configura um ator político, com efeitos concretos sobre as práticas de segurança e direitos fundamentais. Ao fornecer resultados que vinculam rostos a perfis, redes e identidades, o algoritmo participa da construção de suspeitas, fundamenta decisões investigativas e pode influenciar a formação da prova. A opacidade do funcionamento do sistema, com códigos proprietários, segredos comerciais e ausência de auditoria externa, dificulta o exercício do contraditório, da ampla defesa e da contestação técnica.

Segundo Press (2023), uma questão importante é que o uso de TRFs tem levado os profissionais de segurança a desconsiderarem outros elementos relevantes dos casos. O resultado gerado pelo algoritmo tem sido representado uma evidência

contundente, adquirindo o status de "verdade técnica" (Amoore, 2020), o que por sua vez, dificulta a contestação. A evidência algorítmica passa a operar como um filtro de validação, estreitando o campo do contraditório corroendo os fundamentos do direito de defesa e do devido processo legal. Quando o julgamento da culpa se ancora na racionalidade algorítmica probabilística e em um emaranhado de diferentes práticas difusas dos operadores dessas ferramentas, a autoridade deriva não de sua transparência ou objetividade técnica, mas sim da legitimidade institucional e da credibilidade que o sistema ao ser incorporado aos circuitos policiais e judiciais.

Ao reduzir a distância entre o que é captado no cotidiano digital e o que é considerado elemento de ignição para ações penais, o uso de tecnologias como a *Clearview AI* representa uma mudança profunda na arquitetura da justiça criminal. Sua atuação desafia os limites entre o público e o privado, entre o dado e o direito, entre a imagem e a imputação penal. Mais do que uma tecnologia emergente, a *Clearview* encarna uma nova gramática da vigilância, na qual ver, reconhecer e rastrear se tornam operações contínuas, automatizadas e privatizadas.

3. Expansão, controvérsias e ambiguidades regulatórias: localizando o Brasil na circulação de TRF

Se na seção anterior observamos como sistemas como o da *Clearview AI* tensionam os limites entre o público e o privado, o legal e o extralegal. É no contexto brasileiro que essas tensões assumem contornos ainda mais complexos e opacos. Aqui, a circulação e normalização das TRFs operam por meio de mecanismos institucionais que mesclam inovação tecnológica, improvisação normativa, fragmentação burocrática-administrativa e opacidade operacional. Esse quebra-cabeça constitui um campo fértil para que tecnologias de segurança sejam experimentadas, testadas e, em alguns casos, utilizadas informalmente por agentes públicos – sem contratos formais, sem controle social e à margem dos marcos legais de contratação e transparência.

A ausência de uma política nacional sobre o uso dessas tecnologias, somada à falta de transparência na sua implementação e aos labirintos burocráticos que dificultam o acesso à informação, tem contribuído para a consolidação de um ecossistema no qual diferentes entes federativos adotam soluções tecnológicas com lógicas, fornecedores e critérios próprios. Movidos por uma agenda de modernização policial e por promessas de eficiência na identificação de suspeitos, governos estaduais e municipais passaram a investir em projetos-piloto, contratos diretos com empresas de tecnologia e parcerias informais com fornecedores privados. Nesse ambiente, projetos de TRFs s são implementados, testados e difundidos com

agilidade, ao passo que os marcos legais e institucionais que deveriam lhes dar sustentação permanecem ausentes ou em disputa.

Ao analisar como o Brasil se insere na circulação transnacional de TRF, esta seção examina os processos de institucionalização informal, os riscos da vigilância automatizada e os efeitos jurídicos, políticos e sociais da ausência de regulação específica, com especial atenção aos impactos sobre os direitos fundamentais e ao descompasso entre a promessa tecnológica e as garantias processuais. Trata-se, portanto, de compreender como o país tem construído aderência a essas tecnologias e de que maneira isso tem contribuído para a reconfiguração dos regimes de segurança pública.

No Brasil, todos os estados já utilizam ou estão em fase de testes de TRFs. Observa-se um aumento expressivo nos investimentos direcionados ao uso de tecnologias algorítmicas para segurança e vigilância, com destaque para essas ferramentas biométricas. Esse movimento tem seu início nos anos 2010 com os grandes eventos (como as Olimpíadas, Copa do Mundo e a Jornada Mundial da Juventude) (Lima et al., 2024). Apesar de uma certa desmobilização dos projetos após os eventos, tornou-se especialmente popular em 2019 (Nunes; Lima; Cruz, 2023, p. 8). Esse novo ciclo de adesão teve como catalizador a Portaria 793, de 24 outubro de 2019, que regulamenta a aplicação de recursos do Fundo Nacional de Segurança Pública para fomentar a implantação desses sistemas. Segundo a normativa, esses sistemas enquadram-se no conjunto de medidas para redução e controle da violência e da criminalidade. Esse incentivo, contudo, não foi acompanhado da criação de instâncias de controle, de mecanismos de avaliação de impactos ou de canais de participação social.

Essa expansão se dá em meio a um cenário de insegurança pública e violência, pressão por respostas rápidas por parte de gestores e crescente influência do "tecnosolucionismo" (Morozov, 2013) – a crença de que problemas complexos como a criminalidade podem ser resolvidos por meio de inovações tecnológicas. O discurso político em torno dessas ferramentas tende a enfatizar sua capacidade de otimizar o policiamento, reduzir custos operacionais e ampliar a eficiência das ações de segurança.

A ausência de normas unificadas e regulamentação sobre o uso de TRFs propiciou à proliferação de sistemas distintos em operação nos entes federativos, com objetivos, fornecedores e métodos variados. Na prática, observa-se a expansão e dispersão de projetos em todo o país sem a regulamentação adequada, padronização tecnológica ou adoção de mecanismos de publicidade, transparência e avaliação do uso dessas tecnologias como política pública. Além disso, o tratamento de dados para a segurança pública por meio do TRFs é realizado sem salvaguardas mínimas diante dos riscos associados à tecnologia, a despeito da emenda à

Constituição da República, que incluiu a proteção de dados como direito fundamental autônomo[14], dos princípios da administração[15] e da regulação infraconstitucional aplicável[16].

Segundo dados do projeto Panóptico, do Centro de Estudos de Segurança e Cidadania (CESeC), existem 442 projetos que utilizam TRF em espaços públicos, e aproximadamente 82,3 milhões de brasileiros estão potencialmente sob vigilância por câmeras com essa tecnologia[17]. A implementação dessa tecnologia tem avançado sem que haja garantias mínimas de proteção dos direitos fundamentais, tornando os espaços públicos, festas culturais e ambientes esportivos verdadeiros laboratórios de experimentação e coleta massiva de dados biométricos, incluindo crianças e adolescentes (Sousa et al., 2024).

A difusão dos projetos de segurança pública gera preocupações quanto a um possível cenário de desresponsabilização institucional, decorrente da adoção fragmentada dessas tecnologias sem a existência de diretrizes ou regulamentações mínimas. Cabe a cada ente federativo decidir autonomamente sobre a tecnologia a ser utilizada, os *softwares* empregados, as empresas contratadas, os bancos de dados acessados, os critérios para análise de vídeo e os locais de implementação, entre outros fatores. Além disso, faltam regras claras sobre coleta, armazenamento, uso e descarte de dados biométricos, bem como sobre os direitos dos cidadãos eventualmente identificados, detidos ou monitorados por essas tecnologias.

Essa forma descentralizada e pouco transparente de adoção dos sistemas gera inúmeros desafios operacionais, jurídicos, éticos e sociais. Há uma diversidade de pesquisas que demonstram, na prática, a disseminação do uso de TRFs leva à vigilância massiva, indiscriminada e desproporcional dos cidadãos (Amoore, 2020; Lyon, 2008). São amplamente conhecidos os limites, falhas e erros envolvidos na adoção dessas ferramentas, incluindo padrões discriminatórios que afetam desigualmente determinados grupos sociais em função de marcadores de diferenças sociais (Benjamin, 2019; Browne, 2015; Silva, 2020). Diversos estudos demonstraram que a maioria dos erros de identificação registrados pelas polícias no Brasil envolvem pessoas negras, muitas vezes presas de forma indevida e submetidas a processos criminais com base em reconhecimento equivocado (Nunes et al., 2022). Segundo levantamento do projeto Panóptico, entre os casos documentados de erro

14. Art. 5º, inc. LXXIX, Constituição da República.
15. Art. 37, Constituição da República.
16. Por exemplo, a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018, LGPD) e a Lei de Acesso à Informação (Lei 12.257/2011, LAI).
17. Disponível em: [www.opanoptico.com.br]. Acesso em: 25.082025.

de reconhecimento facial no País em 2019, mais de 90% envolviam homens negros (Rede de Observatórios da Segurança, 2019). Essas falhas, muitas vezes decorrentes do uso de imagens de baixa qualidade e bancos de dados desatualizados, agravam-se pela ausência de protocolos uniformes para validação das identificações, registro das operações e auditoria independente dos sistemas.

Esses casos expõem não apenas falhas técnicas, mas também um problema estrutural: a incorporação das TRFs em um sistema penal marcadamente seletivo e estruturalmente desigual (Flauzina, 2006). Assim, a produção sistemática de falsos positivos – os chamados "erros do sistema" – tem gerado diversas formas de constrangimento e violência, em geral, contra pessoas que já se encontram em condições de vulnerabilidade social (Nunes; Lima; Cruz, 2023). Isso é especialmente importante no contexto da segurança pública no Brasil, onde a suspensão dos direitos humanos é cotidiana na vida de grupos já marginalizados e frequentemente enquadrados como elementos de "desordem", como a população negra e periférica (Flauzina, 2006).

Ao revés de corrigirem esses problemas, os algoritmos tendem a reproduzi-los e amplificá-los, ao replicar padrões históricos de suspeição e incriminação com base em dados passados e vieses de classificação e suspeição. A promessa de neutralidade técnica, frequentemente mobilizada pelos fornecedores e operadores da TRFs, oculta o fato de que essas tecnologias são construídas sobre infraestruturas de desigualdade, tanto na coleta de dados quanto na maneira como os sistemas são operacionalizados no cotidiano das práticas policiais. A questão que se coloca não é apontar os erros e possíveis falhas das TRFs, mas entender como, apesar deles, essas tecnologias têm sido utilizadas criado condições de possibilidade de um modo específico de pensar e fazer práticas de identificação e reconhecimento de suspeitos (Lima, 2024, p. 10).

Do ponto de vista normativo, o Brasil possui um marco legal importante com a Lei Geral de Proteção de Dados Pessoais (LGPD – Lei 13.709/2018), que reconhece dados biométricos como sensíveis e estabelece princípios como finalidade, necessidade, transparência e segurança. A Emenda Constitucional 115/2022 elevou a proteção de dados pessoais à condição de direito fundamental. No entanto, ainda não há regulamentação específica para o uso de TRF por órgãos de segurança pública, um vácuo jurídico que permite interpretações diversas e usos muitas vezes arbitrários ou informalizados.

A situação se agrava diante da falta de diretrizes sobre como compatibilizar a proteção de dados com as necessidades de investigação criminal. O anteprojeto da chamada "LGPD Penal" (Projeto de Lei 1.515/2022) – elaborado por comissão de juristas e ainda em tramitação– tenta preencher essa lacuna ao propor regras específicas para o tratamento de dados pessoais para fins de segurança

pública, persecução penal, defesa nacional e segurança do Estado (Azevedo et al., 2022). Entre seus objetivos, estão a delimitação de finalidades, a definição de responsabilidades institucionais e a previsão de direitos e salvaguardas aos titulares dos dados.

No entanto, o projeto tem sido criticado por organizações da sociedade civil por apresentar uma estrutura excessivamente permissiva e vaga, permitindo ampla margem de discricionariedade às autoridades de segurança[18]. Um dos principais problemas identificados é a inversão do princípio da excepcionalidade: ao invés de impor limites rigorosos e salvaguardas à coleta e ao uso de dados sensíveis, o texto cria brechas que legitimam práticas invasivas sob a justificativa genérica de "interesse público". Além disso, o projeto falha em estabelecer mecanismos robustos de controle externo, auditoria independente e direito à contestação por parte dos titulares dos dados. Esse desenho normativo contrasta com marcos regulatórios internacionais mais protetivos, como o Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR), que impõe critérios mais restritivos ao uso de dados sensíveis em contextos de segurança. Assim, ainda que represente um esforço de normatização, o projeto evidencia os limites atuais para compatibilizar, na prática, as exigências da investigação penal com os princípios fundamentais da proteção de dados.

No campo judicial, o Conselho Nacional de Justiça (CNJ) tem discutido o uso de tecnologias digitais e sistemas de IA no Judiciário, inclusive com diretrizes sobre ética, transparência e *accountability*. Em março de 2025, o CNJ promulgou a Resolução 615, estabelecendo diretrizes para o uso de inteligência artificial no Poder Judiciário brasileiro (Brasil, 2025). Essa normativa proíbe expressamente o uso de sistemas de IA para prever crimes com base em características pessoais ou comportamentais, bem como a aplicação de TRFs para detecção de emoções, visando prevenir discriminações e violações de privacidade. Apesar desses avanços, a resolução permanece omissa quanto à admissibilidade de provas obtidas por meio de TRF em processos judiciais.

As lacunas regulatórias contribuem para o crescimento da autoridade epistêmica dos algoritmos, cuja atuação escapa ao controle externo e ao contraditório

18. AZEVEDO, Cynthia Picolo Gonzaga de; LIMA, Eliz Marina Bariviera de; SILVA, Felipe Rocha da; RODRIGUES, Gustavo Ramos; DUTRA, Luiza Corrêa de Magalhães; SANTARÉM, Paulo Rená da Silva; RODRIGUES, Victor Barbieri Vieira. *Nota técnica: análise comparativa entre o anteprojeto de LGPD penal e o PL 1515/2022.* Brasília: Laboratório de Políticas Públicas e Internet (LAPIN) e Instituto de Referência em Internet e Sociedade (IRIS), nov. 2022. Disponível em: [https://lapin.org.br/wp-content/uploads/2022/11/Nota-tecnica-Analise-comparativa-entre-o-anteprojeto-de-LGPD-Penal-e-o-PL-15152022-1.pdf]. Acesso em: 21 out. 2025.

efetivo no processo penal. Em um contexto em que algoritmos se tornam fontes e aparatos de investigação, essa brecha agrava a assimetria entre acusação e defesa, deixando advogados e réus sem acesso à origem dos dados, aos parâmetros técnicos utilizados ou à possibilidade de auditoria independente (Lima, 2024, p. 65).

Dessa forma, o Brasil se encontra diante de um desalinhamento: de um lado, um sistema jurídico que reconhece a proteção de dados como direito fundamental; de outro, um aparato de segurança pública que incorpora tecnologias altamente invasivas sem base legal clara, sem transparência e com elevado potencial de violação de garantias fundamentais. Esse conjunto de fatores – expansão acelerada, ausência de regulação, incentivos estatais, seletividade estrutural e opacidade técnica – cria uma infraestrutura socio-legal "ideal" para a atuação de empresas como a *Clearview AI*, cujas práticas de raspagem massiva de dados e oferta direta a órgãos de segurança operam justamente nesses interstícios regulatórios. É justamente nesse contexto que a empresa tem encontrado brechas para oferecer suas "soluções tecnológicas" e legitimar sua atuação no Brasil, como será analisado na próxima seção.

4. Entre rostos e rastros: *Clearview AI* e os limites do devido processo legal no Brasil

A trajetória da *Clearview AI* no Brasil ilustra como tecnologias de policiamento têm se inserido nas estruturas do Estado por vias informais e, posteriormente, vêm sendo institucionalizadas sem debate público ou definição de uma política clara. Inicialmente, a empresa buscou acesso ao mercado brasileiro por meio de apresentações em feiras de segurança, reuniões técnicas, testes gratuitos para agentes públicos e parcerias com intermediárias comerciais. Essa estratégia de penetração por entre frestas revela não apenas uma lógica de atuação empresarial da empresa, mas também uma ecologia regulatória permissiva e fragmentada, típica de contextos em que a implantação de tecnologias digitais avança mais rapidamente do que os marcos normativos e os mecanismos de controle institucional. Esse arranjo produz condições de possibilidades de experimentação e o uso de tecnologias com baixo *accountability* e alta plasticidade organizacional.

Documentos obtidos por meio da Lei de Acesso à Informação, reportagens investigativas e análise de transcrições públicas de entrevistas com representantes da empresa demonstraram que, desde 2019, a *Clearview AI* busca estabelecer vínculos com agências de segurança pública e autoridades brasileiras. Um ponto a destacar é que a empresa norte-americana não possui representação no Brasil, sendo necessária a presença de uma subsidiária para compra e uso formal no país. A prática de empregar revendedoras nacionais ou intermediárias, embora não caracterize ilegalidade flagrante, expõe uma lacuna significativa em termos de transparência,

uma vez que oculta o nome da empresa nos registros públicos disponíveis em portais da transparência.

A operacionalização dessas tecnologias no Brasil ocorre em um ambiente marcado por labirintos burocráticos e opacidade processual, como discutido na seção anterior. A ausência de regulamentação específica permite que contratos sejam firmados sem o devido escrutínio público e sem diretrizes claras sobre a proteção de dados pessoais. Essa lacuna regulatória favorece a adoção de sistemas cuja eficácia e ética são frequentemente questionadas, comprometendo princípios fundamentais como a privacidade e o devido processo legal. Ainda que o devido processo seja um conceito aberto, ele é fundamental para a garantia de direitos nas engrenagens dos sistemas jurídicos.

Em abril de 2022, a *Clearview* participou da feira ISC Brasil, um dos maiores eventos de segurança da América Latina, realizada em São Paulo. Na ocasião, representantes da empresa apresentaram a tecnologia a agentes de segurança pública, prometeram "testes gratuitos" e demonstraram a capacidade da TRF com base em imagens extraídas de redes sociais. Pouco tempo depois, a empresa participou de 3 reuniões técnicas com a Copaq da Secretaria Nacional de Segurança Pública (Senasp), órgão vinculado ao MJSP. Na primeira reunião, conforme relatado por jornalistas e confirmado por documentos obtidos para essa pesquisa, a *Clearview* ofereceu acesso experimental à ferramenta a agentes públicos, reafirmando seu interesse em atuar no Brasil (Martins, 2023). Como esses testes não entram nos registros burocráticos das agências (uso formalmente sancionado) e podem ser testados por agentes individuais, é difícil obter uma fotografia mais completa da extensão do histórico do uso da ferramenta no Brasil. Esse tipo de atuação revela uma lógica de penetração informal, na qual a empresa evita a via tradicional da contratação pública, optando por estratégias de aproximação técnica e comercial. Ademais, ao apresentar-se como empresa "de apoio à investigação" e não como fornecedora de *software* de reconhecimento facial, a *Clearview AI* reposiciona seu discurso jurídico e político para evitar obrigações contratuais, das exigências da LGPD e mecanismos de controle social. No plano discursivo, também se distancia de controvérsias e críticas públicas ao envolvendo o uso de TRFs no Brasil.

A atuação da *Clearview* se articula com a lógica de funcionamento do sistema de segurança pública brasileiro, que é altamente descentralizado, permeável à inovação tecnológica e vulnerável a pressões políticas e comerciais. Como observado nesta pesquisa, a incorporação de tecnologias de vigilância no Brasil frequentemente se dá por meio de demonstrações, testes-piloto, convênios improvisados ou parcerias informais, que escapam às exigências legais de contratação pública, fiscalização e prestação de contas (Lima et al., 2024). A *Clearview* se insere exatamente nesse modelo, oferecendo seu produto com "testes grátis" para agências

de segurança e como "recurso adicional", sem que isso passe pelo crivo institucional adequado. Dessa forma, o *software* circulou entre diversas agências ao redor do mundo, inclusive no Brasil, sem qualquer formalização contratual, bastando, em muitos casos, o uso de um *e-mail* institucional para obter acesso à ferramenta (Lima, 2024).

Os testes gratuitos geralmente oferecem dias de utilização aos policiais com um número limitado de buscas no sistema, e operam como forma de mostrar a capacidade da ferramenta e incentivar os agentes a promoverem sua aquisição em seus departamentos. Além disso, os próprios agentes passam a disseminar o uso da TRF em conferências ou por meio de redes de contato *online*, ampliando sua visibilidade entre diferentes corporações policiais (Hill, 2023; Haskins; Mac; McDonald, 2020). O uso de *e-mails* institucionais, vinculados a departamentos de polícia ou a endereços governamentais, nesses testes gratuitos gerou situações ambíguas, nas quais as próprias agências de segurança, por vezes, alegavam não ter plena ciência de que a tecnologia estava sendo utilizada por seus agentes. Essa lógica de "informalidade" expõe uma delegação tácita de autoridade tecnológica ao agente individual, sem qualquer protocolo organizacional, treinamento técnico ou orientação administrativa e jurídica claras.

Várias questões empíricas surgem em relação aos usos operacionais da *Clearview* e, de forma mais abrangente das TRFs. Os policiais constroem e, em consequência entendem o conhecimento que recebem de diferentes maneiras (Brayne; Christin, 2020). Entre essas questões, destacam-se: a forma como os julgamentos de risco dos operadores é enquadrada pela informação trazida à sua atenção pela interface com o algoritmo; o impacto nos julgamentos operacionais subsequentes; a natureza dinâmica da interação humano-computador; e como isso afeta os níveis de risco e, portanto, a vontade de intervir (Fussey; Davis; Innes, 2021). Os dados, a informação, não apenas informam, mas também cria forma (Heidegger, 1997, p. 182) de como a suspeita tem sido compreendida pelo operador do sistema e quais ações podem ser tornadas possíveis.

Em 2023, o MJSP adquiriu acesso ao sistema da *Clearview AI* por meio da empresa Inspect Inteligência e Tecnologia Ltda., em um processo sigiloso que omitiu o nome da *Clearview* dos registros oficiais. A contratação, feita sem licitação e sem consulta pública, demonstra como a formalização institucional pode ocorrer à revelia da transparência e da legalidade substancial (Martins, 2025). Ao ocultar a titularidade da tecnologia adquirida, o governo federal evitou o escrutínio social sobre o uso de uma ferramenta altamente controversa, proibida em diversos países da Europa e alvo de ações judiciais nos Estados Unidos, Reino Unido, Canadá e Austrália por violações à privacidade. Além do MJSP, também a polícia do Senado Federal firmou contrato com a *Clearview*, por meio da mesma intermediária, com vigência

entre novembro de 2024 e 2025 (Brasil, 2024). Da mesma forma, o Ministério Público e a Polícia Civil de Minas Gerais adquiriram acesso à tecnologia por três anos (Minas Gerais, 2025), evidenciando a consolidação da presença e operação da empresa no sistema de justiça e segurança brasileiro. Esses contratos marcam uma transição de práticas informais para a institucionalização de uma ferramenta cuja arquitetura tecnológica se baseia na coleta massiva e não autorizada de dados biométricos, o que desafia diretamente os princípios da LGPD e da Emenda Constitucional 115/2022, que reconhece a proteção de dados como direito fundamental.

Além disso, a tecnologia se beneficia de um ambiente jurídico ambíguo, no qual a ausência de norma específica para TRF em segurança pública permite a interpretação de que imagens publicamente disponíveis na *internet* podem ser utilizadas em investigações, mesmo sem autorização judicial, sem consentimento dos titulares e sem qualquer tipo de controle sobre sua origem, qualidade ou contexto. Essa ambiguidade facilita e legitima a circulação da ferramenta e, ao mesmo tempo, compromete os direitos dos cidadãos cujas imagens são capturadas, processadas e comercializadas.

O uso de dados de fontes abertas – prática central no modelo da *Clearview* – insere-se no debate mais amplo sobre o uso de Osint (*Open Source Intelligence*) em investigações criminais (Chermak et al., 2025). Apresentada frequentemente como alternativa legítima ao acesso direto a bases protegidas, essa estratégia de coleta de dados exige, no entanto, critérios jurídicos rigorosos relacionados à finalidade, necessidade e proporcionalidade de uso (Macêdo, 2019). Isso porque o fato de um dado estar acessível e público não significa que ele esteja disponível para qualquer finalidade. No entanto, no caso da *Clearview*, há um deslocamento dessa lógica: as imagens deixam de ser meros insumos investigativos auxiliares e passa a ser ponto de partida para a formulação de suspeitas. Rostos são vinculando automaticamente a identidades, redes de sociabilidades, localizações ações passadas, produzindo associações que ganham status de indícios investigativos. Nesse processo, a TRF não se limita a refletir uma realidade preexistente, mas contribui para materializá-la (Barad, 2007) – criando condições para que determinadas identidades se tornem suspeitas, mesmo sem evidências tradicionais. Trata-se de uma operação que transforma dados visuais processados algoritmicamente em narrativas incriminadoras, tensionando os princípios do devido processo legal, da ampla defesa e da legalidade da prova.

Apesar do uso crescente, a confiabilidade das TRFs em investigações criminais e sua validade como como evidência ainda não foram estabelecidas. Falta transparência mínima sobre como os algoritmos são utilizados na prática e como as evidências produzidas por eles têm sido enquadradas processualmente. Advogados de defesa, procuradores, os juízes e até mesmo os agências de segurança não tem

clareza de como os algoritmos estão sendo operados (Lima, 2024, p. 115). O exemplo da *Clearview AI*, mostra como esse uso pode ocorrer mesmo sem que, de fato, o departamento adquira formalmente a licença de uso, mas sim por meio de testes gratuitos. Isso representa um exemplo mais latente das maneiras pelas quais os a pulverização do uso das TRFs tem acontecido de maneira flexível, uma prática remodelável conforme o contexto organizacional de cada instituição.

Os danos e as violências das abordagens, detenções e investigações errôneas ancoradas nos resultados probabilísticos do algoritmo tendem a se materializar em ações práticas, embora muitas vezes sejam difíceis de quantificar. Trata-se de um problema difundido: a maioria das agências de segurança que usam a tecnologia ao redor do mundo não produzem os dados de buscas feitos pela TRFs, os casos de falso positivos e quais ações eles deram ignição, como número de abordagens ou prisões (Brayne; Christin, 2020; Fussey; Davis; Innes, 2021).

Há também uma outra camada complexa que desafia os regimes jurídicos estabelecidos, quando os resultados dessas ferramentas passam a integrar o processo penal sem observância à cadeia de custódia da prova digital. A ausência de mecanismos claros para garantir a integridade, a autenticidade e a rastreabilidade das provas digitais comprometem sua validade jurídica (Sanglard, 2023; Santos et al., 2021). Esse *déficit* de garantias como a preservação da cadeia de custódia de provas digitais compromete o devido processo legal, um dos pilares do sistema acusatório. Os dados não são entidades neutras, mas efeitos de relações intra-ativas entre atores, dispositivos, normas e materialidades (Barad, 2007; Lima, 2024). O dado gerado pelo algoritmo da *Clearview* não apenas emerge de práticas extrajudiciais de raspagem de dados, mas é reclassificado e recontextualizado como prova penal sem qualquer mediação institucional. Além de criar condições de possibilidade de não apenas ligar a imagem a um reconhecimento de identidade, mas a outros dados de rede sociais, metadados de localização, data e hora, *hashtag* e redirecionar a outras páginas da *internet*. E a partir desses metadados gerar *links* entre indivíduos e lugares.

O que se observa é a ampliação dos espectros de suspeição: rostos e perfis que precisam ser vigiados e/ou neutralizados para a manutenção da ordem e gerenciamento de risco (Amoore, 2020). Nesse sentido, o sistema não opera só sob a lógica do crime que foi cometido, mas também de forma a antecipar outros possíveis crimes, alinhando-se a uma lógica amplamente compartilhada entre os vários esforços para gerenciar risco, dentro do domínio da segurança. O reconhecimento de padrões e classificação algorítmica de pessoas tornam-se, assim, parte do *modus operandi* de diversas práticas históricas de controle de grupos e indivíduos para a manutenção da "ordem" (Cole, 2002).

Portanto, é importante refletir os impactos do uso da tecnologia no regime probatório da justiça criminal de modo que sua legalidade ou validade sejam

adequadamente questionadas nos processos. Trata-se de uma mutação nas formas de reconhecimento legalmente válidas, onde a mediação algorítmica passa a eclipsar outros mecanismos de investigação, produção de evidências e mediação pericial. Em entrevistas e investigações conduzidas por organizações da sociedade civil, defensores públicos relataram que materiais obtidos via TRFs, inclusive de sistemas informais, têm sido utilizados como elementos de convencimento judicial, mesmo sem laudo técnico formal, cadeia de custódia ou auditoria externa (Lima, 2024). O modo de dizer uma verdade do algoritmo ganha *status* de verdade técnica – e o risco de erro, viés ou manipulação torna-se parte da disputa e do debate a ser travado para garantia dos direitos fundamentais.

Nesse sentido, a figura do perito e o enquadramento do algoritmo enquanto *expert*, está inserida e são produtos do que Cole (2002, p. 15) chamou de "compromissos históricos da ciência e da lei para a produção de ordem". Esse processo revela uma transformação profunda: o algoritmo não apenas auxilia a investigação, mas reconfigura os modos de produzir verdade e culpabilidade no processo penal. Os sistemas algorítmicos operam por padrões probabilísticos, e não por certezas jurídicas – mas, ao serem apresentados como "evidências técnicas", acabam ganhando autoridade epistêmica e processual (Lima, 2024). A inteligibilidade pode resultar também na exclusão de narrativas alternativas e outros modos de "contar a verdade". No caso da *Clearview*, essa autoridade se constrói com base em um repositório de dados biométricos com origem contestável, mas cujos resultados são tomados como suficientemente credíveis (Lima, 2024, p. 73). O ciclo se fecha quando promotores, juízes e defensores não têm acesso aos parâmetros técnicos, às imagens comparadas, à taxa de erro do sistema, aos critérios utilizados na identificação e aos procedimentos operacionais padrão de uso institucional da ferramenta.

No Brasil, esse circuito é problemático porque reforça práticas históricas de policiamento e suspeição. Em um sistema penal marcado por seletividade estrutural e desigualdade institucional, o uso de TRF para fins de segurança exige não apenas uma discussão regulatória, jurídica, política e social, mas também um debate mais amplo sobre o regime de segurança pública e do aparato de justiça criminal. Como produzir justiça quando os operadores do direito não têm acesso às bases de funcionamento das ferramentas que sustentam as acusações e que derem ignição a abordagens? Como garantir o contraditório em um ecossistema de provas algorítmicas que escapa aos mecanismos institucionais clássicos de verificação? O que está em jogo não é apenas a proteção de dados pessoais e os desafios à privacidade, mas também a arquitetura de um regime de produção de conhecimento e verdade de segurança e jurídica que opera como condição de possibilidade para uma distribuição desigual de insegurança e direitos.

Nossa tendência é nos tornarmos confortáveis com nossos quadros interpretativos. Por isso, desestabilizar os imaginários sobre o que os algoritmos são e o que podem fazer no sistema de justiça criminal é um passo que pode nos ajudar o entender como essas tecnologias podem sufocar possibilidades de ação e legitimar práticas violentas e excludentes na tentativa de estabilizar uma ordem e domesticar o risco.

5. Conclusão

A trajetória da *Clearview AI* e sua circulação transnacional evidenciam com nitidez os impasses contemporâneos entre inovação tecnológica, segurança pública e efetivação de direitos fundamentais. Ao consolidar uma infraestrutura algorítmica baseada na raspagem massiva de dados biométricos extraídos de fontes públicas, a empresa desafia os direitos fundamentais, marcos regulatórios de proteção da privacidade e dispositivos de *accountability* democrática.

No caso brasileiro, esse modelo se insere em um regime de segurança pública marcado por fragmentação regulatória, improvisação institucional e seletividade estrutural. A circulação da *Clearview,* por meio de testes gratuitos, feiras, reuniões técnicas e contratos pouco claros, ilustra como tecnologias de alto risco a direitos podem ser integradas a práticas policiais e judiciais sem passar por filtros mínimos de controle, transparência ou avaliação pública.

Mais do que uma controvérsia sobre coleta ilícita de dados, o caso *Clearview AI* demonstra a formação de redes sociotécnicas de vigilância nas quais empresas privadas, agentes públicos e operadores do direito coproduzem novas formas de identificar, classificar e incriminar. As TRFs, longe de serem ferramentas neutras, atualizam e automatizam práticas históricas de suspeição ancoradas em marcadores sociais de diferença. Elas não apenas transformam rostos em dados, mas reconfigura as formas de produção de insegurança, alimentando práticas discriminatórias, violentas e atravessadas por desigualdades sociais, tecnológicas e epistemológicas.

No campo da justiça criminal, essas tecnologias impõem desafios concretos: como garantir o contraditório e a ampla defesa quando os dados são opacos, os algoritmos são protegidos por segredo comercial e os critérios de identificação não são auditáveis? Como assegurar a legitimidade da prova penal quando sua origem está ancorada em bancos privados não supervisionados por nenhuma instância pública? A questão não se resume aos riscos de erro ou aos falsos positivos. O que está em jogo é a consolidação de uma nova racionalidade penal, sustentada por tecnologias que tornam rotineira a vigilância massiva, naturalizam a suspeição preditiva e esvaziam as garantias processuais e de direitos. Em um cenário de baixa

transparência, as próprias agências públicas – e a sociedade como um todo – não têm clareza sobre como as TRFs operam nem quais impactos essas tem produzido.

As TRFs vêm sendo utilizadas de maneira persistente por órgãos de segurança mesmo diante de falhas conhecidas e controvérsias em torno de erros, abordagens vexatórias e violações de direitos fundamentais. Na prática, a ausência de regulação inverte o princípio da inocência: exige-se do cidadão uma demonstração contínua de que "não tem nada a esconder" para evitar ser enquadrado como suspeito. Em muitos casos, as buscas através de TRFs sequer se limitam a indivíduos sob investigação, ampliando o escopo da vigilância para a população em geral, como as possibilidades de uso da *Clearview AI.* Várias questões éticas e políticas decorrem do poder crescente dessas tecnologias, especialmente quando operam em contextos marcados pela flexibilização de garantias processuais, que tende a se tornar regra, e não exceção.

Segundo Deleuze e Guattari (1995, p. 175), as próprias máquinas não explicam nada, "é preciso analisar os aparatos coletivos dos quais as máquinas são apenas um componente". Nessa perspectiva, a TRFs não devem ser analisadas isoladamente, mas como parte de arranjos sociotécnicos e institucionais mais amplos. Enfrentar seus impactos exige, portanto, não apenas regulação normativa, mas também uma análise crítica sobre os aparatos coletivos que tornam sua adoção possível – e que a legitimam como forma eficiente, embora opaca, de governar a insegurança. Diante disso, analisar o caso *Clearview* é também refletir sobre os contornos emergentes de uma nova arquitetura do processo penal – mais opaca, mais automatizada e cada vez mais distante das promessas constitucionais de justiça.

Referências

AMERICAN CIVIL LIBERTIES UNION. *ACLU v. Clearview AI*. [S.l.]: ACLU, [s.d.]. Disponível em: [https://aclu.org/cases/aclu-v-clearview-ai]. Acesso em: 21.06.2023.

AMOORE, L. *Cloud ethics*: Algorithms and the attributes of ourselves and others. Durham: Duke University Press, 2020.

ARADAU, C.; BLAKE, T. Algorithmic Surveillance and the Political Life of Error. *Journal for the History of Knowledge*, v. 2, n. 1, p. 10, 2021. [https://doi.org/10.5334/jhk.42].

AZEVEDO, Cynthia Picolo Gonzaga de; LIMA, Eliz Marina Bariviera de; SILVA, Felipe Rocha da; RODRIGUES, Gustavo Ramos; DUTRA, Luiza Corrêa de Magalhães; SANTARÉM, Paulo Renã da Silva; RODRIGUES, Victor Barbieri Vieira. 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. Disponível em: [https://lapin.org.br/wp-content/uploads/2022/11/Nota-tecnica-Analise-comparativa-entre-o-anteprojeto-de-LGPD-Penal--e-o-PL-15152022-1.pdf]. Acesso em: 15.03.2025.

BARAD, K. *Meeting the universe halfway*: Quantum physics and the entanglement of matter and meaning. Durham: Duke University Press, 2007.

BAUMAN, Zygmunt et al. Após Snowden: repensando o impacto da vigilância. *Revista Eco-Pós*, v. 18, n. 2, p. 8-35, 2015.

BENJAMIN, R. Assessing risk, automating racism. *Science*, v. 366, n. 6464, p. 421-422, 2019.

BISCHOFF, Paul. *Facial recognition technology (FRT)*: 100 countries analyzed. Comparitech, 28 de junho de 2021. Disponível em: [https://www.comparitech.com/blog/vpn-privacy/facial-recognition-statistics/]. Acesso em: 21.10.2025.

BRASIL. SENADO FEDERAL. *Transparência e prestação de contas*. Licitações e contratos. Contrato 196/2024. Atualizado em: 13.12.2024. Disponível em: [www6g.senado.gov.br/transparencia/licitacoes-e-contratos/contratos/7982]. Acesso em: 31.03.2025.

BRAYNE, Sarah. Big data surveillance: The case of policing. *American Sociological Review*, v. 82, n. 5, p. 977-1008, 2017.

BRAYNE, Sarah; CHRISTIN, Angèle. Technologies of crime prediction: The reception of algorithms in policing and criminal courts. *Social Problems*, v. 68, n. 3, p. 608-624, 2021.

BROWNE, S. *Dark matters*: On the surveillance of blackness. Durham: Duke University Press, 2015.

BUOLAMWINI, J.; GEBRU, T. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of Machine Learning Research*, v. 81, p. 1-15, 2018. Disponível em: [https://proceedings.mlr.press/v81/buolamwini18a.html].

CHERMAK, S. M. et al. Open-Source Research in Criminology and Criminal Justice. *Annual Review of Criminology*, v. 8, 2025.

CLEARVIEW AI NAMED to Time's inaugural list of the Time100 most influential companies. *Clearview AI*, New York, 29.04.2021. Disponível em: [www.clearview.ai/press-room/clearview-ai-named-to-times-inaugural-list-of--the-time100-most-influential-companies]. Acesso em: 17.04.2025.

CLEARVIEW AI SETTLES ACLU. Illinois Lawsuit confirming continuity of business supporting public safety. *Clearview AI*, New York, 12.05.2022. Disponível em: [www.clearview.ai/press-room/clearview-ai-settles-aclu--illinois-lawsuit-confirming-continuity-of-business-supporting-public--safety]. Acesso em: 17.04.2025.

COLE, Simon A. *Suspect identities*: A history of fingerprinting and criminal identification. Harvard University Press, 2002.

CRAWFORD, K. *The atlas of AI*: Power, politics, and the planetary costs of artificial intelligence. New Haven: Yale University Press, 2021.

FELDSTEIN, Steven. *The global expansion of AI surveillance*. Washington, DC: Carnegie Endowment for International Peace, 2019. Disponível em: [https://carnegieendowment.org/research/2019/09/the-global-expansion-of-ai-surveillance?lang=en]. Acesso em: 21.10.2025.

FERGUSON, A. G. *The rise of big data policing*: Surveillance, race, and the future of law enforcement. New York: NYU Press, 2017.

FLAUZINA, A. L. P. *Corpo negro caído no chão*: o sistema penal e o projeto genocida do Estado brasileiro. 2006.

FUSSEY, Pete; DAVIES, Bethan; INNES, Martin. 'Assisted' facial recognition and the reinvention of suspicion and discretion in digital policing. The British journal of criminology, v. 61, n. 2, p. 325-344, 202.

DELEUZE, Gilles; GUATTARI, Félix. *Introdução*: rizoma. Mil platôs: capitalismo e esquizofrenia, v. 1, p. 11-37, 1995.

HASKINS, C.; MAC, R.; MACDONALD, L. Clearview AI facial recognition software's use by authoritarian regimes. *BuzzFeed News*, 2020. Disponível em: [www.buzzfeednews.com/article/carolinehaskins1/clearview-ai-facial--recognition-authoritarian-regimes-22]. Acesso em: 10.06.2024.

HEIDEGGER, Martin. *Kant and the Problem of Metaphysics, enlarged*. Indiana University Press, 1997.

HILL, K. *Your Face Belongs to Us*: A Tale of AI, a Secretive Startup, and the End of Privacy. New York: Random House, 2023.

KATZ, Yarden. *Artificial whiteness*: Politics and ideology in artificial intelligence. Columbia University Press, 2020.

LIMA, T. G. L. et al. *Vigilância por lentes opacas*: mapeamento da transparência e responsabilização nos projetos de reconhecimento facial no Brasil. Rio de Janeiro: CESeC, 2024.

LIMA, T. G. L. *Better justice through better science-technology?* The entanglements of algorithms and security and legal professionals. 2024. Tese (Doutorado) – Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, Brasil.

LYON, D. Biometrics, identification and surveillance. *Bioethics*, v. 22, n. 9, p. 499-508, 2008. DOI: [https://doi.org/10.1111/j.1467-8519.2008.00697.x].

MAC, R.; HASKINS, C.; PEQUENO IV, A. Police In At Least 24 Countries Have Used Clearview AI. Find Out Which Ones Here. *Buzzfeed*, 25.08.2021. Disponível em: [www.buzzfeednews.com/article/ryanmac/clearview-ai-international-search-table]. Acesso em: 27.03.2024.

MACÊDO, A. S. *A intersecção entre* Osint *e* Humint *através da abordagem de* crowdsourcing *como subsídio para ações de inteligência policial*. 2019. Dissertação (Mestrado em Ciência da Informação) – Universidade Federal de Santa Catarina, Florianópolis, 2019. [https://repositorio.ufsc.br/handle/123456789/219176]. Acesso em: 27.03.2024.

MARTINS, Laís. Exclusivo: em reuniões secretas, Clearview ofereceu 3 bilhões de imagens de brasileiros para polícias e Ministério da Justiça. *Intercept Brasil*, 16.05.2023. Disponível em: [www.intercept.com.br/2023/05/16/em-reunioes-secretas-clearview-policias-ministerio-da-justica/]. Acesso em: 27.03.2024.

MARTINS, Laís. Vigilância turbinada: Ministério da Justiça comprou secretamente tecnologia que coleta fotos sem autorização para reconhecimento facial. *Intercept Brasil*, São Paulo, 03.02.2025. Disponível em: [www.intercept.com.br/2025/02/03/ministerio-da-justica-comprou-secretamente-tecnologia-que-coleta-fotos-sem-autorizacao-para-reconhecimento-facial/]. Acesso em: 31.03.2025.

MCSORLEY, Tim. The case for a ban on facial recognition surveillance in Canada. *Surveillance & Society*, v. 19, n. 2, p. 250-254, 2021.

MINAS GERAIS. *Portal da Transparência do Estado de Minas Gerais*. Contrato 9437287. Belo Horizonte: Governo do Estado, 2025. Disponível em: [www.transparencia.mg.gov.br/licitacoes-e-contratos/compras-e-contratos/comprasecontratos-filtros/5/2024/01-01-2024/31-12-2024/91/87547]. Acesso em: 27.03.2025.

MOROZOV, E. *To save everything, click here*: Technology, solutionism and the urge to fix problems that don't exist. London: Allen Lane, 2013.

NUNES, P.; LIMA, T. G. L.; CRUZ, T. G. *O sertão vai virar mar*: expansão do reconhecimento facial na Bahia. Rio de Janeiro: CESeC, 2023.

O PANÓPTICO. *O Panóptico*. [S.l.]: o Panóptico, [s.d.]. Disponível em: [www.opanoptico.com.br/]. Acesso em: 27.12.2024.

PRESS, E. Does A.I. Lead Police to Ignore Contradictory Evidence? *The New Yorker*, 20 nov. 2023. Disponível em: [www.newyorker.com/magazine/2023/11/20/does-a-i-lead-police-to-ignore-contradictory-evidence]. Acesso em: 13.04.2024.

RAMAGE, Jack. Facial recognition company Clearview AI permanently banned from selling data to private companies. *Euronews*, 10.05.2022. Disponível em: [www.euronews.com/next/2022/05/10/facial-recognition-company--clearview-ai-permanently-banned-from-selling-data-to-private-co]. Acesso em: 13.04.2024.

REDE DE OBSERVATÓRIOS DA SEGURANÇA. *1º Relatório da Rede de Observatórios da Segurança*. [S.l.]: Observatório da Segurança, 2019. Disponível em: [https://observatorioseguranca.com.br/wordpress/wp-content/uploads/2019/11/1relatoriorede.pdf]. Acesso em: 21.10.2025.

REZENDE, Isadora Neroni. Facial recognition in police hands: Assessing the 'Clearview case' from a European perspective. *New Journal of European Criminal Law*, v. 11, n. 3, p. 375-389, 2021.

SANGLARD, J. F. *Cadeia de custódia da prova digital no processo penal brasileiro*. Tese. São Paulo, Universidade Presbiteriana Mackenzie, 2023.

SANTOS, A. J. S.; BORGES, A. F. M.; RODRIGUES, G. L. M. T. A cadeia de custódia na coleta da prova digital de acordo com a Lei 13.964/2019, dos seus artigos 158-A ao 158-F. *RECIMA21:* Revista Científica Multidisciplinar, v. 2, n. 8, e28612, 2021.

SEAVER, Nick. Algorithms as culture: Some tactics for the ethnography of algorithmic systems. *Big data & society*, v. 4, n. 2, p. 2053951717738104, 2017.

SILVA, Tarcízio. *Racismo algorítmico em plataformas digitais*: microagressões e discriminação em código. Comunidades, algoritmos e ativismos digitais: olhares afrodiaspóricos, 2020. p. 121-135.

SOUSA, R. et al. *Sport, data and rights*: use of facial recognition in Brazilian stadiums. Rio de Janeiro: CESeC, 2024.

THYLSTRUP, Nanna Bonde. *The politics of mass digitization*. MIT Press, 2019.

Legislação

BRASIL. Conselho Nacional de Justiça. *Resolução 615, de 11 de março de 2025*. Estabelece diretrizes para o desenvolvimento, utilização e governança de soluções desenvolvidas com recursos de inteligência artificial no Poder Judiciário. Disponível em: [https://atos.cnj.jus.br/files/original155530202 5031467d4517244566.pdf]. Acesso em: 31.03.2025.

BRASIL. Portaria 793, de 24 de outubro de 2019. Ministério da Justiça e Segurança Pública/Gabinete do Ministro. *Diário oficial da União*. Disponível em: [www.in.gov.br/en/web/dou/-/portaria-n-793-de-24-de-outubro-de-2019-223853575].

Recebido em: 31.03.2025.
Aprovado em: 26.05.2025.
Última versão da autora: 05.06.2025.

PESQUISA DO EDITORIAL

Área do Direito: Penal; Digital

Veja também Doutrina relacionada ao tema

- Dados pessoais no processo penal: tutela da personalidade e da inocência diante da tecnologia, de Flaviane de Magalhães Barros Bolzan de Morais, Leonardo Augusto Marinho Marques e Jamilla Monteiro Sarkis – *RBCCrim* 190/117-156;
- Nota técnica sobre o uso de biometria facial no Metrô de São Paulo, de Cristiano Colombo e Guilherme Damasio Goulart – *BRTO* 25;
- O reconhecimento facial na segurança pública e a proteção de dados pessoais como garantia fundamental, de Beatriz Daguer, Luiz Antonio Borri e Rafael Junior Soares – *RDTec* 16;
- Reconhecimento facial e prova ilícita: a possibilidade de se considerar o reconhecimento facial como meio de prova ilícito, de Matheus Della Monica e Rodrigo Marchetti Ribeiro – *RDTec* 13; e
- Vigiar e Punir 4.0: efeitos das tecnologias de policiamento preditivo e reconhecimento facial no brasil e a perpetuação do racismo estrutural, de Fernanda Mateus Rosa da Silva – *RDTec* 16.

Veja também Jurisprudência relacionada ao tema

- TJSP, AgIn 2079077-58.2022.8.26.0000, j. 10.10.2022, *DJe* 18.10.2022.

Lima, Thallita Gabriele Lopes. *Faces make cases*: o caso *Clearview AI* e os desafios do uso de tecnologias algorítmicas no sistema de justiça criminal brasileiro. *Revista Brasileira de Ciências Criminais*. vol. 211. ano 33. p. 85-114. São Paulo: Ed. RT, nov./dez. 2025. DOI: [doi.org/10.5281/zenodo.17058344].

Devida investigação criminal: compromissos epistêmicos e probatórios na extração de dados pessoais em fontes abertas

Due criminal investigation: epistemic and evidential commitments in the extraction of personal data from open sources

Anderson Pires Giampaoli[1]
Universidade de São Paulo, USP. Brasil.
agiampaoli@uol.com.br

Rafael Francisco Marcondes de Moraes[2]
Academia de Polícia "Dr. Coriolano Nogueira Cobra", Acadepol, Brasil.
rafaelfmmoraes@gmail.com

Roberta de Lima e Silva[3]
Pontifícia Universidade Católica do Rio Grande do Sul, PUCRS, Brasil.
robertalsilva1@gmail.com

DOI: [https://doi.org/10.5281/zenodo.17058359].

1. Doutorando em Direito Processual Penal pela Universidade de São Paulo. Mestre em Direito Probatório pela Universidade de Barcelona (2022). Especialista em Bases do Raciocínio Probatório pela Universidade de Girona (2021). Professor da Academia de Polícia "Dr. Coriolano Nogueira Cobra" (Acadepol).
   Lattes: [https://lattes.cnpq.br/6389905236681008].
   ORCID: [https://orcid.org/0000-0003-3762-6843].
   E-mail: agiampaoli@uol.com.br
2. Doutor (2024) e Mestre (2018) em Direito Processual Penal pela Universidade de São Paulo (USP). Professor da Academia de Polícia "Dr. Coriolano Nogueira Cobra" (Acadepol). Graduado pela Faculdade de Direito de Sorocaba (FADI). Pesquisador Associado do Núcleo de Estudos da Violência da Universidade de São Paulo (NEV-USP).
   Lattes: [http://lattes.cnpq.br/6946804943470891].
   ORCID: [https://orcid.org/0000-0001-6515-1692].
   E-mail: rafaelfmmoraes@gmail.com
3. Mestranda em Direito pela Pontifícia Universidade Católica do Rio Grande do Sul. Mestra em Raciocínio Probatório pela Universitat de Girona (Espanha). Pós-graduada em Direito Penal Econômico pela Fundação Getulio Vargas de São Paulo (2020). Especialista em

Área do Direito: Processual; Penal; Digital

Resumo: O presente ensaio cuida do valor probatório e epistêmico dos elementos produzidos no contexto de uma devida investigação criminal, na qual a mineração e a raspagem de dados e informações pessoais em fontes abertas (*knowledge discovery databases)*, mormente redes sociais, colaboram com a adequada determinação dos fatos de interesse criminal e com a justificação sobre aquilo que se afirma sobre esses mesmos fatos (*quaestio facti*). A partir de reflexões sobre a apuração dos eventos conhecidos como ataques de 8 de janeiro de 2023, em Brasília, assim como de premissas teóricas que caracterizam o processo penal contemporâneo, a proposta consiste em balizar a utilização dessas evidências digitais, sobretudo em razão das questões jurídicas envolvidas e os reflexos no campo probatório (*quaestio iuris*). O método de abordagem foi o hipotético-dedutivo, com método de procedimento monográfico ou estudo de caso e método de interpretação sistemático. Para tanto, aplicou-se a técnica de pesquisa de revisão bibliográfica sistemática, aliada às contribuições da epistemologia. O estudo evidenciou a relevância da formulação de protocolos e mecanismos para garantir a autenticidade e a integridade dos vestígios digitais extraídos de fontes abertas, dada a ausência de uma Lei Geral de Proteção de Dados Pessoais penal. A adoção de tais medidas se apresenta como uma possibilidade para garantir a fiabilidade das provas digitais e a conformidade das investigações criminais com base em parâmetros epistemicamente orientados.

Palavras-chave: Devida investigação criminal – Epistemologia – Prova digital – Cadeia de custódia – Fontes abertas.

Abstract: This study deals with the evidentiary and epistemic value of the elements produced in the context of a due criminal investigation, in which the mining and scraping of personal data and information from open sources (knowledge discovery databases), especially social networks, contribute to the adequate determination of facts of criminal interest and to the justification of what is stated about these same facts (*quaestio facti*). Based on reflections on the events known as the January 8, 2023 attacks in Brasília, as well as theoretical premises that characterize the contemporary criminal process, the proposal consists of guiding the use of this digital evidence, especially due to the legal and juridical issues involved and the repercussions in the evidentiary field (*quaestio iuris*). The approach was hypothetical-deductive, with a monographic procedure or case study method and a systematic interpretation method. To this end, the research technique of systematic literature review was applied, combined with the contributions of epistemology. The study highlighted the relevance of formulating protocols and mechanisms to guarantee the authenticity and integrity of digital traces extracted from open sources, given the absence of a General Law on the Protection of Personal Data. The adoption of such measures presents a possibility to guarantee the reliability of digital evidence and the compliance of criminal investigations based on epistemically oriented parameters.

Keywords: Due criminal investigation – Epistemology – Digital evidence – Chain of custody – Open sources.

Prova Testemunhal desde o Raciocínio Probatório e a Psicologia do Testemunho pela Universitat de Girona (Espanha) e em Obtenção, Interpretação e Valoração da Prova pela Universidad de Salamanca (Espanha). Graduada em Direito pela Pontifícia Universidade Católica de São Paulo. Assistente Jurídica no Tribunal de Justiça do Estado de São Paulo.

Currículo Lattes: [http://lattes.cnpq.br/6935852760094787].

ORCID: [https://orcid.org/0009-0009-9183-1750].

E-mail: robertalsilva1@gmail.com

Giampaoli, Anderson Pires; Moraes, Rafael Francisco Marcondes de; Silva, Roberta de Lima e. Devida investigação criminal: compromissos epistêmicos e probatórios na extração de dados pessoais em fontes abertas.
Revista Brasileira de Ciências Criminais. vol. 211. ano 33. p. 115-141. São Paulo: Ed. RT, nov./dez. 2025.
DOI: [https://doi.org/10.5281/zenodo.17058359].

Sumário: 1. Introdução. 2. Ponto de partida: os ataques de 8 de janeiro de 2023. 3. Bases modernas e mínimas do contexto da devida investigação criminal. 4. *Big data*, fontes abertas e agregadores de dados: dimensão epistêmica das ferramentas disponíveis à persecução penal. 5. Natureza jurídica das razões epistêmicas coletadas: o problema do vácuo legislativo. 6. Cadeia de custódia da prova digital: autenticidade e integridade da *digital evidence*. 7. Considerações finais. Referências. Legislação. Jurisprudência.

1. Introdução

Há muitos desafios no campo probatório que permeiam o processo penal contemporâneo. Não se pode mais conceber que a prova penal seja um tema exclusivo do ordenamento jurídico, algo que as questões de direito (*quaestio iuris*) solucionem fácil e de forma satisfatória. O que se quer dizer com tal premissa é que, conquanto os representantes do povo legislem sobre temas ligados à (in)admissibilidade, à produção e à valoração da prova, a literatura jurídica, a jurisprudência e os personagens do sistema de justiça criminal precisam voltar os seus olhares para as questões de fato ou de mundo (*quaestio facti*), abrindo as portas, assim, para o ingresso e a colaboração de saberes oriundos de outros ramos do conhecimento, como a epistemologia.

Nessa linha de pensamento, considerando que um dos objetivos da persecução criminal estatal, para a correta aplicação da lei penal, insere-se na busca de uma verdade possível, sempre respeitando as liberdades das pessoas envolvidas, a epistemologia, enquanto teoria do conhecimento, tem auxiliado na edificação de um devido processo legal, mais justo e equitativo, sobretudo por contribuir com a reconstrução histórica dos fatos de interesse penal e colaborar com todos os atores do sistema de justiça criminal na justificação daquilo que cada um afirma sobre tais episódios.

Logo, para além daquilo que o direito disciplina, no exame de um determinado meio de prova ou de obtenção de prova, é imprescindível verificar o seu potencial epistêmico, ou seja, sua relevância na reconstrução e na determinação dos fatos e, por conseguinte, na busca da verdade sobre o evento apurado.

A temática ganha novas gradações ao se ponderar que significativa parcela dos materiais resultantes dos referidos meios de prova e de obtenção de prova são produzidos na etapa extrajudicial do devido processo penal, trazendo à tona a discussão sobre o controle e o valor a serem conferidos à investigação policial.

Fixadas essas ideias iniciais, premissas teóricas das quais se parte, pode-se dizer que o propósito deste trabalho compreende analisar como informações e dados contidos em fontes abertas, em particular naquilo que se denomina *big data*, podem auxiliar na reconstrução histórica de fatos penalmente relevantes. Em outras palavras, o que se propõe é uma avaliação crítica de como evidências digitais contidas, por exemplo, em redes sociais, contribuem com a atividade de investigação

criminal e, do ponto de vista epistêmico, com a busca da verdade – um dos objetivos do processo penal moderno.

O olhar crítico recairá precisamente no âmbito da *quaestio iuris*. Conforme se verá, a despeito do potencial epistêmico apontado, o problema reside em localizar no ordenamento jurídico brasileiro disposição que tipifique e discipline o procedimento para a coleta das sobreditas evidências digitais, incluindo a questão afeta à cadeia de custódia para a produção desses elementos probatórios.

Traçadas as linhas gerais pelas quais se pretende caminhar, a ideia consiste em partir de reflexões sobre uma situação concreta, ocorrida no dia 8 de janeiro de 2023, em Brasília, Distrito Federal. Fato amplamente noticiado pelos meios de comunicação, o que se observou foram cenas nas quais milhares de pessoas invadiram as sedes do Palácio do Planalto, do Congresso Nacional e do Supremo Tribunal Federal, com o propósito de promover uma ruptura democrática, mediante destruição de bens públicos e perpetração de centenas de fatos dotados de interesse criminal. À luz dos desafios probatórios que o sistema de justiça criminal enfrentou e ainda enfrenta para responsabilizar os envolvidos nos aludidos eventos é que os aspectos teóricos serão debatidos.

Adota-se, neste estudo, o método de abordagem hipotético-dedutivo, partindo-se do acervo teórico e empírico já consolidado sobre as evidências digitais e o avanço das investigações penais que as envolvem. Busca-se, assim, não apenas identificar padrões a partir de generalizações empíricas, mas também propor aportes conceituais que contribuam para a construção teórica e normativa sobre a temática.

Por sua vez, o método de procedimento eleito é o monográfico, para aprofundar o estudo sobre as provas digitais e os métodos de garantia de sua fiabilidade, utilizando-se como contexto a análise das investigações criminais desenvolvidas no marco dos atos antidemocráticos que ocorreram no dia 8 de janeiro de 2023. O método de interpretação é o sistemático, pois se observa o fenômeno a partir de um olhar sistêmico e holístico acerca do tratamento das provas digitais pelo ordenamento jurídico brasileiro, contando-se, ainda, com aportes de outros campos do conhecimento.

A técnica de pesquisa empregada consiste em revisão bibliográfica sistemática, com seleção e análise avaliativa e qualitativa de obras, trabalhos, documentos e julgados da área jurídica, somadas à interlocução com outras áreas do conhecimento, como a epistemologia, com a finalidade de desenvolver uma compreensão ampla e interdisciplinar acerca das problematizações enfrentadas. Consoante destacado, a partir de um evento, do ponto de vista histórico, recente, além de algumas premissas teóricas e gerais definidas, a ideia é explorar e construir soluções para as dificuldades probatórias enfrentadas na coleta de determinadas provas digitais, tarefa esta preponderantemente indutiva.

Giampaoli, Anderson Pires; Moraes, Rafael Francisco Marcondes de; Silva, Roberta de Lima e. Devida investigação criminal: compromissos epistêmicos e probatórios na extração de dados pessoais em fontes abertas.
Revista Brasileira de Ciências Criminais. vol. 211. ano 33. p. 115-141. São Paulo: Ed. RT, nov./dez. 2025.
DOI: [https://doi.org/10.5281/zenodo.17058359].

2. Ponto de partida: os ataques de 8 de janeiro de 2023

O dia 8 de janeiro do ano de 2023 figurará nos livros de história da República Federativa do Brasil[4]. A invasão violenta às sedes dos três Poderes, em Brasília, representou um atentado dirigido à ruptura da jovem democracia brasileira. No entanto, graças à atuação das instituições não corrompidas do controle formal do fenômeno criminoso – seja do sistema de segurança pública, seja do sistema de justiça criminal –, resistiu e, hoje, espera-se que esteja mais fortalecida[5].

É interessante notar que o ocorrido não será apenas retratado pelos historiadores, pesquisadores de fatos e acontecimentos passados. Os atores dos sistemas de segurança pública e justiça criminal, ao percorrerem os formais procedimentos previstos em leis, também são responsáveis, resguardados os direitos e as garantias dos envolvidos, pela correta determinação dos fatos, é dizer, pela reconstrução daqueles acontecimentos objetivos que não se repetirão, tudo com escopo de aplicar, uma vez provadas as condutas, a lei penal apropriada[6].

Pois bem, dois anos após o sucedido, a Corte Constitucional brasileira, também incumbida em algumas hipóteses pela jurisdição penal, divulgou um relatório em que retratou, ainda que de modo parcial, os resultados das atividades de persecução criminal desenvolvidas em relação aos eventos mencionados (Brasil, 2025)[7].

---

4. Embora as narrativas a respeito dos atos antidemocráticos do dia 8 de janeiro de 2023 ainda estejam em aberto, adota-se, neste trabalho, a perspectiva da análise realizada pelo editorial do *Boletim IBCCRIM* de fevereiro de 2024, no qual se atestou que: "Uma semana depois da festa cívica que coroou o exercício da vontade popular por meio do voto secreto, universal e periódico, o país sofreu o pior ataque da história da República inaugurada em 1988. Diante do mais duro golpe à democracia, feroz ao atingir o âmago de suas simbólicas instituições, os líderes de Poderes correram para tomar as medidas mais eficazes a socorrê-las e à população como um todo. A democracia sofreu um ultraje tão covarde quanto inacreditável" (Instituto Brasileiro de Ciências Criminais, 2024, p. 2).
5. O trabalho de Vik Muniz representa esses acontecimentos de forma expressiva. A partir dos destroços arrecadados e fruto das condutas perpetradas pelos responsáveis pela invasão, o artista transformou os cacos da tragédia em uma obra de arte (Brasil, 2024).
6. A menção aos historiadores não é por acaso: tanto o direito como a história são consideradas ciências ideográficas, ou seja, ramos do conhecimento que objetivam investigar eventos únicos e irrepetíveis. Nessa linha de raciocínio e guardadas algumas diferenças, a verdade judicial é uma espécie de verdade histórica. Nesse sentido: Gascón Abellán (2010, p. 105-107) e Ferrajoli (2010, p. 54).
7. O levantamento veicula informações não apenas a respeito de condenações, mas também de soluções penais de consenso, medidas cautelares pessoais, probatórias e de caráter patrimonial, entre outras (Em dois [...], 2025).

Segundo consta do citado documento, na perspectiva da dogmática penal, até janeiro do corrente ano, um total de 898 réus foram responsabilizados criminalmente, dos quais 371 receberam um decreto condenatório de pena privativa de liberdade reconhecendo a prática de crimes graves (e.g., artigos 288, parágrafo único, 359-L e 359-M, todos do Código Penal) ou de delitos mais simples (e.g., artigos 286, parágrafo único, e 288, *caput*, ambos também do Código Penal). Por outro lado, 527 envolvidos foram sancionados com reprimendas alternativas, resultado da celebração de acordos de não persecução penal (ANPP), mecanismos do denominado sistema penal premial-negociado (Moraes, 2022, p. 584).

Para atingir os números indicados, além das custódias cautelares (milhares de prisões em flagrante delito e preventivas), centenas de providências caracterizadas como meios de obtenção de prova foram autorizadas. Para ilustrar, foram expedidos 382 mandados de busca e apreensão e determinados 488 afastamentos de sigilos bancário e/ou telemático (Brasil, 2025). Ainda na seara processual e probatória, consta do sobredito relatório que até o dia 7 de janeiro deste ano foram realizadas pouco mais de mil audiências de instrução, oportunidade em que foram ouvidas 2.379 testemunhas de acusação, 1.366 testemunhas de defesa e 1.092 réus (Brasil, 2025)[8].

Colacionados alguns dados da atividade persecutória fruto das condutas delituosas perpetradas no dia 8 de janeiro de 2023, a questão que se lança, mormente em função dos tópicos e recortes propostos é: para além dos meios de prova e de obtenção de prova supraindicados, de quais outros elementos de prova[9] o sistema de justiça criminal se valeu (ou poderia se valer) para aplicar (e ainda aplicará) a

8. Tais números demonstram de que, a despeito dos avanços no campo probatório pericial e digital, o sistema de justiça criminal ainda consubstancia o reino das provas dependentes da memória. Nesse sentido: Instituto de Defesa do Direito de Defesa (2022, p. 6).

9. Entre as diversas acepções do vocábulo "prova", considera-se aqui meio de prova o instrumento por intermédio do qual a prova é introduzida no processo (e.g., prova testemunhal, pericial, documental etc.). Por outro lado, os meios de obtenção de prova são recursos para a coleta de fontes de prova ou de elementos probatórios (e.g., busca e apreensão, quebras de sigilo etc.). Os primeiros servem diretamente ao convencimento da autoridade judiciária a respeito da veracidade ou falsidade de algo que se afirma sobre os fatos objeto da persecução; já os segundos se prestam apenas de maneira indireta à convicção do Estado-juiz, pois dependem do resultado da atividade probatória desencadeada. Também de interesse para o presente trabalho é o significado de fonte de prova, entendida como tudo o que é apto a oferecer um resultado passível de apreciação pelo julgador (e.g., um documento, uma testemunha, a arma do delito etc.). Por fim, os elementos de prova correspondem aos dados brutos extraídos das fontes de prova e que ainda não foram valorados pelo magistrado de forma devida (e.g., o testemunho prestado, o laudo pericial redigido e juntado aos autos etc.) (Badaró, 2020, p. 431-433).

lei penal nos casos concretos, seja por intermédio de uma sentença penal condenatória, seja graças a ajustes entabulados entre a acusação e a defesa? Essa é uma resposta que o presente ensaio buscará delinear nas linhas seguintes. Todavia, antes de procurar responder à sobredita indagação, faz-se necessário expor algumas premissas teóricas que servirão de ponto de partida.

3. Bases modernas e mínimas do contexto da devida investigação criminal

O processo penal moderno é interdisciplinar (Giampaoli, 2024, p. 97). Não se pode mais conceber que a dogmática processual penal seja autossuficiente para alcançar os objetivos indicados no tópico anterior, vale rememorar: aplicar a lei penal no caso concreto, assegurar o respeito aos direitos e garantias fundamentais e buscar a verdade possível[10]. Nesse diapasão, ainda que o operador do direito tardiamente venha reconhecendo essa indispensável interdisciplinariedade[11], outros saberes extrajurídicos, como a epistemologia, têm muito a contribuir.

Enquanto ramo do conhecimento atrelado à filosofia, entre outras contribuições, a epistemologia ajuda os atores do sistema de justiça criminal na justificação daquilo que se afirma sobre os fatos de interesse penal, auxiliando nos processos decisórios, máxime daqueles que têm a responsabilidade de condenar ou absolver pessoas (Matida; Herdy, 2016, p. 209). Graças à epistemologia, adjetivada de aplicada ou judiciária, é possível uma melhor compreensão do que é prova, como ela se estrutura e o que a torna mais confiável (Badaró, 2019, p. 134).

Não por outra razão, a convergência entre os avanços nos estudos sobre a estrutura processual e os aportes dos filósofos do direito dedicados à teoria do conhecimento sedimentou um vasto caminho para concluir que o processo penal deve ser poroso à verdade dos fatos (Matida; Nardelli; Herdy, 2020b). Tal perspectiva lançou luz sobre um infinito até então relegado às sombras: sua dimensão epistêmica.

10. O processo penal deve se preocupar com a reconstrução histórica do ocorrido (juízo sobre os fatos), a correta interpretação e aplicação da lei criminal aos fatos (juízo de direito) e a adequada atuação do instrumento processual, o que implica respeito a direitos e garantias das partes envolvidas. Nessa linha: Badaró (2019, p. 21-22).

11. Exemplo disso está no julgamento do Habeas Corpus 598.886. Ao prestigiar aportes da psicologia do testemunho e cognitiva, o Superior Tribunal de Justiça, por intermédio da 6ª Turma e sob a relatoria do Ministro Rogerio Schietti Cruz, conferiu nova interpretação ao artigo 226 do Código de Processo Penal, alterando entendimento até então sedimentado a respeito do reconhecimento de pessoas enquanto meio de prova (BRASIL, 2020b). Após a referida decisão, de outubro de 2020, outras vieram, incluindo do Supremo Tribunal Federal, consolidando a viragem interpretativa. Fruto das contribuições da psicologia e da nova jurisprudência, o Conselho Nacional de Justiça editou a Resolução 484, de 22 de dezembro de 2022 e admitiu ser irrepetível o referido meio de prova (Brasil, 2022b).

Afinal, apesar das regras procedimentais e dos princípios que orientam o devido processo, a essência da dinâmica processual reside, fundamentalmente, na locução "buscar conhecer".

Avançando um pouco mais, é certo que no âmago do processo desenvolve-se a instituição probatória, cujo objetivo é demonstrar a efetiva ocorrência dos fatos que condicionam determinada consequência jurídica. Seu êxito se verifica quando os enunciados sobre os fatos provados correspondem à verdade, isto é, àquilo que efetivamente ocorreu no mundo. Assim, pode-se sustentar que a função primordial da prova é determinar a verdade fática, permitindo a incorporação das devidas proposições ao raciocínio decisório.

Nada obstante, o impulso epistemológico sentido pelo processo penal não deve limitar-se à fase processual; a filtragem epistêmica proposta pela epistemologia jurídica (Matida; Nardelli; Herdy, 2020a) precisa igualmente alcançar a investigação preliminar dos fatos, uma vez que, com frequência, o elemento probatório valorado pelo juiz no julgamento de hoje foi descoberto ou produzido na investigação de ontem (Matida; Moscatelli, 2023, p. 99).

Isso posto, e raciocinando a partir de um olhar hodierno do legítimo instrumento do *ius puniendi* estatal, há que se reconhecer que a investigação preliminar não pode mais ser considerada mera etapa pré-processual, estranha ao devido processo penal e unilateralmente voltada a subsidiar eventual ação criminal em juízo (Marques, 2000, p. 61). Cuida-se, em realidade, de procedimento extrajudicial submetido, como pressuposto de validade, ao regime jurídico de garantias próprio da seara processual penal (Moraes, 2025, p. 39).

A investigação criminal ou, na perspectiva epistêmica, o contexto da descoberta (Ubertis, 2021, p. 29-30), integra o devido processo penal[12]. O suspeito da prática de conduta ilícita penal é reconhecido como detentor e sujeito de direitos e garantias fundamentais[13] pela Constituição Federal e por diversos instrumentos de proteção de direitos humanos. Daí a necessidade, na atualidade, de uma devida investigação criminal – como defendem Coelho (2017, p. 47), Baldan (2015, p. 165) e Moraes (2025, p. 80-81) –, com uma série de implicações discutidas nos itens subsequentes.

---

12. Reconhecendo a importância da investigação criminal para a resolução dos casos penais, *vide* Prado (2024, p. 358) e Saad (2024). Ademais, pensando a investigação criminal como parcela essencial da atividade jurisdicional (*nullum iudicium sine investigatione*), *vide* Pereira (2022, p. 65).

13. Aqui a razão de uma interpretação ampliativa da expressão "acusado" em geral, do artigo 5º, inciso LV, da Constituição Federal, a abarcar todo imputado em sentido amplo, seja ele suspeito, indiciado ou réu. Nesse sentido: Saad (2004, p. 234-235).

Todas essas questões levantam outro ponto importante a respeito da moderna concepção de processo penal. Além de constatar que o eixo gravitacional de toda a persecução penal está voltado para a investigação preliminar e que já nessa etapa há incidência de direitos e garantias, com o aporte de conhecimentos oriundos de outros ramos do saber como a epistemologia, é essencial assentir que, atreladas às questões jurídicas (*quaestio iuris*), que demandam interpretação da lei, há questões de fato ou de mundo (*quaestio facti*), pouco conhecidas e exploradas pelos operadores e personagens do sistema de justiça (González Lagier, 2020, p. 11-13)[14].

Para melhor compreensão dessas assertivas, toma-se como referência o ocorrido no dia 8 de janeiro de 2023. Analisar referidos acontecimentos na perspectiva que ora se propõe viabilizará avançar nos tópicos seguintes.

Em consonância com os números apresentados e considerando tudo o que se noticiou a respeito dos fatos sucedidos no Distrito Federal, não é difícil imaginar como a atividade de investigação criminal demandou um esforço enorme para identificar autores, estabelecer eventuais vínculos entre eles, individualizar suas condutas, descrever os acontecimentos e angariar elementos de prova que permitissem delimitar as hipóteses que no futuro servissem como base da pretensão acusatória, inaugurando, assim, a fase judicial do devido processo.

Observe-se, nesse diapasão, que para conferir uma definição jurídica aos fatos pretéritos (e.g., artigos 286, 288, 359-L e 359-M, todos do Código Penal) é

14. Reconhecer a importância das leis e da hermenêutica é fundamental, porém não se pode atribuir às questões jurídicas um *status* mais elevado do que aquele dado às questões que versam sobre o juízo de fato. As faculdades de direito não podem e não devem ser apenas escolas das leis. Nessa toada: Badaró (2019, p. 83-84). Não se ignora, contudo, que a tradicional distinção feita pelos juristas entre *quaestio facti* e *quaestio iuris* não é tão clara quanto parecia. Nada obstante, algo persiste dessa bipartição e se trata de aspecto muito importante. Nas palavras de González Lagier (2025, p. 56-58), "a prova dos fatos externos, nos quais se baseiam as diferentes interpretações sobre as quais, por sua vez, operará a qualificação jurídica; subsiste, ainda, a prova dos fatos interpretados descritivamente [...] Quais são as consequências do enfraquecimento (ou melhor: da reelaboração) da distinção? Parece-me que a consequência mais imediata é se perceber que na argumentação em matéria de fatos, aquilo que é puramente fático e o normativo se entrecruzam, sem que isso, todavia, acarrete que a argumentação sobre os fatos seja indistinguível da argumentação sobre o Direito. Como escreveu Comanducci, 'afirmar que na motivação sobre fatos também há juízos sobre o Direito e vice-versa não implica negar que haja diferenças entre a argumentação e a motivação sobre os fatos e sobre o direito'". Na argumentação sobre fatos, questões normativas e fáticas se entrecruzam, contudo, a premissa teórica da qual se parte reconhece que a argumentação sobre o direito confere razões a favor de uma conclusão justa ou válida; já a argumentação sobre fatos trata de dar suporte que apoie uma conclusão segundo a qual a proposição ou o enunciado fático é verdadeiro ou provável. Nessa perspectiva: Comanducci (1992, p. 224).

necessário, a princípio, provar que tais fatos ocorreram, verificar hipóteses de sua realização ou, na ausência de um conjunto probatório mínimo (justa causa), excluir hipóteses anteriormente vislumbradas[15].

À referida tarefa no curso da devida investigação dá-se o nome de abdução, raciocínio pelo qual, a partir dos fatos e das fontes de prova disponíveis, o policial produz razões epistêmicas[16] que permitirão formular tantas hipóteses quanto forem necessárias para reconstruir o ocorrido e encontrar a melhor explicação para os acontecimentos[17] apurados.

Ocorre que, ao contrário de um fato isolado e penalmente relevante com um único autor, os ataques de 8 de janeiro de 2023 articularam milhares de episódios sucessivos, bosquejados e potencialmente capitulados como infrações penais diversas, além de diversos indivíduos responsáveis pela mobilização para o cometimento de tais atentados criminosos.

Nessa linha de pensamento, tal como delimitado antes, foi importante a agência de polícia judiciária ouvir pessoas (testemunhas, vítimas e suspeitos) e se valer de meios de obtenção de prova, como o afastamento de sigilos e a busca e apreensão. Por óbvio, isso não é suficiente, demandando dos responsáveis pela apuração um esforço investigativo maior, de modo a encontrar outras ferramentas ou instrumentos eficazes para a produção de um conhecimento ou, se quiser, um conjunto probatório que permita justificar proposições fáticas (juízo sobre os fatos), apto a conferir suporte à qualificação jurídica dada a esses enunciados. Por exemplo, a constatação de que os indivíduos A, B, C, D e E associaram-se (artigo 288, *caput*, do Código Penal) para o fim específico de cometer o delito de abolição violenta do estado democrático de direito (artigo 359-L do Código Penal).

A partir desse caso, é possível verificar como já na etapa extrajudicial do devido processo penal são coligidos e produzidos elementos probatórios aptos não apenas a lastrear a peça acusatória, mas também a servir como elementos de convicção e de

15. Para maior detalhamento da concepção mais robusta de justificação epistêmica sob uma perspectiva evidencialista, cujo enfrentamento escapa aos limites deste trabalho, *vide* Aguilera García (2022).

16. Sob o olhar da epistemologia, razões epistêmicas, elementos de prova, indícios, indicadores da verdade e evidências são expressões sinônimas. A preocupação, conforme se procura demonstrar, é muito mais com as questões de fato (*quaestio facti*) do que com as questões de direito (*quaestio iuris*). Assim, não há uma preocupação com os rótulos que o ordenamento jurídico, a jurisprudência ou a doutrina dão ao dado bruto que se extrai de uma fonte de prova.

17. Defendendo a abdução enquanto espécie de raciocínio desenvolvido na etapa de investigação preliminar: Badaró (2019, p. 152), Moscatelli (2023, p. 125-155) e Aguilera García (2020, p. 43).

Giampaoli, Anderson Pires; Moraes, Rafael Francisco Marcondes de; Silva, Roberta de Lima e. Devida investigação criminal: compromissos epistêmicos e probatórios na extração de dados pessoais em fontes abertas.
Revista Brasileira de Ciências Criminais. vol. 211. ano 33. p. 115-141. São Paulo: Ed. RT, nov./dez. 2025.
DOI: [https://doi.org/10.5281/zenodo.17058359].

justificação da racional decisão proferida pelo Estado-juiz ao final da fase judicial, oportunidade em que a lei penal será aplicada[18-19]. Nesse panorama, de reconstrução do fato e busca da verdade para a justa aplicação da dogmática penal, tudo com respeito aos direitos e garantias das partes, é que se concebe o sistema de justiça criminal como um verdadeiro motor epistêmico (Laudan, 2013, p. 23)[20].

Fixadas as premissas teóricas, retomadas nos próximos tópicos, oportuno passar para a análise de algumas ferramentas ou instrumentos epistemicamente úteis para a investigação penal, sem deixar de problematizar a questão.

4. *Big data*, fontes abertas e agregadores de dados: dimensão epistêmica das ferramentas disponíveis à persecução penal

Parte do *big data*[21] compreende uma massa de dados e informações (volume) que se encontra disponível àqueles que utilizam, por exemplo, a rede mundial de computadores[22]. Também alberga quão rápido essas informações e dados são

18. Anota-se que, para além das denominadas provas irrepetíveis, produzidas na fase de investigação e levadas para etapa judicial (e.g., exames periciais), a Corte Constitucional brasileira, nos autos das Ações Diretas de Inconstitucionalidade de números 6.298, 6.299, 6.300 e 6.305, decidiu que os autos do inquérito policial acompanham a peça acusatória e, portanto, integram a ação penal, devendo ser valorados pela autoridade judiciária competente (Brasil, 2023).
19. Não se olvida da redação do artigo 155 do Código de Processo Penal, que não considera propriamente prova os elementos produzidos na etapa extrajudicial da persecução penal, ao empregar a expressão "elementos informativos", na essência, atribuída aos testemunhos prestados em sede policial, a partir de subjacente ideia de que seriam pretensamente repetíveis em juízo, a despeito da maleabilidade e da irrepetibilidade do conteúdo da memória humana, indicadas por saberes de áreas como a psicologia do testemunho. Contudo, conforme referencial teórico adotado e demais premissas e exemplos tratados nos tópicos subsequentes, a perspectiva dos autores é distinta, mormente pelo interesse principal em permear as questões de fato (*quaestio facti*). Para uma nova visão acerca do contexto da investigação criminal: Moraes (2025, p. 211-219).
20. Conceber o sistema de justiça criminal como tal implica afirmar, também na perspectiva epistêmica, que a regra geral e regente da prova é o princípio da liberdade probatória ou *total evidence principle*. Nesse sentido: Ferrer-Beltrán (2021, p. 63), Taruffo (2016, p. 165) e Badaró (2019, p. 54).
21. O presente trabalho limita-se ao tratamento dos dados públicos, disponíveis em fontes abertas, na etapa de investigação preliminar dos fatos. Quanto aos dados privados que podem ser objeto de infiltração informática por *malware*, por exemplo, reporta-se a Mendes (2018).
22. Enquanto os dados representam o material bruto descoberto, as informações retratam o tratamento conferido àquele material. Portanto, uma vez organizados e dotados de significado e compreensão, os dados se transformam em informações (Caselli, 2023, p. 44).

disponibilizados aos usuários (velocidade). Outrossim, abarca a grande quantidade de fontes de onde provêm (variedade). Não se pode olvidar ainda a necessidade de verificar a autenticidade deles (veracidade). Por fim, há que se estimar a valia das informações e dados coletados (valor). A esse conjunto de características dá-se o nome de *Vs de big data* (Caselli, 2023, p. 45).

Por outro lado, considerando o recorte inicial proposto – isto é, os fatos ocorridos no dia 8 de janeiro de 2023 e as correlatas repercussões nos meios de comunicação e principalmente nas redes sociais[23] –, fica fácil imaginar como essas plataformas serviram (ou poderiam servir) de fontes de prova àqueles encarregados da atividade de investigação e instrução[24]. No citado ano, o *Facebook* tinha 2,1 bilhões de usuários; o *X*, antigo *Twitter*, contava com cerca de 528,3 milhões de usuários; já o Instagram estima ter mais de 1,44 bilhão de usuários em 2025 (Influencer Marketing Hub, 2025).

Imagine-se, nessa linha de pensamento, como milhares desses usuários, por intermédio de postagens com textos, imagens ou vídeos, não documentaram suas atividades quando se encontravam na Praça dos Três Poderes, sejam esses registros meras capturas daquilo que ocorria no local, sejam retratos de condutas posteriormente capituladas nos dispositivos penais supramencionados.

A questão que se coloca, embora já se possa projetar o valor epistêmico de tais dados e informações para os encarregados da investigação, é como processar todo esse volume de conhecimento não estruturado e heterogêneo. Pode-se dizer que manual e individualmente tal atividade resta inviável.

---

23. Segundo Barreto e Wendt (2024, p. 97), à inteligência empregada por agentes estatais ou particulares para angariar e analisar dados e informações disponíveis em mídias sociais dá-se o nome de *social media intelligence* (Socmint ou SMI). Referido termo, empregado para atividades realizadas nas mídias sociais, deriva da expressão *open source intelligence* (Osint), mais abrangente. Importante ressaltar que as técnicas de Osint contribuem com a investigação e com o processo de tomada de decisões, interessando, para o presente estudo, as atividades desenvolvidas pelos órgãos a serviço da persecução penal estatal. Como as informações e dados obtidos têm a sua origem, como regra, em fontes abertas, as referidas atividades não abrangem tarefas que esbarram em limitações legais e cláusulas de reserva jurisdicional (e.g., quebras de sigilo de *e-mails*, aparelhos multifuncionais, *hacking* etc.). Nessa toada: Camargo (2022, p. 103).

24. Investigar é pesquisar, ou seja, buscar informações e fontes de prova que permitam elucidar um fato; instruir, por outro lado, é transformar essas informações ou fontes de prova em elementos probatórios, aptos a auxiliar as partes processuais e a autoridade judiciária na correta determinação dos fatos. A concepção que se adota neste trabalho, conforme já ressaltado, é que a devida investigação penal abarca tanto os atos de investigação quanto os de instrução. Nessa perspectiva: Saad (2004, p. 164-167).

Giampaoli, Anderson Pires; Moraes, Rafael Francisco Marcondes de; Silva, Roberta de Lima e. Devida investigação criminal: compromissos epistêmicos e probatórios na extração de dados pessoais em fontes abertas.
Revista Brasileira de Ciências Criminais. vol. 211. ano 33. p. 115-141. São Paulo: Ed. RT, nov./dez. 2025.
DOI: [https://doi.org/10.5281/zenodo.17058359].

Para tanto, os atores dos sistemas de segurança pública e de justiça criminal (agências de polícia judiciária) dispõem daquilo que se designa *knowledge discovery databases*, também conhecido como mineração ou raspagem de dados (*web scraper*)[25]. Referida atividade permite arrecadar os dados no seu formato original (aquisição), organizá-los para um algoritmo (análise), separar o que é aproveitável daquilo que não é (filtro), aplicar operações estatísticas (exploração), planejar como o resultado será apresentado (representação), contextualizar os dados (refino) e aplicar filtros para obtenção de informações detalhadas (interação) (Caselli, 2023, p. 47-49).

Pois bem, todo esse processo deve ser operacionalizado, e para isso o agente responsável conta com ferramentas intituladas agregadores de dados ou *analytics*[26-27]. Entre elas, pode-se citar *o TweetDeck*, o *Snscrape*, o *Talkwalker*, o *Brandwatch*, o *Power BI*, o *Mention* e o *Snap*. O primeiro é uma ferramenta gratuita do Twitter que permite monitorar diversas *timelines* em tempo real, possibilitando acompanhar menções e *hashtags*. Já o segundo, um produto da *Python*, consegue angariar dados do *Twitter*, *Facebook* e *Instagram*. O terceiro auxilia no monitoramento de mídia

25. Os termos "mineração" e "raspagem", para os fins deste trabalho, são tratados como sinônimos. Tanto o *data mining* (mineração de dados) quanto o *web scraper* (raspagem de dados) são responsáveis pela coleta de um grande volume de dados e informações de *sites*, plataformas da *web* e mídias sociais, material posteriormente tratado, organizado e armazenado em diversos tipos de formato. Dotado de valor e compreensão, tal material subsidia o tomador de decisão (Caselli, 2023, p. 50-52).

26. Importante, nesse ponto, diferenciar atividade de inteligência, de segurança pública e de persecução penal. Conforme se observa, a mineração ou raspagem podem ser utilizadas para qualquer um dos três fins: inteligência, segurança e persecução. O critério utilizado neste ensaio para distinguir referidas atividades centra-se no perigo. A inteligência atua antes da segurança pública e não exige qualquer situação de perigo, ou seja, a inteligência não age. A persecução também opera nessa lógica, pois não está vinculada a perigos, mas a suspeitas. Entretanto, diferente da inteligência, na atividade de persecução, há pesquisa, investigação e instrução e, portanto, o agir é essencial a esse tipo de tarefa. Por fim, justamente o que caracteriza a segurança pública é o perigo, ou seja, existem ações estatais que objetivam à proteção da coletividade contra perigos, atuações que afetam determinados destinatários, em regra, no âmbito constitucionalmente tutelado. Nessa linha de pensamento: Gleizer, Montenegro e Viana (2021, p. 81-82). Depreende-se do exposto que o recorte do artigo é direcionado para a atividade de persecução.

27. A utilização de ferramentas analíticas, mormente diante da evolução dos computadores e do incremento da capacidade de armazenamento e tratamento de dados nos últimos trinta anos (fenômeno *big data*), não é atividade de interesse apenas das agências do controle formal do fenômeno criminal, mas também de outras instituições públicas e privadas que objetivam monitorar e controlar as atitudes e os comportamentos dos cidadãos (Camargo, 2022, p. 28).

social e no estudo de dados para identificar tendências em tempo real. O *Brandwatch*, por sua vez, é uma plataforma de análise de mídia social que permite o acompanhamento de conversas *on-line* para pesquisas de mercado. Quanto ao *Power BI*, cuida-se de ferramenta que transforma dados e informações em recursos visuais, o que se dá com a utilização de instrumentos avançados de análise de dados, recursos de inteligência artificial e criação de relatórios. O *Mention* é um programa de monitoramento de mídia social que permite o rastreio a partir de menções a palavras-chave específicas em tempo real. Por fim, o *Snap*, uma ferramenta forense utilizada pelas agências policiais e órgãos de inteligência, possibilita contínua atualização e verificação de vínculos a partir de múltiplas bases de dados em uma única interface.

Para ilustrar quanto esses agregadores ou *analytics* podem colaborar com as instituições do controle formal do fenômeno criminoso, no âmbito do *Instagram*, tem-se o *Instagram-scraper*, o *Instagram-follower-scraper* e o *Instaloader* (Caselli, 2023, p. 477). O primeiro é um *script* público escrito em linguagem Python, que possibilita obter dados de postagem e seus comentários, além de pesquisar por geolocalização e *hashtags*. O segundo permite baixar uma lista descritiva das pessoas que um determinado perfil pesquisado segue, além dos seus próprios seguidores. Já o terceiro viabiliza a mineração de dados simples e complexos (comentários, mídias, postagens, geolocalização, *hashtags*, entre outros), associando-os.

Delimitadas algumas ferramentas que possibilitam àquele que pesquisa e se encarrega de instruir a investigação de atos complexos, como os relativos aos ataques de 8 de janeiro de 2023, é viável pensar no potencial epistêmico desses instrumentos e de como o resultado obtido a partir do uso dos mencionados agregadores contribui com a reconstrução e a determinação dos fatos de interesse penal. Identificar autores, coautores e eventuais ajustes prévios entre diversas pessoas, além de individualizar condutas daqueles que estiveram em Brasília no 8 de janeiro, registrando os seus próprios atos e de terceiros para, na sequência, divulgá-los nas mídias sociais, são apenas alguns exemplos de como a mineração ou raspagem de dados e informações auxiliam o sistema de justiça criminal na consecução de sua missão constitucional.

Para concluir o presente tópico e passar para a questão ligada à natureza jurídica desses instrumentos e indícios produzidos graças às mencionadas ferramentas digitais, não se pode deixar de esclarecer que a premissa da qual se parte é a seguinte: essas informações e dados, mais tarde convertidos em elementos probatórios, estão livremente dispostos, nesse caso, nas mídias sociais. Não se trata, portanto, de algo protegido ou negado, cujo titular do direito nutre uma expectativa de privacidade. Em outras palavras, este estudo concentra-se nas chamadas fontes abertas[28],

28. De forma simples, fontes abertas são aquelas sem impedimentos para obtenção e coleta de dados e informações, daí a ideia de expectativa de publicidade do titular do direito (e.g.,

nas quais há uma disponibilidade com dados ou informações acessíveis a qualquer pessoa, projetadas pelo detentor da informação em caráter de publicidade (Jorge Jr.; Jorge, 2020, p. 53). Isso é importante consignar, pois repercute no âmbito da *quaestio iuris*.

5. Natureza jurídica das razões epistêmicas coletadas: o problema do vácuo legislativo

Retomando um tema para que se possa avançar no debate, foi dito que "prova" é uma palavra polissêmica. Interessa aqui discorrer um pouco mais sobre a diferença classificatória entre meio de prova e meio de obtenção de prova, delimitando, assim, o produto final (elemento probatório, razão epistêmica, evidência, indicador de verdade ou indício) apto a ser valorado pelo Estado-julgador.

Uma primeira distinção, já indicada, diz respeito à valoração, direta ou indireta, pela autoridade judiciária. Os meios de prova são considerados instrumentos por intermédio dos quais a prova é inserida no processo e são objeto de valoração direta pelo magistrado. Por sua vez, os meios de obtenção de prova seriam responsáveis pela coleta de fontes de prova ou de elementos de prova e serviriam apenas indiretamente ao juiz, pois dependem do resultado da atividade probatória desenvolvida.

Avançando, costuma-se dizer e catalogar, não sem controvérsias, que os meios de prova configuram uma atividade endoprocessual (Badaró, 2017), porquanto exercida com contraditório real pelas partes (contraditório para a produção da prova); já nos meios de obtenção de prova, a atividade probatória é extraprocessual, por isso haveria um contraditório diferido (contraditório sobre a prova produzida) (Dezem, 2020, p. 595). E mais, nos meios de prova, a produção não afeta o direito das partes, tendo elas conhecimento prévio da sua realização; já nos meios de obtenção, há afetação do direito das partes e a presença de um fator surpresa na sua produção. Por fim, diante das diferenças apontadas, enquanto os primeiros são regidos por um princípio de liberdade, os segundos devem ser geridos por um princípio de legalidade estrita.

Há, aqui, o ponto fulcral deste trabalho. Pensando nas atividades de pesquisa e de instrução explicitadas no tópico anterior, a partir de casos complexos como aquele dos ataques de 8 de janeiro, tende-se a considerar que a mineração e raspagem com a utilização de agregadores (*knowledge discovery databases*) constituem

jornais, redes sociais, portais de domínio público etc.). Por outro lado, fontes fechadas correspondem àqueles dados e informações negados ou protegidos, daí a ideia de expectativa de privacidade do titular do direito (e.g., dados bancários, fiscais e telefônicos). Nesse sentido: Caselli (2023, p. 34-35), Barreto e Wendt (2024, p. 6).

meios de obtenção de prova, a serem disciplinadas, via tipificação e procedimento, por lei própria (princípio de legalidade estrita).

A indagação que se faz nessa linha de pensamento é: existe essa regulamentação em território nacional? A resposta é negativa. Tem-se, portanto, um problema legal e jurídico, é dizer, algo a ser solucionado pela *quaestio iuris*. De fato, no que tange às provas digitais, inexiste lei ordinária específica disciplinadora de hipóteses de restrições aos direitos fundamentais. Observa-se um arranjo mediante composição de um conjunto de disposições normativas esparsas para obtenção e utilização desse tipo de evidência probatória eletrônica (Pitombo, 2024, p. 40-42).

Dentro dos recortes propostos, a atividade probatória e epistêmica[29] objeto de discussão se dá no interior do contexto da investigação, tendo como origem fontes abertas. Isso quer dizer que as informações e os dados coletados e tratados a partir das mídias sociais são dotados de um potencial epistêmico e estão aptos a auxiliar na justificação daquilo que se afirma sobre os fatos de interesse penal. Em outras palavras, toda essa atividade que colabora com a busca da verdade possível e a aplicação da lei penal, dois dos objetivos do processo penal, esbarra no respeito aos direitos e garantias fundamentais dos sujeitos investigados, o qual figura também como um dos fins da atividade de persecução estatal.

O tratamento massivo de dados pessoais por intermédio do emprego de algoritmos e inteligência artificial reclama não apenas um fortalecimento das garantias pensadas no modelo processual penal liberal, mas possivelmente a criação de novos mecanismos de proteção ao cidadão (Bachmaier Winter, 2025).

Nessa conjuntura, conquanto a proteção de direitos fundamentais tradicionalmente tenha se voltado contra o exercício exacerbado do poder pelo Estado,

29. Este trabalho se compromete com o reconhecimento de uma dimensão epistêmica do processo, considerando-o, assim, um conjunto estruturado de atividades com o fim de obter elementos de conhecimento verídicos sobre os fatos relevantes para a solução da controvérsia. Nesse sentido, vincula-se a um "modelo epistemológico" do conhecimento dos fatos com base nas provas, cuja finalidade é a averiguação da verdade (possível), embora não seja esse o único fim perseguido pelo processo (Taruffo, 2016, p. 159-160). Isso posto, a extensão do raciocínio e das premissas eleitas refletem-se também na etapa da investigação preliminar dos fatos, em especial porque é durante a apuração do fato potencialmente criminoso que se cometem mais erros probatórios, sendo o processo judicial incapaz de corrigi-los posteriormente (Moscatelli, 2023, p. 134). Reconhece-se, assim, que "a investigação criminal é a pedra angular do sistema (Simon, 2012, p. 3), embora este tema seja pouco reconhecido nos debates acadêmicos e públicos. Portanto, é essencial que a agenda da epistemologia jurídica reflita compromissos sérios com o raciocínio probatório utilizado nessa fase penal (Aguilera, 2020, p. 21)" (Moscatelli, 2023, p. 134), visto que "um processo epistemicamente comprometido não pode fechar os olhos para a fase que o antecede e prepara" (Moscatelli, 2023, p. 130).

há um relevante acúmulo de poder pelo setor privado. Esse fenômeno ocorre notadamente nas empresas prestadoras de serviços de *internet* e de gestão de dados, o que demanda reavaliação para discutir a responsabilidade como garantidoras da privacidade dos usuários, além de obrigações previstas nas legislações de proteção de dados, assim como aprofundar seu papel como colaboradoras nas investigações criminais (Bachmaier Winter, 2025, p. 49-50).

No plano normativo brasileiro, a proteção dos dados pessoais, inclusive nos meios digitais, foi alçada expressamente a direito fundamental com a inserção, pela Emenda Constitucional 115/2022, do inciso LXXIX no artigo 5º da Carta Magna nacional. Além disso, a proteção de dados pessoais também encontra respaldo na legislação ordinária, em especial nos seguintes diplomas legais: Lei Federal 8.078/1990 (Código de Proteção e Defesa do Consumidor); Lei Federal 12.414/2011 (Lei do Cadastro Positivo); Lei Federal 12.527/2011 (Lei de Acesso à Informação); Lei Federal 12.965/2014 (Marco Civil da Internet); e Lei Federal 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD).

Quanto às duas últimas, tem-se que o Marco Civil da Internet prevê a proteção dos dados pessoais como princípio, a ser regido na forma de legislação específica (artigo 3º, inciso III). A LGPD, entretanto, não se aplica ao tratamento de dados pessoais para atividades de investigação criminal[30], encontrando-se pendentes iniciativas legislativas voltadas ao advento de uma LGPD penal[31].

Assim, outro questionamento exsurge: o que fazer para minimizar os potenciais efeitos deletérios do vácuo legislativo? E ainda, tendo em vista a lacuna de lei específica para regulamentar a produção dessa espécie de prova digital[32], qual é o papel

30. Prevê o artigo 4º, inciso III, alínea *d*, da Lei Federal 13.709/2018, *in verbis*: "Esta Lei não se aplica ao tratamento de dados pessoais: [...] III – realizado para fins exclusivos de: [...] d) atividades de investigação e repressão de infrações penais" (Brasil, 2018).

31. No final de 2020, foi apresentado ao então presidente da Câmara dos Deputados um anteprojeto de LGPD penal no final de 2020 (Comissão [...], 2020). Há, em paralelo e em tramitação no Congresso Nacional, o Projeto de Lei 1.515/2022, que também pretende cuidar de uma LGPD para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais (Brasil, 2022a). Existe também o Projeto de Lei 4.939/2020, que objetiva dispor sobre diretrizes do direito da tecnologia da informação e normas de obtenção e admissibilidade de provas digitais na investigação e no processo (Brasil, 2020a).

32. A própria Lei Geral de Proteção de Dados prevê a edição de um ato normativo específico. É o que diz o citado artigo 4º, § 1º, *in verbis*: "O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei" (Brasil, 2018).

dos atores e dos operadores do sistema de justiça criminal? Tais questões serão trabalhadas no tópico subsequente.

6. Cadeia de custódia da prova digital: autenticidade e integridade da *digital evidence*

Retomando as indagações do item anterior, é importante, antes de procurar respondê-las, acrescer algumas premissas complementares e recortes deste trabalho, essenciais para as considerações finais que virão adiante. Diferente de uma tradicional busca e apreensão – meio de obtenção de prova regulado entre os artigos 240 e 250 do Código de Processo Penal, no qual a atividade de persecução extrajudicial resulta na arrecadação de instrumentos, armas, drogas, documentos, entre outros –, a atividade de raspagem e mineração com o uso de agregadores, além de não ter previsão legal específica, converte-se em uma evidência digital (*digital evidence*).

Isso significa que a razão epistêmica, desde a sua coleta até o seu refino e representação, apresenta uma linguagem não natural, mas digital. Em outros termos, embora os referidos dados e informações digitais possam ser diretamente percebidos por todos aqueles que têm contato com eles, são desprovidos de uma materialidade imediatamente constatável (Badaró, 2023, p. 175).

Portanto, ao contrário daquelas fontes reais de prova, apreendidas graças aos típicos meios de obtenção, como a busca e a apreensão já indicadas (e.g., documentos, drogas, armas, cartas etc.), na *digital evidence,* as características de desmaterialização e dispersão tornam as razões epistêmicas localizadas no *big data* e nas mídias sociais facilmente alteráveis, sobretudo em razão da sua mutabilidade[33]. Daí a importância da preservação da cadeia de custódia, com destaque para os exemplos de atividade de persecução penal como a tratada neste artigo, em que o responsável pelos atos de pesquisa e posterior instrução e documentação é o próprio agente estatal encarregado da investigação policial[34].

33. Daí a preocupação também da doutrina italiana no sentido da necessidade de uma intervenção legislativa que regulamente a prova digital. Por todos: Daniele (2011, p. 284).

34. Interessante a proposta de Badaró para garantir a integridade da prova digital. Tema da denominada *computer forensics*, o emprego de instrumentos técnicos ou *tools* adequados permitem que a prova seja utilizada no processo. Exige-se assim: a individualização do suporte informático que contém o dado; a coleta por intermédio de técnica de interceptação ou mediante sequestro e cópia ou espelhamento do suporte onde está registrado o arquivo; a conservação dos dados obtidos e copiados em local apropriado e seguro; o exame dos dados devem se dar exclusivamente na cópia do suporte informático; a apresentação dos resultados em juízo deve ocorrer mediante a produção de prova pericial,

Disciplinada entre os artigos 158-A e 158-F da lei processual penal vigente[35], a cadeia de custódia consiste em um conjunto de procedimentos, todos eles concatenados, como elos de uma corrente, cujo objetivo é garantir a integridade, a legalidade e a confiabilidade da prova (Lopes Jr., 2021, p. 460). De outra forma, a cadeia de custódia deve ser compreendida como a sucessão encadeada de atos e pessoas que mantiveram qualquer tipo de contato com a fonte de prova, desde a sua coleta até a sua apresentação em juízo (Badaró, 2023, p. 183). Há que se exigir, para um controle epistêmico do resultado probatório, mesmidade e desconfiança (Prado, 2014). Respeitando o primeiro postulado, garante-se que a prova valorada pelo Estado-juiz é a mesma que foi encontrada pelo Estado-investigação, sem qualquer tipo de manipulação. Observando o segundo, certifica-se de que aquilo que se afirma a respeito do resultado probatório seguiu um procedimento próprio e legítimo.

Diante dessas observações e daquilo que já foi explicitado, verifica-se que a omissão do legislador (problema da *quaestio iuris*) pode ser amenizada pelo compromisso epistêmico daquele que é responsável pela atividade de polícia judiciária. É dizer, o respeito à cadeia de custódia[36] do produto final levado para os autos após todo o processo de raspagem e mineração de informações e dados encontrados em fontes abertas permite atestar a autenticidade e a integridade da razão epistêmica digital que deve ser valorada, ao final da etapa judicial e após o controle das partes com regular exercício de contraditório e de defesa, pelo magistrado competente.

Nesse sentido, deve ser empreendida cautela excessiva no registro procedimental, inclusive com apontamentos de quais equipamentos foram utilizados para aquisição e recolha de fontes de prova digital, bem como mídias de conexão, *hardware* e *software*, pois somente a partir do registro adequado e pormenorizado é que

---

podendo os peritos ser ouvidos em juízo (Badaró, 2023, p. 177-178). Não se nega que o rito indicado garante, nas palavras do mesmo professor, um "experimento probatório com aptidão epistêmica", porém a perspectiva do ensaio é outra. Ao contrário de uma apreensão ou extração de dados de um aparelho multifuncional de interesse para a investigação (e.g., *smartphone*, *tablet*, *notebook* etc.), o que se discute no presente estudo é a busca, em fontes abertas, de informações de interesse para a correta determinação dos fatos, ou seja, conforme se verá, a proposta é que o próprio policial se encarregue da pesquisa e coleta de elementos de prova com aptidão epistêmica.

35. Da leitura do mencionado dispositivo legal, verifica-se que o legislador preocupou-se muito mais com a preservação e o rastreio de vestígios materiais, o que demanda uma cuidadosa exegese quando se pensa na coleta de uma evidência digital.

36. No âmbito das *digital evidence* e *computer forensics*, a expressão "cadeia de custódia" deve ser lida como a elipse de "documentação da cadeia de custódia", cuja responsabilidade fica a cargo dos funcionários públicos que tiverem contato com os elementos materiais que servem de prova, conforme explica Badaró (2021, p. 8).

se pode atribuir confiabilidade à cadeia de custódia (Badaró, 2021, p. 8; Mendes, 2024, p. 337).

No entanto, em razão da alta mutabilidade inerente à *digital evidence*, assim como da necessidade de empregar instrumentos técnicos em sua investigação, ademais da cuidadosa documentação da cadeia de custódia, é imprescindível que se observem as *best practices*[37], respeitando-se os *standards* técnicos instituídos pela comunidade científica, pois, uma vez empregados métodos pouco fiáveis em sua obtenção e produção, carecerão tais elementos de potencial epistêmico, esvaziando por completo sua aptidão probatória (Badaró, 2021, p. 9).

Respeitados os balizamentos supramencionados, acredita-se que os três objetivos do processo penal contemporâneo podem ser alcançados. Primeiro, ter-se-á um conjunto probatório mais completo, algo que contribui para a busca da verdade possível e a reconstrução dos fatos de interesse penal, em especial aqueles mais complexos. Segundo, o peso probatório[38] alcançado ao final da persecução penal permitirá que o juiz natural profira uma decisão mais justa, aplicando a lei penal àqueles que são culpados e absolvendo os inocentes. Por fim, tendo conhecimento do rito probatório que levou a prova digital aos autos, as partes, em particular a defesa, têm os seus direitos e garantias assegurados, com especial ênfase para a ampla defesa, o contraditório, o direito à não autoincriminação e a vedação das provas ilicitamente admitidas e produzidas.

Quanto à vocação do processo de constituir-se em verdadeira garantia dos direitos do cidadão, consoante indicado, não se menospreza que a atividade de persecução desenvolvida em fontes abertas (como as redes sociais), com o uso de agregadores de dados tensiona com salvaguardas insertas em textos constitucionais e instrumentos internacionais de direitos humanos. Daí a importância, repita-se, da transparência quanto aos atos de pesquisa e investigação desencadeados pelas agências de persecução, com a posterior juntada da documentação contemplando a prova digital produzida. Além da publicização do material angariado,

37. De modo exemplificativo, reporta-se às normas da família ISO/IEC 27000. Em síntese, a ISO/IEC 27000:2018 proporciona uma visão geral dos sistemas de gerenciamento de segurança da informação (ISMS). Ela também fornece termos e definições comumente usados na família de normas ISMS, sendo passível de aplicação a todos os tipos e tamanhos de organização, como empresas comerciais, órgãos governamentais, organizações sem fins lucrativos etc.

38. O peso probatório mede o grau de completude e riqueza do conjunto de elementos de juízo aptos para valoração e posterior decisão do Estado-juiz. Quanto maior o peso probatório no contexto de um devido processo, incluindo a devida investigação, maior será o grau de probabilidade de acerto da decisão. Nesse sentido: Ferrer-Beltrán (2021, p. 231).

característica das investigações preliminares modernas, documentar o procedimento permitirá que a defesa contradite, ainda que *a posteriori*, o elemento probatório produzido.

7. Considerações finais

A contemporânea era digital, impulsionada pelo emprego cada vez mais rotineiro de tecnologias de informação e comunicação – acompanhada de uma preocupação também crescente com as dimensões referentes à tutela de direitos fundamentais, como a privacidade e a proteção de dados pessoais – gera espaços virtuais e desafios proporcionais para a produção probatória, em particular no campo criminal. Nesse âmbito, o avanço tecnológico experimentado não apenas permeia a investigação preliminar dos fatos (Mendes, 2024, p. 336), como exerce influência determinante na promoção de novas técnicas de investigação, norteando, ainda, a aquisição e a análise de vestígios.

Neste breve ensaio, procurou-se lançar ponderações acerca do valor probatório e epistêmico dos materiais produzidos a partir do tratamento informativo decorrente da extração de dados pessoais em fontes abertas, com ênfase nas práticas conhecidas como mineração e raspagem.

Diante da lacuna legislativa reguladora do referido tratamento estatal pela omissão em editar uma LGPD no âmbito penal, a formulação de protocolos e mecanismos que assegurem a observância da cadeia de custódia dessa modalidade de prova digital surge como um caminho, ainda que momentâneo. Tal medida destina-se a garantir a autenticidade e a integridade dos vestígios digitais obtidos em fontes abertas, como as plataformas de mídias sociais, de modo a outorgar-lhes maior fiabilidade, tudo a conformar o corolário de uma devida investigação criminal epistemicamente orientada e consentânea com as garantias constitucionais e convencionais historicamente consagradas.

Referências

AGUILERA GARCÍA, Edgar Ramón. Una propuesta de aplicación de la epistemología jurídica en la investigación del delito. In: FERRER-BELTRÁN, Jordi; VÁZQUEZ, Carmen (Orgs.). *Del derecho al razonamiento probatorio*. Madrid: Marcial Pons, 2020. p. 17-44. Disponível em: [www.marcialpons.es/media/pdf/9788491237679.pdf]. Acesso em: 15.08.2025.

AGUILERA GARCÍA, Edgar Ramón. Justificación epistémica, evidencialismo robusto y prueba jurídica. *Quaestio Facti*: Revista Internacional Sobre Razonamiento Probatorio, Girona, n. 3, p. 81-102, 2022. [https://doi.org/10.33115/udg_bib/qf.i3.22733].

BACHMAIER WINTER, Lorena. A luta pelas garantias do devido processo e a mudança de paradigma na teoria da prova: do liberalismo à *mass surveillance* no processo penal europeu. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, v. 11, n. 1, e1164, jan.-abr. 2025. [https://doi.org/10.22197/rbdpp.v11i1.1164].

BADARÓ, Gustavo Henrique. A colaboração premiada: meio de prova, meio de obtenção de prova ou um novo modelo de justiça penal não epistêmica? In: MOURA, Maria Thereza Rocha de Assis; BOTTINI, Pierpaolo Cruz (Coords.). *Colaboração premiada*. São Paulo: Ed. RT, 2017. p. 127-149.

BADARÓ, Gustavo Henrique. *Epistemologia judiciária e prova penal*. São Paulo: Thomson Reuters; Ed. RT, 2019.

BADARÓ, Gustavo Henrique. *Processo penal*. São Paulo: Ed. RT, 2020.

BADARÓ, Gustavo Henrique. Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia. *Boletim IBCCRIM*, São Paulo, v. 29, n. 343, p. 7-9, jun. 2021. Disponível em: [https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1325]. Acesso em: 18.08.2025.

BADARÓ, Gustavo Henrique. A cadeia de custódia da prova digital. In: SARLET, Ingo W. et al. (Org.). *Direito probatório*. Londrina: Thoth, 2023. p. 175-188.

BALDAN, Édson Luís. Devida investigação legal como derivação do devido processo legal e como garantia fundamental do imputado. In: KHALED JR., Salah (Coord.). *Sistema penal e poder punitivo*: estudos em homenagem ao prof. Aury Lopes Jr. Florianópolis: Empório do Direito, 2015. p. 155-182.

BARRETO, Alessandro Gonçalves; WENDT, Emerson. *Inteligência e investigação criminal em fontes abertas*. 4. ed. Rio de Janeiro: Brasport, 2024.

BRASIL. SENADO FEDERAL. *Cicatrizes*: a produção da obra 8 de janeiro de 2023, de Vik Muniz. Brasília: Secretaria de Comunicação Social, 2024. Disponível em: [www2.senado.leg.br/bdsf/bitstream/handle/id/650920/Cicatrizes.pdf]. Acesso em: 07.03.2025.

BRASIL. SUPREMO TRIBUNAL FEDERAL. *8 de janeiro*: 2 anos de atuação. Relatório do gabinete do Ministro Alexandre de Moraes. Brasília: STF, 2025. Disponível em: [https://noticias-stf-wp-prd.s3.sa-east-1.amazonaws.com/wp-content/uploads/wpallimport/uploads/2025/01/07201238/Relatorio-8-de-janeiro-Versao-Final.pdf]. Acesso em: 24.03.2025.

BRASIL. SUPREMO TRIBUNAL FEDERAL. Em dois anos, STF responsabilizou 898 pessoas por atos antidemocráticos de 8 de janeiro: balanço traz os principais dados e números sobre processos que tramitam na Corte sobre a matéria. *Supremo Tribunal Federal*, *Notícias*, Brasília, 07.01.2025. Disponível em: [https://noticias-stf-wp-prd.s3.sa-east-1.amazonaws.com/wp-content/uploads/wpallimport/uploads/2025/01/07201238/Relatorio-8-de-janeiro-Versao-Final.pdf]. Acesso em: 21.02.2025.

CAMARGO, Rodrigo Oliveira. *Tratamento de dados, persecução penal e a garantia do direito de defesa*. 2022. 221 f. Tese (Doutorado em Ciências Criminais) – Escola de Direito, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2022. Disponível em: [https://tede2.pucrs.br/tede2/bitstream/tede/10605/5/TES_RODRIGO_OLIVEIRA_DE_CAMARGO_COMPLETO.pdf]. Acesso em: 27.07.2025.

CASELLI, Guilherme. *Manual de investigação digital*. 3. ed. São Paulo: JusPodivm, 2023.

COELHO, Emerson Ghirardelli. *Investigação criminal constitucional*. São Paulo: Del Rey, 2017.

COMANDUCCI, Paolo. La motivazione in fato. In: UBERTIS, Giulio (Ed.). *La cognoscenza del fato nel processo penale*. Milano: Giuffrè, 1992. p. 215-244.

COMISSÃO entrega à Câmara anteprojeto sobre tratamento de dados pessoais na área criminal. *Superior Tribunal de Justiça*, Notícias, Brasília, 05.11.2020. Disponível em: [www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/05112020-Comissao-entrega-a-Camara-anteprojeto-sobre-tratamento-de-dados-pessoais-na-area-criminal.aspx]. Acesso em: 07.03.2025.

DANIELE, Marcello. La prova digitale nel processo penale. *Rivista di Diritto Processuale*, Padova, v. 66, n. 2, p. 283-298, 2011.

DEZEM, Guilherme Madeira. *Curso de processo penal*. 6. ed. São Paulo: Ed. RT, 2020.

FERRAJOLI, Luigi. *Direito e razão*: teoria do garantismo penal. São Paulo: Ed. RT, 2010.

FERRER-BELTRÁN, Jordi. *Prueba sin convicción*: estándares de prueba y debido proceso. Madrid: Marcial Pons, 2021.

GASCÓN ABELLÁN, Marina. *Los hechos en el derecho*: bases argumentales de la prueba. Madrid: Marcial Pons, 2010.

GIAMPAOLI, Anderson Pires. Provas digitais, extração de dados e informações de dispositivos multifuncionais e proporcionalidade: o papel epistêmico e principiológico do Estado-investigação com respeito à privacidade. In: GASCÓN ABELLÁN, Marina; MATIDA, Janaina (Orgs.). *Melhorar a prova*. São Paulo: Marcial Pons, 2024. p. 89-123.

GLEIZER, Orlandino; MONTENEGRO, Lucas; VIANA, Eduardo. *O direito de proteção de dados no processo penal e na segurança pública*. Rio de Janeiro: Marcial Pons, 2021.

GONZÁLEZ LAGIER, Daniel. *Quaestio facti*: ensayos sobre prueba, causalidad y acción. México: Fontamara, 2020.

GONZÁLEZ LAGIER, Daniel. *Quaestio facti*: ensaios sobre prova, causalidade e ação. Tradução: Luis Felipe Kircher. 3. ed. São Paulo: JusPodivm, 2025.

INFLUENCER MARKETING HUB. Influencer Marketing Benchmark Report 2025. *Influencer Marketing Hub*, 25.04.2025. Disponível em: [https://influencermarketinghub.com/influencer-marketing-benchmark-report/]. Acesso em: 27.03.2025.

INSTITUTO DE DEFESA DO DIREITO DE DEFESA. *Prova sob suspeita*: reconhecimento de pessoas e prova testemunhal: orientações para o sistema de justiça. São Paulo: IDDD, 2022.

INSTITUTO BRASILEIRO DE CIÊNCIAS CRIMINAIS. O que faremos depois de 8 de janeiro? *Boletim IBCCRIM*, São Paulo, v. 31, n. 363, p. 2, 2024. Disponível em: [https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1567]. Acesso em: 03.08.2025.

JORGE JR., Hélio Molina; JORGE, Higor Vinicius Nogueira. Ferramentas disponíveis na internet para investigação em fontes abertas. In: JORGE, Higor Vinicius Nogueira (Coord.). *Tratado de investigação criminal tecnológica*. Salvador: JusPodivm, 2020. p. 53-82.

LAUDAN, Larry. *Verdad, error y proceso penal*: un ensayo sobre epistemología jurídica. Madrid: Marcial Pons, 2013.

LOPES JR., Aury. *Direito processual penal*. 18. ed. São Paulo: Saraiva Educação, 2021.

MARQUES, José Frederico. *Elementos de direito processual penal*. 2. ed. Campinas: Millennium, 2000.

MATIDA, Janaina; HERDY, Rachel. As inferências probatórias: compromissos epistêmicos, normativos e interpretativos. In: CUNHA, José Eduardo (Org.). *Epistemologias críticas do Direito*. Rio de Janeiro: Lumen Juris, 2016. p. 209-239.

MATIDA, Janaina; MOSCATELLI, Lívia. *Os fatos no processo penal*. São Paulo: Marcial Pons, 2023.

MATIDA, Janaina; NARDELLI, Marcella Mascarenhas; HERDY, Rachel. A prova penal precisa passar por uma filtragem epistêmica. *Consultor Jurídico*, São Paulo, 13.03.2020a. Disponível em: [www.conjur.com.br/2020-mar-13/limite-penal-prova-penal-passar-filtragem-epistemica/]. Acesso em: 26.02.2025.

MATIDA, Janaina; NARDELLI, Marcella Mascarenhas; HERDY, Rachel. No processo penal, a verdade dos fatos é garantia. *Consultor Jurídico*, São Paulo, 19.06.2020b. Disponível em: [www.conjur.com.br/2020-jun-19/limite-penal-processo-penal-verdade-fatos-garantia/]. Acesso em: 26.02.2025.

MENDES, Carlos Hélder C. Furtado. *Malware do estado e processo penal*: a proteção de dados informáticos face à infiltração por software na investigação criminal. 2018. 219 f. Dissertação (Mestrado em Ciências Criminais) – Escola de Direito, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2018. Disponível em: [https://tede2.pucrs.br/tede2/bitstream/

tede/8537/5/DIS_CARLOS_HELDER_CARVALHO_FURTADO_MENDES_COMPLETO.pdf]. Acesso em: 03.08.2025.

MENDES, Carlos Hélder C. Furtado. *Prova penal digital*. São Paulo: Tirant lo Blanch, 2024.

MORAES, Maurício Zanoide de. *Processo criminal transformativo*: modelo criminal e sistema processual não violentos. Belo Horizonte, São Paulo: D´Plácido, 2022.

MORAES, Rafael Francisco Marcondes de. *Inquérito policial constitucional e devida investigação criminal*. São Paulo: JusPodivm, 2025.

MOSCATELLI, Livia Yuen Ngan. La importancia de la abducción en la etapa de investigación criminal. *Quaestio Facti*: Revista Internacional Sobre Razonamiento Probatorio, Girona, n. 5, p. 125-155, 2023. [https://doi.org/10.33115/udg_bib/qf.i5.22846].

PEREIRA, Eliomar da Silva. *Teoria da investigação criminal*. 3. ed. São Paulo: Almedina, 2022.

PITOMBO, Cleunice. Reforma do Código de Processo Penal: observações sobre os meios de obtenção de prova digital. In: BRITO CRUZ, Francisco; SIMÃO, Bárbara; HOUANG, André (Ed.). *Direitos fundamentais e processo penal na era digital*: doutrina e prática em debate. São Paulo: InternetLab, 2024. v. VII. p. 36-49.

PRADO, Geraldo. Ainda sobre a "quebra da cadeia de custódia das provas". *Boletim IBCCRIM*, São Paulo, n. 262, p. 16-17, set. 2014.

PRADO, Geraldo. *Curso de processo penal*: fundamentos e sistema. São Paulo: Marcial Pons, 2024. t. 1.

SAAD, Marta. Direito de defesa na etapa preliminar da apuração penal: reconhecimento, novas perspectivas e desafios. *Boletim IBCCRIM*, São Paulo, v. 32, n. 381, p. 13-17, 2024. [https://doi.org/10.5281/zenodo.12709853].

SAAD, Marta. *O direito de defesa no inquérito policial*. São Paulo: Ed. RT, 2004.

TARUFFO, Michele. *Uma simples verdade*: o juiz e a construção dos fatos. Trad. Vitor de Paula Ramos. São Paulo: Marcial Pons, 2016.

UBERTIS, Giulio. *Profili di epistemologia giudiziaria*. 2. ed. Milano: Giuffrè, 2021.

Legislação

BRASIL. *Lei 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Presidência da República, 2018. Disponível em: [www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm]. Acesso em: 04.03.2025.

BRASIL. CONSELHO NACIONAL DE JUSTIÇA. *Resolução 484, de 19 de dezembro de 2022*. Estabelece diretrizes para a realização do reconhecimento

de pessoas em procedimentos e processos criminais e sua avaliação no âmbito do Poder Judiciário. Brasília: CNJ, 2022b. Disponível em: [https://atos.cnj.jus.br/files/original2118372022122763ab612da6997.pdf]. Acesso em: 25.02.2025.

BRASIL. *Projeto de Lei 1.515, de 7 de junho de 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. Brasília: Câmara dos Deputados, 2022a. Disponível em: [www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2326300&fichaAmigavel=nao]. Acesso em: 07.03.2025.

BRASIL. *Projeto de Lei 4.939, de 15 de outubro de 2020*. Dispõe sobre as diretrizes do direito da Tecnologia da Informação e as normas de obtenção e admissibilidade de provas digitais na investigação e no processo, além de outras providências. Brasília, DF: Câmara dos Deputados, 2020a. Disponível em: [www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2264367]. Acesso em: 10.03.2025.

Jurisprudência

BRASIL. Superior Tribunal de Justiça, 6ª T., *Habeas Corpus* 598.886 Santa Catarina, rel. Min. Rogerio Schietti Cruz, 27.10.2020b. Disponível em: [www.stj.jus.br/sites/portalp/SiteAssets/documentos/noticias/27102020%20HC-598886-SC.pdf]. Acesso em: 25.02.2025.

BRASIL. Supremo Tribunal Federal, Plenário, Ação Direta de Inconstitucionalidade 6.298 Distrito Federal, rel. Min. Luiz Fux, 24.08.2023. Disponível em: [https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=773560651]. Acesso em: 27.02.2025.

Recebido em: 30.03.2025.
Aprovado em: 25.07.2025.
Última versão dos autores: 05.08.2025.



PESQUISA DO EDITORIAL



Área do Direito: Processual; Penal; Digital

Veja também Doutrina relacionada ao tema

- Meios de obtenção de prova na fase preliminar criminal: considerações sobre reconhecimento pessoal no brasil e na legislação comparada, de Rafael Francisco França – *RBCCrim* 112/331-366; *Doutrinas Essenciais Direito Penal e Processo Penal* 6; e
- Valoração da prova digital: entre a desconfiança e a crença, de Luíza Guimarães Campos Batista Gomes e André Ricardo Godoy de Souza – *RePro* 359/175-207.

Veja também Jurisprudência relacionada ao tema

- STJ, EDcl no AgRg no HC 966772, j. 25.04.2025, *DJe* 30.04.2025.

Giampaoli, Anderson Pires; Moraes, Rafael Francisco Marcondes de; Silva, Roberta de Lima e. Devida investigação criminal: compromissos epistêmicos e probatórios na extração de dados pessoais em fontes abertas. *Revista Brasileira de Ciências Criminais*. vol. 211. ano 33. p. 115-141. São Paulo: Ed. RT, nov./dez. 2025. DOI: [https://doi.org/10.5281/zenodo.17058359].

Reconhecimento facial: biopolítica granular e controle customizado no Brasil

Facial recognition: granular biopolitics and customized control in Brazil

Assista aos comentários dos autores sobre este artigo

Gabriel Saad Travassos[1]
Pontifícia Universidade Católica do Rio Grande do Sul, PUCRS, Brasil.
travassosgabrielsaad@gmail.com

Augusto Jobim do Amaral[2]
Pontifícia Universidade Católica do Rio Grande do Sul, PUCRS, Brasil.
augusto.amaral@pucrs.br

DOI: [doi.org/10.5281/zenodo.17058382].

Área do Direito: Penal; Digital; Constitucional

Resumo: No contexto da pandemia da Covid-19, mecanismos automatizados de reconhecimento facial à distância foram impulsionados em espaços públicos e privados como formas de controle de acesso e aferição de risco. Enquanto o contato

Abstract: In the context of the Covid-19 pandemic, automated remote facial recognition mechanisms have been implemented in public and private spaces as a means of access control and risk assessment. Although some groups'

1. Doutorando em Ciências Criminais (PUCRS). Mestre em Direito e Justiça Social (FURG). Defensor Público Federal.
Currículo Lattes: [http://lattes.cnpq.br/3903303580918758].
ORCID: [https://orcid.org/0000-0002-5451-6833].
E-mail: travassosgabrielsaad@gmail.com
2. Professor dos Programas de Pós-Graduação em Ciências Criminais e em Filosofia, ambos da PUCRS.
Currículo Lattes: [http://lattes.cnpq.br/4048832153516187].
ORCID: [https://orcid.org/0000-0003-0874-0583].
E-mail: augusto.amaral@pucrs.br

de alguns grupos com a biometria facial se limita a situações de conveniência, outros são objeto de monitoramento e detenção. Essa realidade é presente no Brasil, onde o reconhecimento facial tem se espalhado de forma heterogênea e desregulamentada. A partir da análise foucaultiana ao nível das técnicas e suas estratégias, o ensaio tem como problema de pesquisa compreender a relação entre a biopolítica e as tecnologias de reconhecimento facial, buscando linhas de continuidade e ruptura. A pesquisa é qualitativa, assumindo como procedimento de pesquisa a revisão bibliográfica e a pesquisa documental. O método é o genealógico-crítico, identificando as tecnologias de reconhecimento facial como emergência de um novo tipo de controle e modo de subjetivação que avança sobre o poder disciplinar e sobrepõe-se à modulação ambiental pensada ao nível da população. Ao final, a partir da compreensão da governamentalidade algorítmica, apresenta-se o conceito de "biopolítica granular" buscando a reflexão sobre um tipo de controle modular simultaneamente massivo e customizado sobre indivíduos proposto pelas tecnologias de reconhecimento facial.

Palavras-chave: Reconhecimento facial – Biopoder – Anátomo-política – Biopolítica granular – Governamentalidade algorítmica.

contact with facial biometrics is restricted in situations of convenience, others are subject to monitoring and detention. This reality is present in Brazil, where facial recognition has spread in a heterogeneous and unregulated manner. Based on Foucault's analysis at the level of techniques and their strategies, the essay's research problem is to understand the relationship between biopolitics and facial recognition technologies, seeking lines of continuity and rupture. The research is qualitative, adopting bibliographic review and documentary research as research procedures. The method is genealogical-critical, identifying facial recognition technologies as the emergence of a new type of control and mode of subjectivation that advances over disciplinary power and overlaps environmental modulation thought at the population level. Finally, based on the understanding of algorithmic governmentality, the concept of "granular biopolitics" is presented, seeking to reflect on a type of modular control that is simultaneously massive and customized over individuals proposed by facial recognition technologies.

Keywords: Facial recognition – Biopower – Anatomical politics – Granular biopolitics – Algorithmic governmentality.

Sumário: 1. Introdução. 2. Reconhecimento facial entre circuitos de exposição e controle no Brasil. 2.1. A expressão do reconhecimento facial no regime de visibilidade moderno. 2.2. As realidades "verticais" do reconhecimento facial no Brasil. 3. Anátomo-política dos corpos e biopolítica das populações: efeitos da governamentalidade algorítmica na customização do controle populacional. 3.1. Do corpo adestrado à gestão modular do ambiente: duas faces do biopoder. 3.2. Biopolítica granular: os efeitos da governamentalidade algorítmica na gestão customizada das populações. 4. Considerações finais. Referências.

1. Introdução

Em diversos países, tecnologias de reconhecimento facial (TRFs) foram instaladas como mecanismos automatizados que garantiriam segurança e mobilidade, simultaneamente, para estimular a circulação de pessoas a partir de infraestruturas que dispensariam checagens manuais e apresentação de documentos.

Estudos apontam que 70% das forças policiais possuem algum tipo de reconhecimento facial e 60% dos países utilizam essa tecnologia nos aeroportos (Matulionyte; Zalnieriute, 2024, p. 1.). Além da utilização nas fronteiras e na área de segurança pública, as TRFs espalharam-se pelo cotidiano de estádios de futebol, hotéis, casas de *shows*, condomínios, instituições bancárias e aplicativos como formas seguras e convenientes para o controle de acesso. Esse contexto de sistemas biométricos teve um impulso considerável pela emergência da pandemia da Covid-19 e pela busca da realização das transações sem contato físico.

O ensaio tem como problema de pesquisa entender qual tipo de relações de poder se exerce nessas tecnologias de reconhecimento facial. Busca-se, assim, problematizar ao nível das técnicas, estratégias e seus dispositivos, como propôs Foucault (2003, p. 241), em que medida uma gestão modular da população própria da biopolítica é impactada com o surgimento de técnicas que asseguram, ao mesmo tempo, o controle das massas e a corporificação individual do risco.

A pesquisa é qualitativa, assumindo como técnicas de pesquisa a revisão bibliográfica e a pesquisa documental. A partir do problema que mobiliza a pesquisa, aplica-se o método genealógico-crítico (Harcourt, 2024) propondo identificar as práticas genealógicas que nutrem positivamente nossa atividade e, com isso, promovam a ambição de uma filosofia crítica, na direção de se engajar de forma consciente, deliberada e cuidadosa numa história do pensamento que revigore nossa atividade. Portanto, pretende-se identificar as tecnologias de reconhecimento facial como emergência de um novo tipo de controle e modo de subjetivação que avança sobre o poder disciplinar e sobrepõe-se à modulação ambiental pensada ao nível da população.

Na primeira seção, será estudada a tecnologia de reconhecimento facial e a sua inserção no regime escópico a partir de circuitos de exposição e controle, com enfoque no cenário brasileiro de incorporação desregulamentada e heterogênea, pautada na classificação de risco. Na segunda seção, trataremos da análise de Foucault sobre anátomo-política dos corpos e biopolítica das populações e abordaremos aquilo que pesquisadores definiram como *biopolítica granular*, em alusão aos efeitos decorrentes do emprego das tecnologias de reconhecimento facial na gestão dos espaços das multidões, na sua correlação com o conceito de governamentalidade algorítmica.

2. Reconhecimento facial entre circuitos de exposição e controle no Brasil

2.1. A expressão do reconhecimento facial no regime de visibilidade moderno

As tecnologias de reconhecimento facial podem ser divididas em três tipos básicos: i) verificação; ii) identificação; e iii) classificação (Dushi, 2020). As tecnologias

de verificação, do tipo um-para-um, são aquelas que têm por objetivo comparar a face capturada com uma única imagem no banco de dados. É o caso da maioria dos *smartphones*. O reconhecimento facial por identificação busca, a partir de cálculos probabilísticos, identificar entre multidões rostos cujas dimensões antropométricas correspondam às dimensões armazenadas em uma lista que compõe a base de dados. É o caso das câmeras instaladas em locais de grande fluxo ou grandes eventos para a busca de pessoas desaparecidas ou procurados pela polícia. As últimas, de classificação, estão concentradas na extração de significados a partir do semblante ou de outros aspectos biológicos por meio da face, a exemplo da temperatura ou de sentimentos como alegria, medo, raiva, tristeza etc.

As TRFs ainda podem ser classificadas segundo o aspecto temporal: *livestream* ou diferido. No primeiro caso, a captura e análise ocorrem em tempo real, enquanto no segundo caso, os dados biométricos capturados são posteriormente comparados. Independentemente do tipo, o risco é um elemento central do funcionamento dessas tecnologias. As câmeras são estruturadas com modelos algorítmicos para, a partir de comportamentos, identificar a existência de um risco ou, ainda, associar faces a bancos de suspeitos policiais (O'Neil, 2020, p. 19).

Fernanda Bruno (2013, p. 39) observa que mesmo que estudos demonstrem a inexistência de nexo entre o aumento da videovigilância e a redução da criminalidade, a apropriação da noção de risco pelo discurso policial securitário é capaz de transformar as falhas em sua própria justificativa para ampliação do regime de vigilância. Em outras palavras, se o crime não reduz, não é porque o equipamento de segurança não é efetivo, mas sim porque ainda estaria em quantidade insuficiente. Edifica-se, então, um modelo autorreferenciado entre risco, segurança e vigilância, com curva de tendência exponencial, tendo em vista que a própria falha é seu motor de expansão.

Essa é uma característica importante das sociedades de controle (Deleuze, 1992, p. 221). Os dispositivos de controle não estão restritos à tônica disciplinar dos corpos, mas sim ao monitoramento ao ar livre (Amaral, 2024, p. 15). É um controle que produz ativamente a circulação como forma de vigiar a liberdade segundo paradigmas do risco. Ambientes movimentados, como o metrô, por exemplo, operam câmeras com alarme de risco quando um indivíduo é monitorado por permanecer muito tempo parado. Câmeras com reconhecimento facial aplicam inteligência artificial para, a partir das características do rosto, como a distância entre as sobrancelhas, nariz, boca, atribuir um *score* e conferir um resultado aproximativo entre a face visualizada e a face buscada.

Em ambos os casos, indivíduos fora do padrão são associados ao risco: pessoas em situação de rua que permanecem estáticas divergem do modelo desenhado para o metrô; tecnologias de reconhecimento facial atribuem falsos positivos a grupos

historicamente marginalizados (Benjamin, 2019). Nesses corpos está materializada a noção de risco, dessa vez sob o discurso da neutralidade dos olhos maquínicos.

Apesar dos registros das primeiras pesquisas sobre reconhecimento facial automatizado remontarem à década de 1960 (Bledsoe, 1965), a utilização em larga escala ocorre apenas no século XXI. A partir década de 2010, com a multiplicação exponencial de câmeras de alta definição instaladas em dispositivos pessoais, objetos, espaços públicos e privados, a matéria-prima para o desenvolvimento dos sistemas estava dada: bases gigantescas de imagens faciais para treinamento, processamento e sistematização (Selwyn et al., 2024, p. 13).

Essa virada visual nas tecnologias de consumo digital, que tem como marca a popularização da *selfie* e das fotografias digitais, permitiu a formação das bases de dados que eram operadas a partir de sistema computacionais de alta capacidade e técnicas de *deep learning* para a identificação automatizada de rostos (Selwyn et al., 2024).

Empresas como a *Clearview AI* realizaram, nos últimos anos, gigantescas varreduras na *internet* para a captura indiscriminada de rostos para fins de treinamento e execução do reconhecimento facial automatizado. Estima-se que foram capturadas mais de 20 bilhões de imagens e dados pessoais na criação da base de dados (Gentile, 2024, p. 176).

Aqui se percebe como um elemento sociocultural – a fotografia – graças a uma capacidade de adesão subjetiva, que é própria do sistema econômico e político, permitiu o emprego de uma técnica com potencial de alterar a própria subjetividade[3]. Se estamos tratando de uma ferramenta que permite o controle individual no meio de multidões, antes anônimas, isso terá um efeito sobre o comportamento individual e social nos espaços públicos e privados.

Destacando os aspectos sociotécnicos desse processo, é possível notar uma ambiguidade própria das tecnologias de reconhecimento facial em que uma miríade de experiências com o artefato pode emergir[4]. Do mesmo modo que uma câmera pode ser utilizada para garantir um acesso ágil em aeroportos, é capaz de impedir o acesso de grupos identificados como de risco.

A dualidade de emprego das TRFs pode ser descrita desde a correlação entre circuitos de exposição e segurança, expressão exata dos vetores de regime de visibilidade moderno, com implicações fundamentais para a subjetividade: a disciplina e o espetáculo. Embora sejam circuitos distintos, entrecruzam-se no processo de subjetivação moderno, tendo em vista que a adesão subjetiva aos novos artefatos

3. ROUVROY; BERNS, 2015, p. 38.

4. ANDREJEVIC, 2020, p. 10.

tecnológicos é fundamental para garantir sua difusão social e, assim, pavimentar o caminho de sua utilização como instrumento disciplinar e de segurança[5].

As tecnologias desenvolvidas no regime econômico codificam as tendências prevalentes no meio social, como é o caso do racismo e outros modos de discriminação de minorias[6]. Essa assimetria sobre como a tecnologia é absorvida ajuda a explicar o dilema em torno do reconhecimento facial, que parece ser uma ferramenta útil e inofensiva para alguns grupos sociais, pois não são aqueles vigiados e vítimas do desvio de seu uso.

Essa dupla característica das TRFs é identificada por Selwyn et al. como a *function creep* da tecnologia, isto é, "desvios de função" a fim de alcançar outras finalidades que tenham uma destinação mais polêmica porquanto invadam a esfera da privacidade, busquem predizer comportamentos ou simplesmente discriminem grupos inteiros[7].

Essa complexa rede diversificada e heterogênea de uso e impacto das tecnologias de reconhecimento facial demanda uma reflexão a vários níveis, sobretudo que tipo de economia do poder mobiliza e, simultaneamente, em que medida seu uso remodela certas práticas biopolíticas.

2.2. As realidades "verticais" do reconhecimento facial no Brasil

No Brasil, a implementação de sistemas de reconhecimento facial à distância teve como traço de emergência o modelo policial de vigilância tecnológico pensado para grandes eventos, notadamente a Copa do Mundo de 2014 e as Olimpíadas de 2016[8]. Em 2014, são divulgados os primeiros testes em estádios para a implementação dos sistemas de reconhecimento facial[9] e, dez anos depois, 22 estádios no Brasil possuem tais tecnologias – 18 em uso, 2 em teste e 2 em estudo –, em diversas capitais do país[10].

Mas a expansão das tecnologias de reconhecimento facial não se limitou às arenas esportivas. Estudos recentes apontam que essas tecnologias estão presentes em

5. HARCOURT, 2015.
6. SILVA, 2022, p. 79.
7. SELWYN; ANDREJEVIC; O'NEILL; GU; SMITH, 2024, p. 19.
8. AUGUSTO et al., 2025.
9. Beira Rio irá testar sistema de reconhecimento facial contra bagunceiros. *UOL Notícias*. Disponível em: [https://copadomundo.uol.com.br/noticias/redacao/2014/04/19/beira-rio-ira-testar-sistema-de-reconhecimento-facial-contra-bagunceiros.htm]. Acesso em: 30.01.2025.
10. SOUSA et al., 2024, p. 9.

escolas[11], em estações de metrô[12], e em milhares de cidades em espaços públicos como praças, paradas de ônibus etc.[13].

A Portaria 793, de 2019, do Ministério da Justiça e Segurança Pública, incentivou o financiamento de novas tecnologias para a "implantação de sistemas de videomonitoramento com soluções de reconhecimento facial, por *Optical Character Recognition* – OCR, uso de inteligência artificial ou outros". A *Clearview AI,* empresa processada e sancionada em diversos países europeus em virtude da varredura indiscriminada das imagens faciais na *internet* para composição do banco de dados, foi licenciada pelo Ministério da Justiça em 2023 para a elaboração de pesquisas por imagens em mídias sociais ao valor estimado de R$ 2,5 milhões. A empresa também já conseguiu contratos com a Polícia Legislativa do Senado, com a Polícia Militar de Minas Gerais e com a Superintendência Regional da Polícia Federal do Paraná[14].

O produto oferecido pela empresa é um banco de dados com bilhões de rostos capturados sem consentimento dos usuários da *internet*. A busca por uma base ampliada tem por objetivo garantir que todas as faces estejam catalogadas e identificadas para futura e eventual intervenção policial.

Essa intervenção tem ganhado destaque nas notícias nos cumprimentos de mandados de prisão durante as aglomerações das festas de carnaval. No Rio de Janeiro[15] e na Bahia,[16] as autoridades divulgaram o reconhecimento facial para a coleta de imagens faciais e a identificação de suspeitos. Em São Paulo, a Prefeitura decidiu implementar um "prisômetro", uma espécie de marcador *livestream* com a quantidade de pessoas presas como decorrência da utilização do reconhecimento facial[17].

Usualmente são apontados alguns casos em que as forças policiais conseguiram localizar pessoas que estavam foragidas da Justiça. No entanto, pouco é descrito quanto aos erros que a nova tecnologia algorítmica projeta, os conhecidos falsos positivos, bem como sobre o gasto público com a instalação dos equipamentos.

11. ISRAEL et al., 2023.
12. BRUNO, 2018, p. 239-256.
13. NUNES; LIMA; CRUZ, 2023a.
14. MARTINS, 2025.
15. SOUZA, 2024.
16. GAMA, 2024.
17. G1. Prefeitura de SP lança 'prisômetro' em meio a críticas da Defensoria sobre uso de reconhecimento facial no Carnaval. *G1*, São Paulo, 25.02.2025. Disponível em: [https://g1.globo.com/sp/saopaulo/carnaval/2025/noticia/2025/02/25/prefeitura-de-sp-lanca-prisometro-em-meio-a-criticas-da-defensoria-sobre-uso-de-reconhecimento-facial-no-carnaval.ghtml]. Acesso em: 18.03.2025.

Também, quase nula é a divulgação sobre as empresas privadas que armazenam as imagens faciais e como fazem a gestão do *software,* tampouco sobre as cautelas com o tratamento de dados pessoais sensíveis[18].

Nesse contexto, enquanto a população festejava mais um carnaval, suas faces estavam sob contínuo monitoramento e seus corpos suscetíveis à pronta intervenção policial. Porém, enquanto para alguns grupos os rostos são senhas para o ingresso em camarotes, arenas e espaços festivos, para outros a fisionomia carrega consigo a marca do risco, risco de um falso positivo que pode ser fatal.

O falso positivo não é um desvio do reconhecimento facial; além de ser seu padrão, é tecnicamente o que se busca, pois afinal, dentro da lógica recursiva cibernética, quanto mais erros, mais aperfeiçoamento se produzirá. Estudo conduzido pelo *National Institute of Standards and Technology* (NIST) avaliou *softwares* de algoritmos de reconhecimento facial de 99 desenvolvedores de 189 organizações, incluindo *Toshiba*, *Intel* e *Microsoft*. A pesquisa apontou que a maioria dos algoritmos de reconhecimento facial apresentam diferenças demográficas, isto é, a capacidade de comparação dos sistemas varia de um grupo – sexo, etnia, idade – para outro[19]. Na tecnologia de reconhecimento facial um-para-um os pesquisadores encontraram índices de falsos positivos de 10 a 100 vezes maiores para pessoas asiáticas ou negras em comparação com pessoas brancas. Na tecnologia de comparação um-para-muitos, os números apontam para altas taxas de falsos positivos entre mulheres negras[20].

Essa simultaneidade entre carnaval – circuito de exposição – e policiamento – circuito de segurança – está no cerne do que Ruha Benjamin define como *realidades verticais*. Longe de ser um tratamento homogêneo e objetivo, as tecnologias asseguram liberdade e segurança para alguns e vigilância e controle para outros[21]. A globalização, nesse ponto, produziu uma demanda de redução dos pontos de contato para aceleração da circulação de certas pessoas e bens por um lado e rápida intervenção e detenção de outras pessoas que não interessam ao modelo econômico de

18. Sintomático que o referencial da política de segurança pública seja o número de prisões, que normalmente é sinal do fracasso das propostas de prevenção ao delito. Mas não será estranho, pois o âmago desse tipo de solucionismo tecnológico aplicadas em geral às dinâmicas preditivas é que sua lógica se vende como perfeita. Se há menos constatações de foragidos, suspeitos ou condenados é sinal de que o mecanismo está funcionando e prevenindo o crime; se, pelo contrário, aumentam os números é porque a eficiência também está sendo constatada. Cf.: WANG, 2022, p. 209-230.
19. GROTHER; NGAN; HANAOKA, 2019.
20. NATIONAL INSTITUTE OF STANDARDS AND TECNHOLOGY, 2019.
21. BENJAMIN, 2019, p. 150.

outro[22]. As tecnologias de reconhecimento facial atendem a esse reclamo e, paradoxalmente, multiplicam barreiras de acesso para uns e facilitam os espaços de circulação para outros. O corpo se transformou no portador da fronteira, inscrito em múltiplos limites de acessos codificados[23].

O cenário é acentuado na realidade brasileira com alguns aspectos ainda mais complexos decorrentes da implementação desregulamentada e heterogênea no âmbito nacional. Dados atualizados sobre o reconhecimento facial no Brasil apontam que, até janeiro de 2025, 364 projetos de reconhecimento facial estavam em aplicação no país, o que significa uma estimativa de mais de 82 milhões de pessoas potencialmente vigiadas pelo mecanismo biométrico[24].

Esses projetos alcançam custos de operação na ordem de mais de R$ 969 milhões, com variados *softwares* administrados pelas empresas fornecedoras, incluindo *Axxon Next SW-ANV-FRCT-RTL*, *Hiki Center Professional*, *SecurOS*, *SAFR*, *Holosens Huawei*, *VMS Digifort* versão *Enterprise 7.3.0.1*, *Digifort* e *Dahua*[25]. Apesar do expressivo montante, não há transparência sobre os critérios de escolha das empresas, o operador do projeto, o custo total e políticas de proteção de dados.

Em 72,5% dos casos pesquisados pelo projeto *O Panóptico,* que realiza o monitoramento das tecnologias de reconhecimento facial no Brasil, as entidades não informaram a elaboração de relatórios de impacto à proteção de dados pessoais. De acordo com o relatório, os projetos operam sem atender os padrões mínimos de transparência ativa e passiva, o que fragiliza o controle social, abre espaços para abusos, desvios, usos desproporcionais e práticas discriminatórias[26].

No Estado de Goiás, por exemplo, o reconhecimento facial foi conjugado com a municipalização da segurança pública. Os municípios goianos receberam vultosos recursos públicos por meio de emendas parlamentares e repasses da Portaria 793 do Ministério da Justiça. Como aponta o relatório do projeto *O Panóptico,* dos 89 projetos de financiamento federal para o reconhecimento facial submetidos em 2019, 51 eram de municípios goianos[27]. Mais de 30 milhões de reais em emendas parlamentares para implementação do videomonitoramento foram destinados a 95 nos municípios naquele Estado entre 2017 e 2022[28].

22. ANDREJEVIC; O'NEILL; SMITH; SELWYN; GU, 2024, p. 1204-1226.
23. AMOORE, 2006, p. 336-351.
24. O Panóptico. *Monitor de novas tecnologias na segurança pública do Brasil*. Disponível em: [www.opanoptico.com.br/#regioes]. Acesso em: 20.03.2025.
25. LIMA et al., 2024, p. 19.
26. LIMA et al., 2024, p. 40.
27. NUNES; LIMA; RODRIGUES, 2023b.
28. NUNES; LIMA; RODRIGUES, 2023b.

Cada município contratou uma empresa de tecnologia de reconhecimento facial, mas as principais fornecedoras são as empresas *Arcade Tecnologia*, *Tecno Marra* e *SS2 Tecnologia*. Essas duas últimas foram fundadas, respectivamente, em 2015 e 2018. Ambas foram criadas por famílias tradicionais da elite goiana e, mesmo sendo relativamente novas no mercado, ganharam a maior parte dos pregões. O relatório aponta ainda a inexistência de estudos de impacto, a falta de transparência no funcionamento dos *softwares* e na metodologia de produção, armazenamento e análise dos dados[29].

Dos municípios goianos pesquisados, a maioria não possui rede de esgotamento sanitário adequada, experimenta carência nas estruturas das unidades de saúde e de ensino. O número de delitos nesses municípios, em média, não ultrapassa 50 casos anuais, geralmente ligados a crimes patrimoniais[30]. Apesar desse cenário, milhões de reais foram gastos pelo poder público com a contratação de empresas para a implementação do reconhecimento facial, sem qualquer regulamentação ou controle da eficiência, proporcionalidade e necessidade da tecnologia.

Na Bahia, Estado que apresentou um aumento de mais de 300% na letalidade policial entre os anos de 2013 e 2021, o governo investiu na empresa *Oi Móvel S/A* e no *software* da companhia chinesa *Huawei* tendo como meta a construção de um banco de dados com "todos os 15 milhões de baianos"[31]. Em 2019, foi assinado o contrato 03/2021 para a implementação do reconhecimento facial na capital e em 78 municípios baianos. A Administração Pública baiana não tem a gestão dos equipamentos, da infraestrutura ou dos *softwares*, que são fornecidos pela empresa contratada. O relatório aponta uma taxa de acerto de 3,6% e de 0,27% nos eventos que utilizaram essa tecnologia na cidade de Feira de Santana e da capital.

A partir de 2022, com o projeto *Câmera Interativa*, pretende-se ampliar a rede para incluir câmeras residenciais e de empresas privadas. A proposta é criar uma rede extensa e ramificada de vigilância, incluindo monitoramento em espaços privados[32]. Mas essa rede não possui estudos de impacto sobre a proteção dos dados pessoais, tampouco mecanismos claros de prevenção contra vieses discriminatórios e falsos positivos. Do mesmo modo que o Estado de Goiás, municípios com altos níveis de miséria e *déficit* educacional e sanitário foram "contemplados" com o projeto, que significou o gasto de mais de R$ 683 milhões[33].

29. NUNES; LIMA; RODRIGUES, 2023b.
30. NUNES; LIMA; RODRIGUES,2023b.
31. NUNES; LIMA; CRUZ, 2023a, p. 12.
32. NUNES; LIMA; CRUZ, 2023a, p. 20.
33. Para o aprofundamento do caso baiano, cf. FERREIRA; AMARAL, 2024, p. 45-58.

Na esfera federal, o projeto *IRIS*, da Receita Federal, tem por objetivo realizar a análise de risco por parametrização eletrônica e a identificação por biometria facial. De acordo com os autores, o grande desafio era "atingir o equilíbrio entre a liberação dos passageiros de forma ágil e a execução do controle aduaneiro"[34].

O sistema se estrutura a partir de cruzamento de dados dos passageiros enviados pelas companhias aéreas com dados da Polícia Federal, Interpol, Agência Brasileira de Inteligência. Esses dados são avaliados em conjunto com a Declaração Eletrônica de Bens de Viajante (e-DBV) para "analisar e selecionar com antecedência aqueles que representam um maior risco aduaneiro, baseado em critérios de seleção moduláveis"[35]. Após a seleção dos viajantes, a identificação do passageiro é realizada pela biometria facial à distância, que "permitirá a sua segregação dos outros passageiros e o respectivo encaminhamento para processo fiscalizatório, agilizando a liberação dos demais"[36]. O projeto destaca como consequência a especialização do foco em "passageiros de interesse, objetivo primário de aumento de segurança e mais conforto e celeridade ao fluxo de viajantes de baixo risco"[37]. À época da publicação, em 2019, informava-se a operacionalização do sistema em 14 aeroportos do país. No entanto, não há explicação sobre quais são os critérios de mensuração do risco, qual é a publicidade conferida à utilização dos equipamentos, a empresa fornecedora, o custo do projeto, e as cautelas na proteção de dados e no controle do viés discriminatório.

O quadro nacional, heterogêneo e desregulamentado, é sintomático de uma nova dimensão de biopoder, que conjuga a gestão modular e a customização do risco, materializando as "realidades verticais" entre os corpos aptos à circulação e aqueles sujeitos aos dispositivos securitários de antemão, como veremos nas próximas seções.

3. Anátomo-política dos corpos e biopolítica das populações: efeitos da governamentalidade algorítmica na customização do controle populacional

3.1. Do corpo adestrado à gestão modular do ambiente: duas faces do biopoder

O processo pelo qual emerge uma burguesia política no século XVIII, que implementa uma gramática jurídica de exercício de poder, encerra também a

34. BRASIL. MINISTÉRIO DA FAZENDA, 2019.
35. BRASIL. MINISTÉRIO DA FAZENDA, 2019.
36. BRASIL. MINISTÉRIO DA FAZENDA, 2019.
37. BRASIL. MINISTÉRIO DA FAZENDA, 2019.

formulação de dispositivos de controle dos corpos para a adequação ao regime econômico liberal[38]. O crescimento desse modelo econômico – e do modelo político que o acompanha – fez apelo à modalidade específica do poder disciplinar. Esse poder implicou numa política dos corpos, uma anátomo-política, vinculada a técnicas, mecanismos e tecnologias de submissão, adestramento, classificação, seleção e racionalização da lógica econômica[39].

A anátomo-política do corpo humano centra-se no corpo como máquina: "no seu adestramento, (...) no crescimento paralelo de sua utilidade e docilidade, na sua integração em sistemas de controle eficazes e econômicos"[40]. Foucault situa essa anátomo-política em um dos polos do desenvolvimento interligado de todo um feixe intermediário de relações. O outro polo se centra no corpo-espécie, isto é, no corpo transpassado pela mecânica do ser vivo e envolto em processos biológicos que podem ser medidas, calculados, examinados e ajustados. Nesse polo está a biopolítica[41].

Ao tratar sobre a biopolítica, Foucault observa como a nova arte de governar a partir do século XVIII assume características de um naturalismo no sentido fisiocrata: a gestão do ambiente a partir da descoberta de mecanismos espontâneos da economia; a condução política de conhecimento preciso, claro, contínuo e distinto do que acontece na sociedade, no mercado, nos circuitos econômicos; a liberdade como mercadoria produzida e gerida a partir do princípio de cálculo dessa produção: a segurança[42].

No âmago da nova razão governamental se insere o jogo entre liberdade e segurança que contornam a economia de poder própria do liberalismo. Se no antigo sistema político existia entre o soberano e o súdito uma série de relações jurídica e econômicas que traziam para o primeiro a obrigação de proteção do último contra o perigo, no liberalismo é diferente. Essa arte de governar fundada na organização de interesses transita entre a gestão dos perigos e os mecanismos de segurança e liberdade:

> "Podemos dizer que, afinal de contas, o lema do liberalismo é 'viver perigosamente'. 'Viver perigosamente' significa que os indivíduos são postos perpetuamente em situação de perigo, ou antes, são condicionados a experimentar sua situação, sua vida, seu presente, seu futuro como portadores de perigo.

38. FOUCAULT, 1987, p. 182.
39. FOUCAULT, 1987, p. 182.
40. FOUCAULT, 1999, p. 131.
41. FOUCAULT, 1999, p. 131.
42. FOUCAULT, 2008a, p. 84-89.

> E é essa espécie de estímulo do perigo que vai ser, a meu ver, uma das principais implicações do liberalismo."[43]

Assim, segundo Foucault, o liberalismo pressupõe uma educação e uma cultura do perigo. O perigo cotidiano, perpetuamente animado, atualizado, posto em circulação, o que atrairá, por exemplo, um interesse jornalístico pelo crime a partir de meados do século XIX[44]. E se agora o perigo pudesse ser extraído das faces, como pretendiam os fisiognomistas do século XIX?

Essa ideia de perigo em circulação, que é própria da razão liberal, é chave para compreender o princípio de funcionamento das tecnologias de reconhecimento facial. Ao mesmo tempo que esses sistemas garantem aceleração no processo de checagem, ingresso e fruição de serviços – a exemplo de controles de passaporte em aeroportos –, projetam sobre as faces monitoradas *scores* de risco que indicam os corpos com doses de perigo que acionam o mecanismo de segurança. E nisso se difere ao mesmo tempo em que se agrega ao regime disciplinar.

No regime disciplinar se investe em um tipo de individualização descendente que reclama a produção de um modo de subjetivação específico de ambientes de controle e confinamento:

> "Esse espaço fechado, recortado, vigiado em todos os seus pontos, onde os indivíduos estão inseridos num lugar fixo, onde os menores movimentos são controlados, onde todos os acontecimentos são registrados, onde um trabalho ininterrupto de escrita liga o centro e a periferia, onde o poder é exercido sem divisão, segundo uma figura hierárquica contínua, onde cada indivíduo é constantemente localizado, examinado e distribuído entre os vivos, os doentes e os mortos – isso tudo constitui um modelo compacto do dispositivo disciplinar."[45]

A grande questão da gestão das massas em movimento, para a razão liberal, era até então, diferentemente das práticas disciplinares, a questão do exercício desse tipo individualizado de controle. Justamente porque as massas, a população, estava sujeita a uma arte própria de governar que Foucault designou como biopolítica: uma forma de tratar a população como um conjunto de seres vivos afetados por processos próprios da vida – nascimento, morte, doença, (re)produção – e coexistentes que apresentam características biológicas e patológicas específicas[46].

43. FOUCAULT, 2008a, p. 90.
44. FOUCAULT, 2008a, p. 90.
45. FOUCAULT, 1987, p. 163.
46. FOUCAULT, 2008b, p. 494.

Não significa, em qualquer hipótese, a exclusão das técnicas de disciplina, mas sim um novo campo de articulação dessas técnicas com os dispositivos de regulação. À anátomo-política do corpo humano se agrega, no final do século XVIII, a biopolítica da espécie humana[47].

Desse modo, no que diz respeito às formas de controle, na biopolítica estamos diante de técnicas e dispositivos que não operam no nível da subjetivação, como no caso dos regimes disciplinares, mas no ambiente. É o que Deleuze reflete na transição entre o controle disciplinar e o controle biopolítico: "os confinamentos são moldes, distintas moldagens, mas os controles são uma modulação"[48]. Disciplina do corpo e regulação da população, explica Chignola, são os dois polos constitutivos em torno dos quais se desenvolveu a organização do poder sobre a vida, um biopoder calcado em uma tecnologia de duas faces[49].

3.2. Biopolítica granular: os efeitos da governamentalidade algorítmica na gestão customizada das populações

Nesta seção, analisaremos como as transformações das técnicas de regulação, especialmente a partir do emprego da lógica algorítmica nas tecnologias de *surveillance*, podem sobrepor os dois polos constitutivos do biopoder. Antes, porém, é necessário compreender como a governamentalidade algorítmica opera aos níveis do indivíduo e da população.

Antoniette Rouvroy e Thomas Berns distinguem três etapas da governamentalidade algorítmica: o *dataveillance,* o *datamining* e o *datanticipating*[50]. O *dataveillance* é caracterizado pela coleta e conservação automatizada de uma quantidade massiva de dados não classificados, constitutiva do *Big Data.* Esses dados são extraídos das mais diversas atividades no fluxo digital, como pesquisas em buscadores, troca de mensagens em redes sociais, postagens, curtidas, preenchimento de formulários em lojas virtuais etc. São chamados por Rouvroy como constitutivos do "comportamentalismo digital", pois exprimem as múltiplas facetas do real, desdobrando-o em sua totalidade, mas de maneira segmentada.

São sinais expurgados de um ato individual em que não se pretende investigar a complexidade do sujeito que o realiza, mas apenas e de forma bem objetiva o conteúdo do sinal. Ao realizarmos uma compra *online,* por exemplo, a máquina não está preocupada se o produto se destina a um casamento ou a um velório, o seu estado emocional e o sentido daquele comportamento naquele momento da sua vida; está

47. FOUCAULT, 2008b, p. 514.

48. DELEUZE, 1992, p. 221.

49. CHIGNOLA, 2018.

50. ROUVROY; BERNS, 2015.

preocupada em identificar o padrão da compra, o usuário, o dia e horário e, com isso, prospectar padrões em meio a um emaranhado gigantesco de outros dados.

Isso nos leva à segunda etapa da governamentalidade algorítmica, o *datamining,* que se caracteriza pelo tratamento dessa quantidade massiva de dados de modo a fazer emergir sutis correlações, muitas vezes até mesmo indecifráveis, que são construídas a partir desse verdadeiro garimpo digital.

Nesse estágio, a heterogeneidade de informações não classificadas dá lugar à homogeneidade dos resultados extraídos a partir do mecanismo maquínico relacional. É como se a produção do saber se transformasse em um elemento absolutamente objetivo de triagem cujas normas emergem do próprio real. Essas correlações apelam à ideia da neutralidade maquínica, mas cuja grande questão é saber em que nível a programação para tratamento e a própria origem dos dados não está contornada de subjetivismo que são próprios às relações humanas.

Nesse ponto, vale lembrar o que Cathy O'Neil nos explica sobre os algoritmos de destruição matemática. Os algoritmos são modelos compostos por um conjunto de instruções que representam abstratamente algum processo destinado a extrair alguns resultados buscados pelos criadores desses modelos. A neutralidade não existe nem nos dados coletados nem nos modelos estruturados, tampouco na interpretação dos resultados obtidos[51]. As decisões algorítmicas, assim, não deveriam ser fetichizadas como "apenas matemáticas", o que tende a desviar o fato de que a *big data* é uma tecnologia marcada por uma inevitabilidade do social que é próprio das relações e ações humanas[52].

O terceiro momento identificado por Rouvroy e Berns consiste no uso desses saberes probabilistas e estatísticos para antecipar os comportamentos individuais, sempre a partir de um mecanismo preditivo aplicado aos perfis determinados pela mineração a partir de uma base de correlações estabelecidas. É aqui que tomam lugar os *scores de crédito* para obtenção de um financiamento, para a contratação de um seguro, para uma vaga de emprego, para a formulação dos anúncios direcionados e, até mesmo, alguns modelos computacionais para a análise do risco de reincidência criminal.

Esses três momentos se relacionam e são retroalimentados na conformação da governamentalidade algorítmica, identificada pelos autores como um tipo de racionalidade (a)normativa ou (a)política que embasa na coleta, agregação e análise automatizada de dados em quantidade massiva de modo a modelizar, antecipar e afetar os comportamentos possíveis[53].

51. O'NEIL, 2020, p. 22.

52. BRAYNE, 2021, p. 166.

53. ROUVROY; BERNS, 2015. p. 42.

Se o século XIX é marcado pela efervescência da estatística como métrica de governança do corpo social, o século XXI testemunha a passagem do governo estatístico para o governo algorítmico que encaminha a rarefação dos processos de subjetivação[54]. A régua do homem médio de que tratava Quetelet[55] dá lugar a uma aparente individualização da estatística.

Mas essa individualização pouco tem a ver com a então categoria do indivíduo. Está relacionada ao perfil extraído de uma multiplicidade de correlações que determinaram a probabilidade do comportamento futuro (perfil de bom/mau pagador; perfil saudável/doente; perfil criminoso/bom cidadão etc.).

Como o fluxo de dados se transforma em uma condição imanente da própria vida (basta pensar na indispensabilidade dos aparelhos telefônicos, aplicativos de comunicação e outras facilidades), o sistema pressupõe o consentimento/adesão tácita do indivíduo ao modelo de governo. Disso decorre o "declínio da reflexividade subjetivante e o distanciamento das ocasiões de contestação das produções de 'saber' fundadas no *datamining* e na elaboração dos perfis"[56]. A governamentalidade algorítmica escapa assim à contestação, alimentando-se de fragmentos individuais insignificantes aos olhos humanos para criar modelos de comportamento e perfis sem precisar ou se preocupar em interpelar o sujeito, tampouco trazê-lo ao debate sobre o que ele é ou o que pode se tornar. É um padrão monológico de gestão das subjetividades sem sujeito.

A sua perfeita adequação à viralidade – cada dado é incorporado, e até mesmo os desvios – garante que as falhas serão reassimiladas na definição dos modelos e perfis de comportamento. Nas palavras de Rouvroy e Berns:

> "(...) seguindo o objetivo do aplicativo que é feito de dispositivos algorítmicos – por exemplo, a prevenção das fraudes, do crime, do terrorismo – os 'falso positivos' não serão nunca interpretados como 'falhas' uma vez que o sistema segue uma lógica de rastreamento mais do que de diagnóstico: o objetivo é não deixar escapar qualquer positivo verdadeiro, qualquer que seja a taxa de falsos positivos."[57]

É um jogo em que a banca determina as regras e as chances do jogador, mas que não para de embaralhar as cartas para expurgar qualquer perspectiva histórica ou genealógica. O jogador é atravessado pelos múltiplos perfis que lhe são atribuídos, muitas vezes de maneira automática com base nos rastros digitais de sua existência.

54. ROUVROY; BERNS, 2015.
55. SEKULA, 1986, p. 3-64.
56. ROUVROY; BERNS, 2015, p. 42.
57. ROUVROY; BERNS, 2015, p. 42.

Não se trata mais de atingir um corpo físico ou a sua consciência moral para adequá-lo ao padrão do jogo, mas sim de determinar quais são os caminhos possíveis dentro do tabuleiro com base nos caminhos que já foram traçados no passado. Aqui Rouvroy e Berns enxergam uma aproximação com o conceito de dispositivo de segurança de Foucault, não tão preocupado em fixar os limites ou moldar o sujeito, mas sim em determinar as posições e espaços de circulação[58].

Diferentemente da disciplina, que é centrípeta e opera isolando um espaço e um segmento no qual seu poder e os mecanismos correlatos funcionarão plenamente, os dispositivos de segurança são centrífugos e tendem a se ampliar perpetuamente:

> "(...) novos elementos são o tempo todo integrados, integra-se a produção, os comportamentos, as maneiras de fazer dos produtores, dos compradores, dos consumidores, dos importadores, dos exportadores, integra-se o mercado mundial. Trata-se, portanto, de organizar ou, em todo caso, de deixar circuitos cada vez mais amplos se desenvolverem.[59]

É a partir desse aspecto que Andrejevic et al. analisam a "biopolítica granular" nas tecnologias de reconhecimento facial, mormente após a pandemia de Covid, a partir de 2019, que acelerou os processos de gestão biométrica à distância[60]. Os autores apontam que o imperativo de distanciamento social acelerou o desenvolvimento e o emprego de formas de monitoramento e detecção que, mais à frente, permitiriam expandir as formas "dividualizadas" de controle social. A biopolítica granular permite, então, dentro do paradigma da regulação (biopolítica), customizar a intervenção (anátomo-política) ao mesmo tempo que expande os níveis de modulação.

Na perspectiva fisiocrata, o *milieu* se referia ao padrão obtido das análises estatísticas. Assim, o desvio era extraído a partir do que a régua média definisse como "normal". E se essa régua pudesse ser customizada ao nível do indivíduo? Na pesquisa conduzida por Andrejevic, que acompanhou por 18 meses reuniões e eventos de empresas de tecnologia facial, os autores perceberam o sutil desenvolvimento dessa nova forma de gestão ambiental.

Executivos de empresas de tecnologia de reconhecimento facial anunciavam novos modelos que seriam capazes de distinguir, a partir da leitura do rosto, os níveis de acesso ou risco dos indivíduos monitorados. Encontrar pontualmente na multidão e aplicar o modelo ao perfil. Em um dos eventos acompanhados pela equipe de pesquisa de Andrejevic, um representante da Schindler, especializada

58. ROUVROY; BERNS, 2015.

59. FOUCAULT, 2008, p. 59.

60. ANDREJEVIC; O'NEILL; SMITH; SELWYN; GU, 2024, p. 1204-1226.

em elevadores, apresentou um estudo de caso de um edifício em Singapura em que o sistema de reconhecimento instalado nos elevadores era capaz de identificar as faces e apontar em qual andar a pessoa deveria descer. Sem botões ou teclas. O rosto carrega consigo a indicação de quais níveis são permitidos ou proibidos de ingressar[61].

A biopolítica granular proporciona o tipo de controle individualizado do regime disciplinar sem o imperativo da subjetificação e, ao mesmo tempo, modula as regras do jogo ao nível médio da população, garantindo uma forma de controle que investe no ambiente, mas não apenas, como também no indivíduo[62].

O conjunto de companhias que investem nas tecnologias de reconhecimento facial, desde a elaboração de *softwares* de comparação, passando pelos *hardwares* de armazenamento e equipamento de operacionalização, iniciou, na esteira do imperativo de distanciamento, o câmbio entre privacidade e conveniência. Como David Clark, pesquisador no *MIT* e membro do Hall da Fama da *Internet*, observou, as pessoas tendem a privilegiar a conveniência independentemente das consequências negativas futuras[63].

Ingressos em estádios de futebol, filas de aeroportos e estações ferroviárias, acesso a condomínios e hotéis, métodos de pagamento, tudo feito sem a necessidade de senhas bancárias ou contato, apenas com a biometria facial, acelerando os fluxos de reconhecimento e pagamento. É o que Shade identificou como *friction-free surveillance capitalism,* o imperativo comercial de produtos sem fricção, contato entendido agora como um obstáculo à aceleração dos fluxos[64].

Os fluxos automatizados do reconhecimento facial, observam Andrejevic et al., caminham na mesma direção de uma economia política de velocidade, em que a aceleração dos processos de circulação e troca é uma condição da lucratividade dos mercados. No entanto, essa é uma realidade de experiência com a tecnologia de reconhecimento facial que não é a mesma para todos. Indivíduos pertencentes a grupos considerados de risco carregam em suas faces esta marca, traduzido na codificação algorítmica como um objeto de especial atenção da máquina para correspondência com a lista de comparação.

A pandemia, nesse aspecto, serviu como um laboratório de tecnologias de controle que, posteriormente, foram reconfiguradas para esse monitoramento do risco de forma individual. Na Índia, equipamentos de reconhecimento facial instalados para monitoramento da quarentena médica em casa passaram a ser utilizados para

61. ANDREJEVIC; O'NEILL; SMITH; SELWYN; GU, 2024, p. 1204-1226.

62. ANDREJEVIC; O'NEILL; SMITH; SELWYN; GU, 2024, p. 1204-1226.

63. RAINIE; ANDERSON, 2017.

64. SHADE, 2020.

garantir o cumprimento da prisão domiciliar. No Reino Unido, uma companhia especializada na produção de equipamentos de monitoramento de idosos foi contratada para produzir relógios com reconhecimento facial capazes de rastrear a localização de migrantes que foram acusados da prática de delitos. Os monitorados precisam escanear a face e realizar o *login* com a geolocalização nos relógios cinco vezes ao dia (Selwyn et al., 2024, p. 19).

Cabe salientar que a análise sobre o poder que Foucault realiza não parte do nível da teoria política, mas sim dos mecanismos, técnicas e tecnologias do poder (Foucault, 2003, p. 241). As modificações entre poder soberano de "deixar viver e fazer morrer" e o poder disciplinar de "fazer viver e deixar morrer" são compreendidas por grades de análises que estudarão exatamente como essas técnicas e dispositivos centradas no corpo se encarregaram de realizam a distribuição espacial, a separação, a classificação, a vigilância e o controle sobre os corpos (Foucault, 2003, p. 242).

Além do regime disciplinar centrado no corpo, Foucault observou a emergência, a partir da segunda metade do século XVIII, de uma nova tecnologia de poder centrada no ser humano como ser vivo e que tem como objeto a população. Essa camada de poder não é focada na individualização do corpo, mas no controle dos corpos enquanto massa na população. Essa camada é a biopolítica (Foucault, 2003, p. 243). Também aqui a doença tem um papel central, pois enquanto o poder disciplinar respondeu às epidemias que causaram a morte de milhões, a biopolítica lida com a doença como uma questão endêmica, em outras palavras, "a forma, a natureza, a extensão, a duração e a intensidade da doença prevalente na população" (Foucault, 2003, p. 243).

Andrejevic et al. (2024) observam a mesma transformação no que diz respeito ao tratamento da Covid-19. Primeiro como questão epidêmica sujeita a técnicas de gestão disciplinar, mas atualmente como uma forma endêmica, sujeita a controle por meio de taxas de ocorrência, número de leitos ocupados, óbitos etc. O óbito em si não é um problema, mas desde que não ultrapasse o *milieu*. Esse modelo de engenharia ambiental biopolítico, se analisado a partir do nível de técnicas e dispositivos, alcança uma nova dimensão a partir do emprego de sistemas de biometria facial à distância que permitem costumizar a governança ambiental:

> "Como a análise foucaultiana sugere, a resposta à Covid-19 se enquadra melhor na trajetória geral da resposta excepcional para a gestão endêmica. (...) Uma gama crescente de doenças (e outras formas de percepção de risco) pode ser submetida à lógica da biopolítica granular (...). As medidas gerais de morbidade e mortalidade tornam-se cada vez mais especificadas, abrangendo grupos cada vez menores – resultando em pontuações de risco customizadas e probabilidades

> individualizadas. Estes, por sua vez, exigem respostas personalizadas em tempo real: modulação ambiental direcionada e antecipação do risco. O momento pandêmico ajuda assim a destacar o modelo de bipolítica granular antecipado pela perspectiva de monitoramento em tempo real customizado das massas" (trad. livre).

As tecnologias de reconhecimento facial se propõem a realizar essas projeções de risco individualizadas em meio à multidão. Propõem uma arquitetura de modulação própria da biopolítica, em que pavimentam os caminhos da circulação da população ao mesmo tempo em que investem sobre o corpo individual que acione o limiar de risco, o que nos remete a formas de controle e intervenção típicas da anátomo-política.

A biopolítica granular ilumina esse ponto de customização das formas de intervenção sobre as massas. Possui como pressupostos os reclamos de automação e aceleração do tempo próprio do regime econômico, a conveniência nas relações econômicas e sociais, a multiplicação de fronteiras não físicas de controle, a modulação do espaço e o tipo endêmico de gestão. É, nessa esteira, que Andrejevic et al. propõem uma lógica pós-população que dialoga com a governamentalidade algorítmica na reflexão sobre modelos que dispensam a reflexividade humana, alimentados por dados granulares individuais que não possuem qualquer significado se vistos isoladamente, para construir modelos de comportamento ou perfil supraindividuais[65].

Smart é uma designação que destaca o fator de conveniência para a incorporação de máquinas que coletam, estratificam e gerenciam a circulação do público em tempo real, mas sem que isso se traduza em uma realidade homogênea. A intervenção será de forma individual de acordo com o grau de risco atribuído a cada indivíduo a partir da análise das suas características faciais. Nesse contexto, as propostas *smart* são o retorno, no século XXI, dos modelos fisiognomistas do século XIX, sob nova roupagem na qual a discriminação por fenótipo é objeto de uma blindagem tecnocrata a partir do discurso da neutralidade e da objetividade maquínica. Não é a superação dos dispositivos de disciplina, controle ou segurança, mas a sua intensificação aos níveis do ambiente e do indivíduo codificados.

4. Considerações finais

Tal como na formação das técnicas disciplinares, a doença assume um papel relevante na estruturação da biopolítica granular. A dicotomia biológico-patológico,

65. ANDREJEVIC; O'NEILL; SMITH; SELWYN; GU, 2024, p. 1204-1226.

central na emergência das medidas disciplinares de contenção da Covid-19, moldou novas formas de sistemas de controle à distância, com destaque à biometria facial, que atendessem às demandas de circulação próprias do regime econômico.

Com o crescimento exponencial de câmeras de alta definição e da capacidade operacional de sistemas de armazenamento de dados, a partir da década de 2010, verifica-se uma virada visual nas tecnologias de reconhecimento facial pautadas em torno da noção de risco. Esse movimento não teria sido possível sem a adesão subjetiva às fotografias e filmagens com capturas faciais disponibilizadas na *internet* e capturadas em larga escala por companhias privadas. Nesse caminho se entrecruzam realidade verticais entre os circuitos de exposição e segurança no regime de visibilidade moderno. Para determinados grupos, a conveniência do *frictionfree surveillance capitalism* tem prevalecido sobre preocupações com violações da privacidade. Para outros, a experiência com os sistemas biométricos tem significado a multiplicação de fronteiras invisíveis de controle sobre os corpos.

Essa ambiguidade da relação entre a tecnologia e os grupos populacionais já está presente no cenário nacional onde projetos como o IRIS, da Receita Federal, classificam indivíduos mediante cruzamento automatizado de dados e reconhecimento facial. Aliado ao risco de discriminação sistêmica, a forma de espraiamento da biometria facial no Brasil causa preocupações no que diz respeito à falta de transparência, à municipalização da segurança pública, ao *déficit* na relação custo-efeito, ao locupletamento de empresas sem condições técnicas de gestão e à violação em massa de dados pessoais sensíveis.

Nesse cenário, se observa um tipo de gestão modular que é própria da biopolítica afetada à altura de técnicas que permitem, agora, a absorção de um controle customizado no nível da corporificação individual de risco. Kelly Gates descreve como *mass individuation* o processo de extensão das tecnologias de reconhecimento automatizado por toda a população e, simultaneamente, o tratamento de cada indivíduo como um caso específico (Gates, 2011, p. 15). A autora identifica esse processo como uma estratégia moderna de governo para segurança e gestão da população; um modelo regulatório que conjuga modulação com conhecimento detalhado da identidade de cada membro para diferenciar indivíduos de acordo com níveis de acesso, privilégio e risco (Gates, 2011, p. 15).

O século XXI testemunha a passagem do governo estatístico para o governo algorítmico em que, dentro do paradigma da regulação, customiza-se a intervenção individualmente sem demandar apenas processos disciplinares. A "novidade" tecnológica da empresa de elevadores Schindler está longe de ser uma metáfora do que o sistema projeta para o futuro: representa a realidade de indivíduos carregando na face quais andares são acessíveis ou proibidos dentro da circulação social.

Uma biopolítica granular gestionará tal fluxo de acordo com o que convenha ao jogo algorítmico.

Os dois polos foucaultianos de biopoder se expressam num emergente tipo de controle, a biopolítica granular, em que uma governamentalidade algorítmica não está somente preocupada com o adestramento do corpo, mas também comprometida com a diferenciação dos corpos em circulação e seus imanentes alertas de perigo que carregam como marca.

Referências

AMARAL, Augusto Jobim do; DIAS, Felipe da Veiga. *Tecnopolítica criminal*. São Paulo: Tirant lo Blanc, 2024.

AMOORE, Louise. Biometric borders: Governing mobilities in the war on terror. *Political Geography*, n. 25, 2006. p. 336-351.

ANDREJEVIC, Mark. *Automated Media*. New York: Teylor & Francis, 2020.

ANDREJEVIC, Mark; O'NEILL, Chris; SMITH, Gavin; SELWYN, Neil; GU, Xin. Granular biopolitics: facial recognition, pandemics and the securitization of circulation. *New media & society*, v. 26 (3), p. 1204-1226, 2024.

AUGUSTO, Acácio et al. O legado securitário após 10 anos da Copa do Mundo FIFA no Brasil. *Boletim (anti)segurança*, n. 36, Lasintec, p. 2-8, 2025.

BEIRA Rio irá testar sistema de reconhecimento facial contra bagunceiros. *UOL Notícias*. Disponível em: [https://copadomundo.uol.com.br/noticias/redacao/2014/04/19/beira-rio-ira-testar-sistema-de-reconhecimento-facial-contra-bagunceiros.htm]. Acesso em: 30.01.2025.

BENJAMIN, Ruha. *Race after technology*: Abolitionist Tools for the New Jim Code. Cambridge: Polity Press, 2019.

BLEDSOE, W.W. *Letter from Woody Bledsow to Dr. Samuel Koslov regarding facial recognition to determine racial and environmental backgrounds*. The University of Texas History. Briscoe Center for American History. Palo Alto, CA, 1965.

BRASIL. MINISTÉRIO DA FAZENDA. Coordenação-Geral de TI da Receita Federal. *Projeto IRIS:* reconhecimento facial de viajantes. Disponível em: [http://repositorio.enap.gov.br/handle/1/4132]. Acesso em: 02.12.2024.

BRASIL. MINISTÉRIO DA FAZENDA. *Projeto Iris:* reconhecimento facial de viajantes. Brasília: ENAP, 2019. Disponível em: [https://repositorio.enap.gov.br/jspui/handle/1/4132]. Acesso em: 20.03.2025.

BRAYNE, Sarah. *Predict and Surveil*: data, discretion, and the future of policing. Oxford: Oxford University Press, 2021.

BRUNO, Fernanda. *Máquinas de ver, modos de ser*: vigilância, tecnologia e subjetividade. Porto Alegre: Sulina, 2013.

BRUNO, Fernanda. Visões maquínicas da cidade maravilhosa: do centro de operações do Rio à Vila Autódromo. In: BRUNO, Fernanda et al. (Orgs.). *Tecnopolíticas da vigilância*: perspectivas da margem. São Paulo: Boitempo, 2018. p. 239-256.

CHIGNOLA, Sandro. A toupeira e a serpente. Trad. Augusto Jobim do Amaral. *R. Dir. Gar. Fund*., Vitória, v. 19, n. 3, p. 239-270, set.-dez. 2018.

DELEUZE, Gilles. *Conversações*, 1972-1990. Trad. Peter Pál Pelbart. Rio de Janeiro: Ed. 34, 1992.

DUSHI, Desara. The use of facial recognition technology in EU law enforcement: Fundamental rights implications. In: *Global Campus South East Europe*, 2020.

FERREIRA, Ana Gabriela; AMARAL, Augusto Jobim do. Solucionismo Tecnológico na Segurança Pública Brasileira: o caso do reconhecimento facial na Bahia. In: SARLET et al. (Orgs.). *Tecnologia e antidiscriminação*. Londrina: Thoth, 2024. p. 45-58.

FOUCAULT, Michel. *Vigiar e punir*: nascimento da prisão. Trad. Raquel Ramalhete. Petrópolis: Vozes, 1987.

FOUCAULT, Michel. *História da sexualidade I*: a vontade de saber. Trad. Maria Thereza da Costa Albuquerque e J. A. Guilhon Albuquerque. 13. ed. Rio de Janeiro: Edições Graal, 1999.

FOUCAULT, Michel. *Society must be defended*: lectures at the Collège de France, 1975-1976. Transl. David Macey. New York: Picador, 2003.

FOUCAULT, Michel. *Nascimento da biopolítica*: curso dado no Collège de France (1978-1979). Trad. Eduardo Brandão. São Paulo: Martins Fontes, 2008a.

FOUCAULT, Michel. *Segurança, território e população*: curso dado no Collège de France (1977-1978). Trad. Eduardo Brandão com revisão de Claudia Berliner. São Paulo: Martins Fontes, 2008b.

GAMA, Guilherme. Reconhecimento facial: seis foragidos da Justiça foram localizados no Carnaval de Salvador. *CNN Brasil*, São Paulo, 10.02.2024. Disponível em: [www.cnnbrasil.com.br/nacional/reconhecimento-facial--seis-foragidos-da-justica-foram-localizados-no-carnaval-de-salvador/]. Acesso em: 12.01.2025.

GATES, Kelly A. *Our biometric future*: facial recognition technology and the Culture of Surveillance. New York: New York University Press, 2011.

GENTILE, Giulia. Does Big Brother Exist? Facial Recognition Technology in the United Kingdom. In: MATULIONYTE, Rita; ZALNIERIUTE, Monika (Orgs.). *The Cambridge Handbook of Facial Recognition in the Modern State*. Cambridge: Cambridge University Press, 2024.

GROTHER, Patrick; NGAN, Mei; HANAOKA, Kayee. Face Recognition Vendor Test – Part 3: Demographic Effects. *National Institute of Standards and*

Technology. U.S. Departmente of Commerce, 2019. Disponível em: [https://doi.org/10.6028/NIST.IR.8280]. Acesso em: 13.01.2025.

HARCOURT, Bernard E. *Exposed*: Desire and Desobedience in the Digital Age. Cambridge/London: Harvard Massachusetts Press, 2015.

HARCOURT, Bernard. On critical genealogy. *Contemporary Political Theory*, 2024. [https://doi.org/10.1057/s41296-024-00715-y].

ISRAEL, Carolina B. et al. *Reconhecimento facial nas escolas públicas do Paraná*. Curitiba, UFPR, 2023.

LIMA, Thallita et al. *Vigilância por lentes opacas*: mapeamento da transparência e responsabilização nos projetos de reconhecimento facial no Brasil. Rio de Janeiro: CESeC, 2024.

MARTINS, Laís. Vigilância turbinada: Ministério da Justiça comprou secretamente tecnologia que coleta fotos sem autorização para reconhecimento facial. *The Intercept Brasil*. Disponível em: [www.intercept.com.br/2025/02/03/ministerio-da-justica-comprou-secretamente-tecnologia-que-coleta-fotos-sem-autorizacao-para-reconhecimento-facial/]. Acesso em: 18.03.2025.

MATULIONYTE, Rita; ZALNIERIUTE, Monika. *The Cambridge Handbook of Facial Recognition in the Modern State*. Cambridge: Cambridge University Press, 2024.

NATIONAL INSTITUTE OF STANDARDS AND TECNHOLOGY. *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*. Dec.19.2019. Disponível em: [www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software]. Acesso em: 20.01.2025.

NUNES, Pablo; LIMA, Thallita G. L.; CRUZ, Thaís G. *O sertão vai virar mar*: expansão do reconhecimento facial na Bahia. Rio de Janeiro: CESeC, 2023a.

NUNES, Pablo; LIMA, Thallita G. L.; RODRIGUES, Yasmin. *Das planícies ao planalto*: como Goiás influenciou a expansão do reconhecimento facial na segurança pública brasileira. Rio de Janeiro: CESeC, 2023b.

O PANÓPTICO. *Monitor de novas tecnologias na segurança pública do Brasil*. Disponível em: [www.opanoptico.com.br/#regioes]. Acesso em: 20.03.2025.

O'NEIL, Cathy. *Algoritmos de destruição em massa*: como o *big data* aumenta a desigualdade e ameaça a democracia. Trad. Rafael Abraham, Santo André: Editora Rua do Sabão, 2020.

PREFEITURA de SP lança 'prisômetro' em meio a críticas da Defensoria sobre uso de reconhecimento facial no Carnaval. *G1*, São Paulo, 25.02.2025. Disponível em: [https://g1.globo.com/sp/sao-paulo/carnaval/2025/noticia/2025/02/25/prefeitura-de-sp-lanca-prisometro-em-meio-a-criticas-da-defensoria-sobre-uso-de-reconhecimento-facial-no-carnaval.ghtml]. Acesso em: 18.03.2025.

RAINIE, Lee; ANDERSON, Janna. *The Internet of Things Connectivity Binge*: What Are de Implications? 2017. Available at: [www.pewresearch.org/internet/2017/06/06/the-internet-of-things-connectivity-binge-what-are-the--implications/]. Acesso em: 16.02.2025.

ROUVROY, Antoinette; BERNS, Thomas. *Governamentalidade algorítmica e perspectivas de emancipação*: o díspar como condição de individuação pela relação? Trad. Pedro Henrique Andrade. *Revista Eco Pós*, v. 18, n. 2, 2015.

SEKULA, Allan. *The Body and the Archive*. October, v. 39 (Winter, 1986).

SELWYN, Neil; ANDREJEVIC, Mark; O'NEILL, Chris; GU, Xin; SMITH, Gavin. Facial Recognition Technology: Key Issues and Emerging Concerns. In: MATULIONYTE, Rita; ZALNIERIUTE, Monika (Orgs.). *The Cambridge Handbook of Facial Recognition in the Modern State*. Cambridge: Cambridge University Press, 2024.

SHADE, Leslie R. Nudging interventions in regulating the digital gangsters in an era of frictionfree surveillance capitalism. In: BOLER; DAVIS (Orgs.). *Affective Politics of Digital Media*: Propaganda by Other Means. London: Routledge. 2020. p. 314-329.

SILVA, Tarcízio. *Racismo algorítmico*: inteligência artificial e discriminação nas redes digitais. São Paulo: SESC, 2022.

SOUSA, Raquel et al. *Esporte, dados e direitos*: o uso de reconhecimento facial nos estádios brasileiros. Rio de Janeiro: CESeC, 2024.

SOUZA, Roberta de. Carnaval do Rio terá monitoramento com reconhecimento facial e drones, divulga governo em plano de segurança. *O Globo,* Rio de Janeiro, 05.02.2024. Disponível em: [https://oglobo.globo.com/rio/carnaval/noticia/2024/02/05/carnaval-do-rio-tera-monitoramento-com-reconhecimento-facial-e-drones-divulga-governo-em-plano-de-seguranca.ghtml]. Acesso em: 12.06.2024.

WANG, Jackie. Esta é uma história sobre nerds e policiais: PredPol e Policiamento Algorítmico. In: *Capitalismo Carcerário*. Trad. Bruno Xavier. São Paulo: Igrá Kniga, 2022. p. 209-230.

Recebido em: 30.03.2025.
Aprovado em: 25.04.2025.
Última versão dos autores: 25.04.2025.

PESQUISA DO EDITORIAL

Área do Direito: Penal; Digital; Constitucional

Veja também Doutrina relacionada ao tema

- Meios de obtenção de prova na fase preliminar criminal: considerações sobre reconhecimento pessoal no brasil e na legislação comparada, de Rafael Francisco França – *RBCCrim* 112/331-366, *Doutrinas Essenciais Direito Penal e Processo Penal* 6; e
- Valoração da prova digital: entre a desconfiança e a crença, de Luíza Guimarães Campos Batista Gomes e André Ricardo Godoy de Souza – *RePro* 359/175-207.

Veja também Jurisprudência relacionada ao tema

- STJ, EDcl no AgRg no HC 966772, j. 25.04.2025, *DJe* 30.04.2025.

Travassos, Gabriel Saad; Amaral, Augusto Jobim do. Reconhecimento facial:
biopolítica granular e controle customizado no Brasil.
Revista Brasileira de Ciências Criminais. vol. 211. ano 33. p. 143-168. São Paulo: Ed. RT, nov./dez. 2025.
DOI: [doi.org/10.5281/zenodo.17058382].

O uso da inteligência artificial na predição do feminicídio e o direito à explicabilidade e à autodeterminação informativa

The use of artificial intelligence in the prediction of femicide and the right to explainability and informational self-determination

Assista aos comentários da autora sobre este artigo

Araceli Martins Beliato[1]
Universidade de São Paulo, USP, Brasil.
araceli.beliato@usp.br

DOI: [doi.org/10.5281/zenodo.17058373].

Área do Direito: Penal; Digital; Constitucional

Resumo: O presente artigo examina criticamente os limites éticos e jurídicos do uso da inteligência artificial na formulação de políticas públicas voltadas à predição de feminicídios, com especial atenção aos riscos impostos à privacidade, ao sigilo médico e à autodeterminação informativa. Toma-se como estudo de caso o projeto desenvolvido por *Vital Strategies* e FrameNet Brasil, que analisou, sem o consentimento expresso das pacientes, registros médicos de mulheres vítimas de violência doméstica atendidas na rede pública de saúde de Recife-PE. A partir dessa experiência concreta, discutem-se a opacidade algorítmica, os usos secundários dos dados sensíveis e os

Abstract: This article critically examines the ethical and legal boundaries of using artificial intelligence in the development of public policies aimed at predicting femicides, with particular attention to the risks posed to privacy, medical confidentiality, and informational self-determination. As a case study, it analyzes the project developed by Vital Strategies and FrameNet Brasil, which examined medical records of women victims of domestic violence treated in the public health system in Recife without their explicit consent. From this concrete experience, the article explores algorithmic opacity, the secondary use of sensitive data, and the effects of digital

1. Doutoranda em Direito Processual Penal na Faculdade de Direito da Universidade de São Paulo (FD-USP). Mestre em Direito Político e Econômico e Bacharel em Direito pela Universidade Presbiteriana Mackenzie.
Currículo Lattes: [http://lattes.cnpq.br/3002635574708602].
ORCID: [https://orcid.org/0009-0001-2332-8645].
E-mail: araceli.beliato@usp.br.

efeitos da vigilância digital sobre corpos vulnerabilizados. O texto também investiga a tendência de relativização dos direitos fundamentais sob o discurso da segurança pública e demonstra como as tecnologias que se apresentam como soluções de proteção podem, na prática, reforçar estruturas de poder, criminalização e controle social. Propõe, ao final, uma reconfiguração normativa e institucional que resgate os princípios da privacidade, da transparência e da dignidade humana diante do processo de tecnificação crescente das políticas públicas de segurança e saúde.

Palavras-chave: Proteção de dados – Privacidade – Opacidade – Sigilo médico – Feminicídios.

surveillance on vulnerable bodies. It also investigates the growing trend of relativizing fundamental rights under the discourse of public security, demonstrating how technologies presented as protective tools may, in practice, reinforce structures of power, criminalization, and social control. The research ultimately advocates for a normative and institutional reconfiguration capable of restoring the principles of privacy, transparency, and human dignity in the face of the increasing technification of public health and security policies.

Keywords: Data protection – Privacy – Opacity – Medical confidentiality – Femicides.

Sumário: 1. Introdução. 2. Noções propedêuticas sobre Inteligência Artificial (IA). 2.1. Conceitos de IA. 2.2. Aplicações da IA na segurança pública e na saúde. 3. Proteção de dados, privacidade e autodeterminação informativa: aspectos legais. 3.1. Sistema brasileiro. 3.1.1. Proteção de dados. 3.1.2. Privacidade. 3.1.3. Autodeterminação informativa. 3.2. União Europeia. 3.3. Sigilo médico. 4. Opacidade algorítmica. 4.1. Conceito e níveis de opacidade. 4.2. Explicabilidade. 5. Relativização de direitos fundamentais para fins de segurança pública. 6. Considerações finais. Referências bibliográficas. Legislação.

1. Introdução

"Os donos dos dados são os donos do futuro".

Yuval Noah Harari (2018, p. 102)

No dia 21 de dezembro de 2024, foi amplamente veiculado na mídia o resultado de um estudo produzido por pesquisadores da organização internacional de saúde pública *Vital Strategies*, em colaboração com o laboratório de linguística computacional FrameNet Brasil da Universidade Federal de Juiz de Fora (UFJF), o qual concluiu que algoritmos podem prever, com até 92 dias de antecedência, padrões de atendimento médico que indicam o risco de agravamento da violência doméstica contra mulheres. Foram analisados, no Recife-PE, os prontuários de saúde de 13 mil mulheres atendidas ao longo de dez anos, sem o consentimento explícito delas. Os resultados também incluem a constatação de que antes de sofrerem agressões mais graves ou fatais, as vítimas alteravam seus padrões de visitas às unidades básicas de saúde para buscar mais atendimentos e relatar problemas de saúde mental (Folha de São Paulo, 2024; Motta, 2024; O Tempo, 2024; Vianez, 2025).

Embora a violência contra as mulheres figure como um dos temas mais urgentes e que iniciativas para reduzir os altos índices no Brasil sejam indispensáveis, a proposta em questão – recebida por muitos entusiastas como um "marco na prevenção de feminicídios" – levanta questões fundamentais sobre privacidade, autodeterminação informativa e o uso de dados sensíveis não consentidos.

A hipótese aqui ventilada é de que a utilização de informações médicas sem o consentimento expresso das pacientes compromete garantias essenciais de privacidade e de controle sobre os próprios dados. Mais do que isso, contribui para legitimar práticas de vigilância biomédica desprovidas de amparo normativo. O acesso a prontuários sob o argumento da prevenção do feminicídio pode, na prática, abrir caminho para o uso indiscriminado de dados sensíveis, com base na ideia de que certas violações individuais seriam toleráveis em nome de um suposto bem coletivo.

Ainda que se alegue que os dados pessoais das vítimas foram anonimizados, como consta nas reportagens mencionadas, exsurgem diversos questionamentos: se não há identificação individual, como garantir uma intervenção eficaz? A privacidade de algumas mulheres pode ser negociada para supostamente prevenir a violência de modo geral? Quem garante que essas informações não serão usadas para outros fins? E, sobretudo, até que ponto confiar na tecnologia para resolver problemas estruturais não seria uma forma de desviar o foco de soluções políticas e sociais mais efetivas?

Para além da proteção à privacidade, é preciso examinar criticamente uma ideia que costuma ser mobilizada para relativizar as garantias fundamentais: a segurança pública. Nos últimos anos, diversos governos e empresas recorreram ao argumento da repressão ao crime organizado ou ao terrorismo para justificar a ampliação de práticas de vigilância que restringem liberdades individuais. Em muitos casos, o discurso da segurança tem servido como ferramenta para a expansão de dispositivos de controle social e para legitimar a supressão de direitos em nome de um bem coletivo que raramente se realiza de forma equitativa.

A partir da literatura selecionada, é possível observar a produção de conhecimento sobre mulheres vítimas de violência como um mecanismo de controle social, especialmente com base nos conceitos de biopoder e biopolítica desenvolvidos por Foucault (2005). Nesse sentido, a lógica foucaultiana pode ser aplicada para entender como a produção de conhecimento estatístico e biomédico pode servir ao controle e predição do comportamento das vítimas, amplificado em larga escala pelo *big data*.

O objetivo principal é refletir sobre como iniciativas tecnológicas que se apresentam como instrumentos de proteção podem, na realidade, reforçar estruturas de poder e perpetuar formas de controle social que restringem direitos das próprias pessoas que anunciam como protegidas.

2. Noções propedêuticas sobre Inteligência Artificial (IA)

2.1. Conceitos de IA

O conceito de Inteligência Artificial (IA) se apresenta como um construto teórico e tecnológico em desenvolvimento. Embora o próprio significado de "inteligência" não seja unívoco e desperte diversas interpretações e controvérsias epistemológicas, a IA se refere, fundamentalmente, à construção de sistemas computacionais capazes de desempenhar tarefas que normalmente, exigiriam habilidades cognitivas humanas, como raciocínio, aprendizado, resolução de problemas e capacidade de adaptação.

Cozman e Neri (2021, p. 22) advertem sobre a fluidez desses conceitos e como vão sendo superados a partir do desenvolvimento humano, social e tecnológico: "o que hoje é considerado uma atividade inteligente pode se tornar uma atividade banal assim que suas regras são codificadas de forma computacional".

Na visão de Russell e Norvig (2021, p. 8, tradução livre), IA é o "o estudo de agentes que recebem percepções do ambiente e realizam ações"[2]. "Estudo de agentes" significa investigar, projetar e construir sistemas que percebem seu ambiente e agem sobre ele, com o objetivo de alcançar metas ou objetivos definidos. Essa perspectiva técnica é conhecida como a abordagem do agente racional, que domina a obra dos autores e marca uma mudança importante no campo: em vez de focar em "imitar o ser humano", a IA passa a ser vista como a construção de sistemas autônomos, adaptativos e orientados a metas, capazes de perceber e agir racionalmente em diferentes ambientes.

Neste ponto, convém esclarecer que os algoritmos[3] formam a base lógica e operacional de qualquer sistema de inteligência artificial. Em termos simplificados, um algoritmo é um conjunto finito e ordenado de instruções ou regras formuladas

2. Texto original: "We define AI as the study of agents that receive percepts from the environment and perform actions".

3. Um algoritmo é uma sequência finita e bem definida de instruções ou operações destinadas a resolver um problema específico ou realizar uma tarefa. Donald E. Knuth, renomado cientista da computação e autor da obra "The Art of Computer Programming", caracteriza um algoritmo por cinco propriedades fundamentais: a) finitude: o algoritmo deve sempre concluir após um número limitado de etapas; b) definição precisa: cada instrução deve ser claramente especificada, sem ambiguidades, assegurando que as ações a serem executadas sejam rigorosamente definidas; c) entrada (*input*): o algoritmo recebe zero ou mais entradas, que são os dados fornecidos antes ou durante sua execução; d) saída (*output*): produz uma ou mais saídas, que são os resultados relacionados às entradas processadas; e) eficácia: todas as operações devem ser suficientemente simples para serem executadas de forma exata e em tempo finito por um agente computacional (Knuth, 1997, p. 4-6).

de modo preciso, destinado à execução de uma tarefa ou à solução de um problema, e pode ser projetado para aprender e se adaptar a partir de dados, ajustando parâmetros internos para melhorar seu desempenho (característica central dos métodos de *machine learning* e *deep learning*). Assim, enquanto a IA se circunscreve ao campo mais amplo do desenvolvimento de sistemas capazes de simular capacidades cognitivas humanas, o algoritmo é o instrumento técnico que materializa essas capacidades, definindo como o sistema processa informações, toma decisões e interage com o ambiente.

Cozman e Cortese (2019) relembram que o interesse pelo desenvolvimento de inteligências artificiais não é recente, mas encontra sua gênese histórica em propostas iniciais como o teste de Turing[4], concebido por Alan Turing em 1950[5], que busca identificar inteligência por meio da capacidade de um sistema simular convincentemente a comunicação humana.

No âmbito jurídico, o Conselho Nacional de Justiça (CNJ), na Resolução 332/2020, que tratou inicialmente da utilização da IA no Poder Judiciário brasileiro, não apresentou definição de IA, mas definiu "modelo de Inteligência Artificial" como:

> "[...] conjunto de dados e algoritmos computacionais, concebidos a partir de modelos matemáticos, cujo objetivo é oferecer resultados inteligentes, associados ou comparáveis a determinados aspectos do pensamento, do saber ou da atividade humana." (Brasil, 2020, art. 3º, II)

Em 12 de dezembro de 2024, foi aprovada nova minuta na 9ª Reunião do Grupo de Trabalho, que resultou na versão final consolidada na Resolução 615, de 11 de março de 2025, a qual passou a prever no art. 4º, inc. IX, a seguinte definição de "inteligência artificial generativa" (IA generativa ou IAGen): "sistema de IA especificamente destinado a gerar ou modificar significativamente, com diferentes níveis de autonomia, texto, imagens, áudio, vídeo ou código de software" (Brasil, 2025).

4. "De forma simplificada: nesse jogo há um juiz humano que interage com duas outras entidades sem vê-las; uma das entidades é um ser humano e a outra é um dispositivo artificial. O "teste" é simples: se o juiz humano não conseguir distinguir entre o dispositivo e o ser humano, então o primeiro é qualificado como inteligência artificial" (Cozman; Cortese, 2019, p. 60).
5. Matemático britânico que, durante a Segunda Guerra Mundial, atuou em Bletchley Park na decodificação dos sistemas criptográficos alemães. Após o fim do conflito, Turing concentrou seus esforços no desenvolvimento de um computador com capacidade de pensamento, publicando em 1950 um dos trabalhos pioneiros sobre o assunto, intitulado *Computing Machinery & Intelligence*.

Em complemento, o inciso I apresenta a definição de "sistema de inteligência artificial (IA)", que consiste em:

> "[...] sistema baseado em máquina que, com diferentes níveis de autonomia e para objetivos explícitos ou implícitos, processa um conjunto de dados ou informações fornecido e gera resultados prováveis e coerentes de decisão, recomendação ou conteúdo, que possam influenciar o ambiente virtual, físico ou real." (Brasil, 2025)

A ausência de consenso em torno do conceito de IA ainda representa um desafio acadêmico e impacta diretamente a precisão e a efetividade dos mecanismos de regulação. É evidente que essa dificuldade não decorre apenas da complexidade técnica do tema, mas do fato de que se trata de um objeto que atravessa dimensões econômicas, políticas, culturais e jurídicas profundamente distintas entre países e blocos regionais.

2.2. Aplicações da IA na segurança pública e na saúde

O uso de inteligência artificial em setores como a segurança pública e a saúde tem se expandido de forma acelerada, impulsionado tanto pelo avanço tecnológico quanto pela busca por respostas mais eficazes a problemas sociais de alta complexidade. No campo da segurança, ferramentas algorítmicas vêm sendo incorporadas à rotina das instituições policiais com o objetivo de aperfeiçoar ações preventivas e investigativas, sobretudo por meio do cruzamento de grandes volumes de dados e da identificação de padrões que possam antecipar ocorrências criminosas. Segundo Telles:

> "Ferramentas de policiamento preditivo estão sendo implementadas pelos departamentos de polícia da América do Norte, Europa Ocidental e partes da Ásia. Os departamentos de polícia geralmente usam mapas térmicos indicando os locais e horários em que a probabilidade de crime é mais alta. [...] Essa chamada 'estratégia de policiamento de hot spots', mesclando análise de dados com policiamento direcionado, existe há mais de duas décadas" (Telles, 2021, p. 251).

Modelos de aprendizado de máquina capazes de prever áreas geográficas com maior probabilidade de ocorrência criminal já são realidade em vários países, o que permite a alocação de recursos com precisão e eficácia superiores aos métodos tradicionais (Ferguson, 2019).

Ratcliffe (2019), por exemplo, demonstra como algoritmos bem ajustados conseguem reduzir significativamente as taxas de criminalidade urbana por meio da otimização das rondas policiais e da ampliação da presença ostensiva em pontos identificados como críticos. Nesse sentido:

> "São diversos os estados e municípios que passaram a utilizar câmeras de reconhecimento facial, drones com captação de imagens e afins, ferramentas estas já na esteira do maior escopo proporcionado por algoritmos de policiamento preditivo, reforçando uma tendência de incremento na adoção de tecnologias preditivas" (Ambrosio; Barbosa, 2024, p. 76).

Além disso, tecnologias de reconhecimento facial têm sido amplamente integradas à vigilância urbana e aeroportuária, possibilitando, supostamente, a identificação rápida de indivíduos procurados pela justiça ou suspeitos de envolvimento em atividades criminosas. Embora promissora, essa aplicação enfrenta críticas fundamentadas em potenciais riscos à privacidade e em erros relacionados a vieses algorítmicos, especialmente contra minorias étnicas (Buolamwini; Gebru, 2018). O que se tem visto, no entanto, é a expansão dessas tecnologias, sem debate público, muitas vezes sem regulamentação específica e sem qualquer transparência quanto aos critérios adotados ou aos dados utilizados em sua calibração.

A eficácia técnica da IA depende da qualidade dos dados que a alimentam. Em sociedades como a nossa, os dados disponíveis tendem a refletir os mesmos vieses e preconceitos que a estruturam. Assim, em vez de neutralizar as injustiças, os algoritmos podem reforçá-las, e classificar determinados territórios ou populações como de "alto risco", com base em padrões herdados da seletividade penal (Lum; Isaac, 2020; Završnik, 2019; Oliveira, 2024; FBSP, 2025). Richardson et al. (2019) acrescentam que essa lógica favorece a supercriminalização de grupos já vulnerabilizados e perpetua práticas discriminatórias sob a aparência de racionalidade estatística.

No campo da saúde, as ferramentas baseadas em IA têm sido bastante úteis para apresentar diagnósticos precoces, especialmente na identificação de cânceres, doenças cardíacas e patologias neurológicas. Métodos de processamento avançado de imagens médicas por algoritmos de aprendizado profundo alcançam níveis de precisão diagnóstica comparáveis ou superiores aos de especialistas humanos, reduzindo erros e permitindo intervenções mais eficazes[6] e tempestivas (Esteva et al., 2019; Pham et al., 2017; Topol 2019):

> "Na medicina, isso está começando a ter impacto em três níveis: para os profissionais de saúde, principalmente por meio da interpretação rápida e precisa de imagens; para os sistemas de saúde, ao melhorar o fluxo de trabalho e o potencial de redução de erros médicos; e para os pacientes, ao capacitá-los a processar seus próprios dados para promover a saúde" (Topol, 2019, p. 44).

6. Topol (2019, p. 45) aponta que "um algoritmo de aprendizado profundo pode interpretar as imagens 150 vezes mais rápido do que os radiologistas (1,2 contra 177 segundos)".

Ao discorrer sobre o *DeepCare,* arquitetura de rede neural recorrente do tipo *Long Short-Term Memory* (LSTM), projetada especificamente para processar registros médicos eletrônicos, Pham et al. mencionam que:

> "A medicina preditiva personalizada exige a modelagem dos processos relacionados à doença e ao tratamento do paciente, que têm dependências temporais de longo prazo. [...] DeepCare explicitamente modela intervenções médicas capazes de modificar o curso da doença e influenciar futuros riscos médicos" (Pham et al., 2017, p. 218).

Para os autores, o *DeepCare* é capaz de armazenar o histórico de enfermidades de um paciente, inferir seu estado atual de saúde e prever desfechos clínicos futuros. Sua principal inovação está na habilidade de lidar com dados irregulares ao longo do tempo e em modelar o impacto das intervenções médicas ao longo das internações, sendo eficaz tanto para prever a progressão de doenças quanto para recomendar tratamentos personalizados. Tem sido particularmente usado em pacientes com diabetes e com transtornos mentais, e supostamente supera métodos tradicionais em tarefas como: previsão de progressão da doença; indicação de procedimentos clínicos; e cálculo de risco futuro (como mortalidade ou nova internação) (Pham et al., 2017).

Outro uso crescente é a aplicação de sistemas de IA na vigilância epidemiológica e no controle de surtos infecciosos. Durante a pandemia da COVID-19, algoritmos avançados foram essenciais para monitorar a disseminação do vírus em tempo real, prever picos de infecção e planejar estratégias adequadas de contenção e distribuição de recursos médicos, tais como leitos hospitalares e vacinas, otimizando consideravelmente a resposta das autoridades sanitárias (Vaishya et al., 2020).

Embora as aplicações de inteligência artificial na segurança pública e na saúde revelem potencial, persistem dilemas como a opacidade, os riscos à privacidade e os impactos desiguais das decisões automatizadas, que demandam atuação coordenada entre especialistas, juristas e formuladores de políticas para assegurar sistemas auditáveis, sensíveis ao contexto e compatíveis com marcos de proteção de direitos.

3. Proteção de dados, privacidade e autodeterminação informativa: aspectos legais

3.1. Sistema brasileiro

3.1.1. Proteção de dados

O ordenamento jurídico brasileiro tem avançado significativamente na salvaguarda dos direitos fundamentais atinentes à proteção de dados pessoais, à

privacidade e à autodeterminação informativa. Esses direitos são alicerçados em dispositivos constitucionais, legislações específicas e projetos de lei em tramitação, que refletem a crescente preocupação com a tutela das informações pessoais no cenário digital contemporâneo.

A Constituição Federal de 1988, em seu art. 5º, inc. X, assegura a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, garantindo o direito de indenização pelo dano material ou moral decorrente de sua violação. Adicionalmente, a Emenda Constitucional 115, promulgada em 2022, introduziu o inc. LXXIX ao art. 5º, e estabeleceu que é assegurado, nos termos da lei, o direito à "proteção dos dados pessoais, inclusive nos meios digitais" (Brasil, 2022). Essa inclusão eleva a proteção de dados pessoais ao *status* de direito fundamental, em reforço ao entendimento já manifestado pelo Supremo Tribunal Federal[7], que reconheceu implicitamente esse direito, associando-o a princípios como a dignidade da pessoa humana e aos direitos à privacidade e à intimidade (Sarlet, 2025).

No plano infraconstitucional, a Lei 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD ou LGPDP), é a responsável por regular as atividades de tratamento de dados pessoais. Contudo, ela não se aplica às situações relacionadas à "segurança pública" e à "investigação e repressão de infrações penais", conforme dispõe o art. 4º, inc. III, alíneas "a" e "d", bem como o § 1º do mesmo artigo, que determina expressamente a necessidade de uma legislação específica para tratar dessas matérias, ainda pendente de criação – a chamada LGPD Penal (Brasil, 2018).

De acordo com o art. 5º da LGPD, "dado pessoal" é toda informação relacionada a pessoa natural identificada ou identificável (inc. I). Dado pessoal sensível, por sua vez, refere-se a "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (inc. II). Já o dado anonimizado é definido como aquele "relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento" (inc. III) (Brasil, 2018).

É importante destacar que, desde 2014, com a promulgação do Marco Civil da Internet (Lei 12.965/2014), já se reconhecia a proteção de dados e a privacidade

7. Decisão paradigmática proferida pelo Plenário, chancelando provimento monocrático, em sede de liminar, da ministra Rosa Weber no bojo da ADI 6.387 MC-Ref/DF (julgada com as ADIs 6.388, 6.389, 6.390 e 6.393). Em oportunidades posteriores o STF também se manifestou no mesmo sentido, *v.g.* ADI 5.545, HC 222.141, ADI 6.529, ADI 6.649 e a ADPF 695.

como direitos fundamentais, reforçando a exigência do tratamento adequado das informações dos usuários no ambiente digital brasileiro.

Outro marco significativo foi a adesão do Brasil à Convenção de Budapeste, formalizada por meio do Decreto 11.491/2023, voltada ao combate aos crimes cibernéticos e que visa harmonizar as legislações nacionais dos países signatários, estabelecer a criminalização de condutas ilícitas no ambiente digital, definir normas para a investigação e produção de provas, além de fortalecer os mecanismos de cooperação jurídica internacional, como a extradição e a assistência jurídica mútua (Brasil, 2023).

Do ponto de vista doutrinário, o conceito de "dado" pode ser entendido como informação ainda não processada, ou seja, um elemento bruto da informação. Para Setzer (2015), dado é "uma sequência de símbolos quantificados ou quantificáveis", sendo que "quantificável significa que algo pode ser quantificado e depois reproduzido sem que se perceba a diferença para com o original". Assim, textos, fotos, figuras, sons gravados e animações também são considerados dados, pois podem ser introduzidos em um computador e quantificados de tal modo que sua reprodução se torne praticamente indistinguível do original.

Zuboff (2021), por outro lado, define dados como vestígios digitais resultantes das atividades humanas, tanto on-line quanto off-line, que são capturados, analisados e empregados para prever e influenciar comportamentos. Esses dados são extraídos das interações dos indivíduos com as tecnologias – desde pesquisas na internet e postagens em redes sociais até o uso de aplicativos e movimentações físicas monitoradas por dispositivos como *smartphones*, relógios inteligentes e veículos conectados.

Para a autora, os dados extrapolam as informações básicas, como nome e endereço, e englobam comportamentos, preferências, sentimentos e até estados emocionais. Após serem capturados, esses dados são transformados em produtos preditivos, que permitem às empresas tecnológicas anteciparem e moldarem o comportamento dos usuários para fins comerciais. Essa prática representa uma invasão da privacidade e modifica profundamente a dinâmica entre consumidores e empresas, porque desloca o poder para quem detém e manipula os dados. Desse modo, os dados se tornam a matéria-prima do chamado "capitalismo de vigilância", cujo valor reside na capacidade de prever e influenciar as ações futuras dos indivíduos (Zuboff, 2021).

3.1.2. Privacidade

Privacidade, em sua dimensão mais ampla, refere-se ao direito, constitucionalmente assegurado (CF, art. 5º, X), de o indivíduo receber proteção contra

interferências arbitrárias ou abusivas de terceiros, sejam eles particulares ou órgãos governamentais, na sua vida privada e intimidade. É também reconhecida no art. 12 da Declaração Universal dos Direitos Humanos, no art. 17 do Pacto Internacional sobre Direitos Civis e Políticos e em muitos outros instrumentos internacionais e regionais de direitos humanos.

A relevância da privacidade se relaciona diretamente à proteção da dignidade humana e à preservação da autonomia individual, valores centrais em democracias constitucionais. Moraes (2025, loc. 148) preleciona que:

> "Desta forma, a defesa da privacidade deve proteger o homem contra: (a) a interferência em sua vida privada, familiar e doméstica; (b) a ingerência em sua integridade física ou mental, ou em sua liberdade intelectual e moral; (c) os ataques à sua honra e reputação; (d) sua colocação em perspectiva falsa; (e) a comunicação de fatos relevantes e embaraçosos relativos à sua intimidade; (f) o uso de seu nome, identidade e retrato; (g) a espionagem e a espreita; (h) a intervenção na correspondência; (i) a má utilização de informações escritas e orais; (j) a transmissão de informes dados ou recebidos em razão de segredo profissional."

Ainda que consolidadas no plano jurídico, essas garantias vêm sendo tensionadas por transformações tecnológicas que, nas últimas décadas, têm remodelado profundamente as formas de vigilância, controle e acesso à informação. A própria essência da privacidade está sendo alterada pela lógica subjacente à operação das tecnologias de IA, particularmente pelos algoritmos de aprendizado profundo, cuja eficácia depende diretamente da constante coleta e processamento de grandes volumes de informações pessoais.

O relatório do Gabinete do Alto Comissariado das Nações Unidas para os Direitos Humanos alerta que a privacidade, na era digital, enfrenta ameaças de amplitude inédita. Entre elas, destaca-se o uso indiscriminado de ferramentas de hackeamento, capazes de invadir dispositivos, interceptar comunicações e extrair dados sem consentimento, expandindo indevidamente o alcance da vigilância estatal e privada. Soma-se a isso a importância estratégica da criptografia, cuja integridade é condição indispensável para a proteção de comunicações, informações sensíveis e para a preservação de outros direitos correlatos. Por fim, o monitoramento extensivo de espaços públicos, viabilizado por câmeras inteligentes e sistemas de reconhecimento facial, fomenta a coleta massiva de dados biométricos e comportamentais (UN, 2022), instaurando, por assim dizer, um novo arranjo panóptico, que reconfigura a experiência da presença no espaço coletivo e molda condutas sob a lógica da vigilância permanente.

Esses desafios contemporâneos acabam por afetar a estrutura conceitual da privacidade, mas também os instrumentos jurídicos que a resguardam. Entre esses,

o consentimento informado ocupa posição estratégica, pois funciona como condição de legitimidade para a coleta e o tratamento de dados pessoais. Contudo, no ambiente digital, esse consentimento se torna cada vez mais difícil de ser efetivado, especialmente devido aos longos contratos de adesão, à opacidade das políticas de privacidade e à assimetria de informações entre usuários e provedores de tecnologia (Solove, 2020).

Outra preocupação central envolve a cibersegurança. Embora a IA necessite acessar dados amplos e detalhados para funcionar adequadamente, cada vez mais incidentes de vazamento ou utilização indevida de dados pessoais vêm à tona, expondo cidadãos a potenciais prejuízos econômicos, sociais e psicológicos. Consequentemente, pesquisadores e ativistas têm defendido mecanismos mais eficientes de auditoria e controle sobre a gestão dessas informações para minimizar riscos e promover maior transparência das operações baseadas em IA.

3.1.3. Autodeterminação informativa

A autodeterminação informativa ou informacional é "um conceito jusfilosófico que se refere ao controle que um indivíduo tem sobre suas próprias informações pessoais;" [...] "trata-se da autonomia do indivíduo em relação ao gerenciamento e proteção de suas informações privadas", e envolve cinco garantias principais: a) consentimento informado: o uso dos dados exige autorização clara e consciente da pessoa, com base em informações acessíveis; b) acesso e transparência: o titular dos dados deve saber quais informações são coletadas, como são usadas e por quem; c) correção e exclusão: é possível corrigir dados incorretos e pedir a exclusão de dados desnecessários; d) segurança: quem trata os dados deve protegê-los contra acessos indevidos, perdas ou vazamentos; e) portabilidade: o titular pode transferir seus dados entre serviços ou provedores de forma simples e segura (Beliato, 2025a, p. 71-72).

Esse conceito surgiu na Alemanha, a partir da decisão do Tribunal Constitucional Federal, em 1983[8], que reconheceu a prerrogativa individual de determinar a divulgação e utilização de seus dados pessoais, fundamentando-se nos princípios da dignidade humana e do livre desenvolvimento da personalidade (Sarlet, 2021). Convém ressaltar que, ainda segundo Sarlet (2021), não há qualquer hierarquia entre os direitos à proteção de dados, à privacidade e à autodeterminação informativa, e que esses institutos não se confundem. A autodeterminação informativa possui uma dimensão dupla: individual, ao garantir que cada pessoa decida sobre o uso de seus dados pessoais; e coletiva, ao funcionar como condição essencial para

8. Para aprofundamento do tema vide Mendes (2020).

uma ordem comunicacional livre e democrática, superando visões individualistas e isolacionistas da privacidade, como o tradicional "direito de estar só".

Embora a expressão "autodeterminação informativa" não apareça literalmente no texto do Marco Civil da Internet (Lei 12.965/2014), seu conteúdo essencial foi ali incorporado, ao estabelecer que o tratamento de dados pessoais depende do consentimento livre e informado do titular, garantir o acesso às informações sobre o uso de seus próprios dados e reconhecer a privacidade como direito fundamental no ambiente digital. Dessa forma, o Marco Civil concretiza, de forma implícita, o princípio da autodeterminação informativa, antecipando diretrizes que seriam posteriormente detalhadas pela LGPD. Esta, em seu art. 2º, II, apesar de não conceituar "autodeterminação informativa", consagra-a expressamente entre seus fundamentos e confere aos titulares de dados pessoais direitos como acesso, correção, exclusão e portabilidade de suas informações. Buarque e Ehrhardt Júnior (2023) alertam que o modelo de consentimento informado previsto na LGPD revela-se insuficiente diante das assimetrias de poder entre controladores e titulares, da opacidade nos termos de uso e da complexidade dos sistemas algorítmicos.

Esse cenário é agravado por uma economia digital sustentada pela monetização dos dados pessoais, muitas vezes cedidos como contrapartida para o uso de serviços considerados essenciais, como preconizado pela Zuboff (2021).

> "O consentimento, embora previsto como expressão livre, informada e inequívoca, é frequentemente condicionado ao acesso a serviços digitais, tornando-se uma exigência desprovida de substância" (Buarque; Ehrhardt Júnior, 2023, p. 87).

Segundo Yan Chang, "a essência do direito à autodeterminação da informação é enfatizar o controle pessoal dos cidadãos sobre seus dados" (Chang, 2023, p. 19). Tal perspectiva implica reconhecer o consentimento como critério central para legitimar qualquer forma de coleta, tratamento ou compartilhamento de dados. Como reafirma a autora: "o cerne do direito à informação pessoal é o direito à autodeterminação, isto é, o direito de o titular decidir se, como e em que medida suas informações podem ser conhecidas por terceiros" (Chang, 2023, p. 22).

A autodeterminação informativa é reconhecida, também, pela Corte Interamericana de Direitos Humanos (Corte IDH) como um direito humano autônomo, essencial para a proteção da privacidade e do livre desenvolvimento da personalidade. Esse reconhecimento foi consolidado em outubro de 2023, quando a Corte afirmou expressamente que a Convenção Americana sobre Direitos Humanos implica o direito à autodeterminação informativa, permitindo que indivíduos acessem e controlem seus dados pessoais mantidos em arquivos públicos (Corte IDH, 2023). Com efeito, no julgamento do emblemático caso "Corporação Coletivo de

Advogados José Alvear Restrepo" (CAJAR) vs. Estado da Colômbia, a Corte IDH determinou que as atividades de vigilância e inteligência realizadas sem o devido controle e consentimento dos indivíduos violaram o direito à autodeterminação informativa dos membros do CAJAR (Beliato, 2025b).

A proteção da autodeterminação informativa no âmbito interamericano reflete uma tendência global de reconhecer a importância do controle individual sobre os dados pessoais e fortalece a obrigação dos Estados de implementar medidas que garantam esse direito e promovam a transparência e a proteção da privacidade, em consonância com os princípios democráticos e os direitos humanos.

3.2. União Europeia

No contexto europeu, o Regulamento Geral sobre a Proteção de Dados (GDPR – *General Data Protection Regulation*), formalizado como Regulamento (UE) 2016/679, representa a principal legislação sobre proteção de dados pessoais, servindo como referência internacional. Aprovado em abril de 2016, entrou em vigor em 25 de maio de 2018, substituindo a anterior Diretiva 95/46/CE e harmonizando as normas de privacidade e segurança de dados em toda a União Europeia (UE).

O GDPR se aplica a todas as entidades, públicas ou privadas, que processem dados pessoais de residentes da UE, independentemente da localização geográfica da organização. Isso significa que empresas situadas fora do território europeu, mas que oferecem bens ou serviços a indivíduos na UE ou monitoram seu comportamento, também estão sujeitas às disposições do regulamento.

Entre os princípios fundamentais estabelecidos pelo GDPR estão: a licitude, lealdade e transparência no tratamento dos dados; a limitação da finalidade da coleta e uso das informações; a minimização dos dados coletados, que devem ser estritamente necessários para os fins pretendidos; a exatidão das informações, assegurando sua atualização e correção; a limitação da conservação dos dados, que só devem ser mantidos pelo tempo necessário; e a integridade e confidencialidade, por meio da adoção de medidas técnicas e organizacionais capazes de proteger os dados contra acessos não autorizados ou ilícitos, bem como contra perdas e danos acidentais. O GDPR também consagra expressamente a autodeterminação informativa (UE, 2016).

O regulamento confere aos titulares diversos direitos, como o acesso às informações pessoais que lhes dizem respeito; o direito de retificação de dados imprecisos ou incompletos; o direito ao apagamento dos dados em determinadas situações (conhecido como "direito ao esquecimento"); o direito à restrição do tratamento dos dados; o direito à portabilidade dos dados, que permite ao titular transferir seus dados para outro controlador; o direito de oposição ao tratamento em

determinadas circunstâncias; e a proteção contra decisões baseadas unicamente em tratamento automatizado, inclusive *profiling*, que possam produzir efeitos jurídicos ou igualmente significativos para o titular.

Entidades que lidam com dados pessoais têm o dever de obter o consentimento dos titulares de forma clara, livre, específica, informada e inequívoca. Além disso, devem adotar medidas técnicas e administrativas adequadas para garantir a segurança das informações sob sua custódia. Em caso de violação, a comunicação à autoridade supervisora competente deve ocorrer em até 72 horas após a detecção do incidente.

Em determinadas circunstâncias, também se exige a nomeação de um Encarregado pelo Tratamento de Dados Pessoais (*Data Protection Officer* – DPO), cuja função consiste em acompanhar o cumprimento das normas de proteção de dados e atuar como ponto de contato com os órgãos reguladores.

O regulamento prevê sanções severas para os casos de descumprimento, com multas que podem atingir até 4% do faturamento anual global da organização, ou € 20 milhões, o que for maior (UE, 2016).

Além do GDPR, a União Europeia avançou na regulamentação da inteligência artificial com a aprovação, em 2024, do *Artificial Intelligence Act* (*AI Act*), Regulamento (UE) 2024/1689. Trata-se de um regulamento pioneiro que estabelece um quadro jurídico unificado para o desenvolvimento, comercialização e utilização de sistemas de IA nos Estados-Membros. O objetivo central do *AI Act* é assegurar que tais sistemas sejam seguros, transparentes, éticos e compatíveis com os direitos fundamentais dos cidadãos europeus (UE, 2024).

O *AI Act* adota uma abordagem regulatória baseada no risco, classificando os sistemas de IA conforme o potencial de causar danos. Sistemas de risco inaceitável, que representem ameaça direta aos direitos fundamentais, como o social *scoring* utilizado por governos, são proibidos. Aplicações de alto risco, como as utilizadas em áreas sensíveis como saúde, educação, recrutamento e infraestrutura crítica, estão sujeitas a obrigações rigorosas, incluindo avaliações de conformidade e exigências de supervisão humana. Sistemas de risco limitado devem garantir transparência e informar os usuários sobre sua natureza automatizada, enquanto sistemas de risco mínimo, como filtros de *spam* ou jogos digitais, não estão sujeitos a requisitos adicionais.

Os principais objetivos do *AI Act* incluem a proteção dos direitos fundamentais, a promoção de um ambiente favorável à inovação por meio de instrumentos como *sandboxes* regulatórias, e o fortalecimento da transparência e da responsabilidade dos desenvolvedores e operadores de IA. A regulamentação reforça a posição da União Europeia como referência global no tratamento ético da inteligência artificial, embora enfrente desafios quanto à sua implementação uniforme entre os

Estados-Membros e à adequação de suas exigências às realidades econômicas e tecnológicas do setor privado (UE, 2024).

3.3. Sigilo médico

O sigilo médico é um princípio ético-jurídico essencial, pautado pela relação de confiança entre médico e paciente, e que impõe ao profissional da saúde a obrigação de preservar em segredo todas as informações às quais tiver acesso em razão do exercício da sua atividade. Esse dever de confidencialidade tem como fundamento basilar a proteção da privacidade, da dignidade humana e da autonomia individual, permitindo que o paciente tenha liberdade plena para fornecer informações sensíveis sem o temor de exposição indevida.

O sigilo médico encontra respaldo normativo no art. 5º, inc. X, da Constituição Federal, que garante a inviolabilidade da intimidade e da vida privada das pessoas. Além disso, está previsto no art. 154 do Código Penal, que criminaliza a violação do segredo profissional e no Código de Ética Médica[9], do Conselho Federal de Medicina (CFM), que determina ao profissional o dever de preservar a confidencialidade das informações obtidas no exercício profissional, mesmo após o término do atendimento ou após o falecimento do paciente (arts. 73 a 79 do Código de Ética Médica).

Há, entretanto, situações excepcionais em que o sigilo médico pode ser legitimamente relativizado, especialmente quando sua manutenção representa risco concreto à saúde pública ou perigo imediato para o paciente ou para terceiros. Exemplo clássico consiste na comunicação obrigatória às autoridades sanitárias sobre doenças de notificação compulsória, como as previstas na Lei 6.259/1975: "I – de doenças que podem implicar medidas de isolamento ou quarentena, de acordo com o Regulamento Sanitário Internacional" e "II – de doenças constantes de relação elaborada pelo Ministério da Saúde, para cada Unidade da Federação, a ser atualizada periodicamente" (vide Brasil, 1975, arts. 7º a 13).

No caso de violência doméstica, a Lei 13.931, de 10 de dezembro de 2019, alterou a Lei 10.778, de 24 de novembro de 2003, para estabelecer a notificação compulsória dos casos de suspeita ou confirmação de violência contra a mulher atendida em serviços de saúde públicos ou privados. Conforme o novel § 4º do art. 1º, os profissionais de saúde são obrigados a comunicar tais casos à autoridade policial no prazo de 24 horas, tanto para a adoção das providências cabíveis quanto para fins estatísticos.

9. Resolução CFM 2.217, de 27 de setembro de 2018, modificada pelas Resoluções CFM 2.222/2018 e 2.226/2019.

Nesses casos, o interesse público prevalece sobre o direito individual à privacidade, porém, a quebra do sigilo deve se restringir às informações necessárias e pertinentes à situação específica.

Quanto à responsabilidade decorrente da violação do sigilo médico, pode haver consequências no âmbito penal, ético-disciplinar e no civil. Penalmente, conforme o mencionado art. 154 do Código Penal, o profissional pode ser condenado à pena de detenção de três meses a um ano ou à multa. No plano ético-disciplinar, o Conselho Regional de Medicina (CRM) poderá instaurar processo administrativo e impor sanções que vão desde advertências até a cassação do registro profissional, em casos mais graves. Por fim, na esfera civil, o médico pode ser responsabilizado por danos morais e materiais decorrentes da exposição indevida de dados pessoais do paciente.

À vista desse arcabouço normativo e das exceções estritas ao dever de confidencialidade, impõe-se perguntar como tais balizas têm sido observadas na prática assistencial. A experiência recente nos serviços de saúde evidencia fricções precisamente nos atendimentos relacionados a outros temas sensíveis e que envolvem a saúde da mulher, como o abortamento, contexto atravessado por estigma e medo e no qual se verifica a extrapolação de deveres legais e o desvirtuamento da finalidade assistencial em função de interesses punitivistas e moralizantes.

Com efeito, casos recentes no Brasil evidenciam violações do sigilo médico por profissionais de saúde que denunciaram pacientes após suspeitarem de abortos. Em março de 2023, o Superior Tribunal de Justiça (STJ) trancou uma ação penal contra uma mulher acusada de aborto, após constatar que o médico que a atendeu quebrou o sigilo profissional ao acionar a polícia e fornecer o prontuário da paciente como prova. O ministro Sebastião Reis Júnior destacou que o médico, como confidente necessário, está proibido de revelar segredos obtidos em razão da profissão. Além de ter acionado a polícia por suspeitar da prática do delito, o médico foi arrolado como testemunha no processo – situações que, para o colegiado, violaram o art. 207 do Código de Processo Penal, e geraram a nulidade das provas reunidas naqueles autos (STJ, 2023).

Outro caso que merece destaque ocorreu em Minas Gerais, em 2020, quando uma jovem procurou atendimento médico devido a complicações decorrentes de um aborto inseguro. O médico que a atendeu acionou a Polícia Militar, resultando na prisão da paciente, que permaneceu algemada no hospital por três dias (Sousa; Suarez, 2023).

Não se trata de fatos isolados. Pesquisas recentes mostram que a quebra do sigilo médico, nesses contextos, ocorre com uma frequência preocupante. A Universidade Federal do Paraná analisou processos entre 2017 e 2019 e revelou que, em 44% dos casos, as mulheres foram denunciadas por profissionais de saúde; em 65%,

os prontuários foram compartilhados com a polícia sem consentimento; e em 58%, os profissionais atuaram como testemunhas de acusação (Sousa; Suarez, 2023). Esse cenário brasileiro dialoga com pesquisas internacionais que apontam a confiança histórica depositada nos médicos como fator essencial para a manutenção do vínculo terapêutico. Murdoch (2021, p. 3) observa que "uma pesquisa de 2018 com quatro mil adultos norte-americanos revelou que apenas 11% estavam dispostos a compartilhar dados de saúde com empresas de tecnologia, contra 72% que confiavam essa informação aos médicos".

Não obstante a existência de exceções legais à regra do sigilo médico, a interpretação e a aplicação delas exigem criteriosa ponderação, sob pena de se converterem em mecanismos de perseguição disfarçados de zelo técnico. A banalização da quebra de confidencialidade, particularmente em contextos marcados por estigmas sociais e morais – como o aborto e a violência doméstica –, denota uma preocupante inversão de prioridades, em que o aparato médico-jurídico deixa de proteger o sujeito vulnerável para atuar como instrumento de controle punitivo. Assim, é imperativo reafirmar que o sigilo médico não se resume a um dever formal, mas constitui um pilar civilizatório da prática clínica, cuja ruptura compromete a integridade do vínculo terapêutico e a própria noção de cuidado como expressão de respeito à dignidade humana.

4. Opacidade algorítmica

4.1. Conceito e níveis de opacidade

A opacidade, no âmbito da tecnologia e da proteção de dados, diz respeito à ausência de transparência quanto à forma como os dados pessoais são coletados, processados, armazenados e utilizados. Os sistemas baseados em inteligência artificial apresentam barreiras de acesso – muitas vezes intransponíveis – que impedem os indivíduos de compreender e controlar o uso de suas informações, bem como de entender os critérios que levam a máquina a produzir determinado resultado (*output*) (Sousa, 2020). Isso torna inviável a determinação ou explicação do processo que conduz ao resultado algorítmico.

Moraes (2023), ao refletir sobre o âmbito da Justiça Criminal, alerta que a introdução de sistemas de IA opacos – ou seja, cujos critérios de funcionamento, seleção de dados, ponderação de variáveis e geração de resultados não são conhecidos ou auditáveis – compromete pilares fundamentais do Estado de Direito, como: a) a transparência do procedimento penal: investigações e julgamentos devem ser compreensíveis e verificáveis por todos os envolvidos, inclusive o acusado. Um sistema opaco impede que se compreenda por que determinada pessoa foi identificada como suspeita ou por que foi atribuída maior periculosidade a um indivíduo do

que a outro; b) o contraditório e a ampla defesa: se um sistema baseado em IA aponta um "alerta de risco" ou uma "previsão de reincidência", e os critérios usados para essa avaliação não são acessíveis ou compreensíveis, a defesa não tem meios para contestar a conclusão da máquina, o que viola o devido processo legal; e c) a *accountability* democrática: decisões com consequências penais devem estar sujeitas a controle e responsabilização pública. Sistemas opacos, muitas vezes operados por empresas privadas, escapam ao escrutínio das partes, da sociedade e até do próprio sistema judiciário (Moraes, 2022).

A opacidade algorítmica institucionaliza a assimetria de poder entre quem desenvolve e opera os sistemas de IA e aqueles sobre quem recaem seus efeitos, o que cria um cenário incompatível com a racionalidade democrática do processo penal, que exige publicidade, fundamentação e possibilidade de contestação das decisões.

Nessa trilha, tem-se discutido a existência de três formas distintas de opacidade: a) opacidade corporativa, relacionada à proteção do segredo industrial pelas empresas responsáveis pelo desenvolvimento dos algoritmos; b) opacidade cognitiva ou epistêmica, que se refere às desigualdades no acesso, compreensão e controle sobre os dados entre diferentes grupos sociais – o que configura uma forma de desigualdade epistêmica. Decisões baseadas em dados, nesse caso, podem impactar diretamente políticas públicas, ofertas de serviços e até o funcionamento do processo penal; e c) opacidade técnica, associada à ausência de clareza sobre o funcionamento de certos modelos complexos de inteligência artificial, especialmente no modo como os dados de entrada (*inputs*) são transformados em resultados (*outputs*). Embora os *inputs* e *outputs* sejam observáveis, o processo intermediário que realiza essa conversão permanece inacessível à verificação (Sousa, 2020; Burrell, 2016).

Outro modo de classificar a opacidade é distingui-la em três tipos principais: técnica, intencional e interpretativa. A opacidade técnica decorre da estrutura matemática e estatística dos algoritmos, que envolvem milhares ou milhões de parâmetros ajustáveis, dificultando a compreensão do modo pelo qual o sistema chega à determinada decisão (Kroll et al., 2017). A opacidade intencional, por sua vez, é produto de barreiras jurídicas e comerciais, como o segredo industrial e a proteção da propriedade intelectual, que impedem o acesso ao código-fonte ou à lógica interna dos modelos. Por fim, a opacidade interpretativa diz respeito às dificuldades de traduzir em linguagem acessível os resultados gerados, mesmo quando o funcionamento técnico é conhecido (Lepri et al., 2018).

A opacidade algorítmica também serve como blindagem para a reprodução de vieses discriminatórios históricos. Buolamwini e Gebru (2018) revelaram que sistemas de reconhecimento facial desenvolvidos por grandes corporações tecnológicas apresentavam taxas de erro significativamente mais elevadas para mulheres

negras do que para homens brancos, o que evidencia a desigualdade epistêmica na coleta e no treinamento de dados. De modo semelhante, a análise de sistemas de pontuação de risco utilizados no sistema penal norte-americano (como o COMPAS) mostrou que tais algoritmos tendiam a superestimar o risco de reincidência de pessoas negras em comparação com pessoas brancas, ainda que com base em histórico criminal semelhante (Angwin et al., 2016).

De igual modo, no campo da saúde, a literatura indica que algoritmos aplicados à medicina preditiva podem incorporar suposições discriminatórias sobre raça, gênero ou classe social, reforçando padrões de exclusão sob a aparência de neutralidade técnica (Obermeyer et al., 2019). Em realidades atravessadas por desigualdades estruturais, a ausência de transparência nos sistemas de inteligência artificial tende a aprofundar assimetrias de poder e dificultar a identificação dos critérios que orientam decisões, encobrindo erros recorrentes e dispersando a responsabilidade por suas consequências.

Diante desse quadro, garantir que os algoritmos sejam compreensíveis, auditáveis e submetidos a mecanismos efetivos de controle configura uma demanda técnica e uma exigência democrática que se impõe com urgência.

4.2. Explicabilidade

Intimamente ligada à noção de opacidade está a explicabilidade (ou *explainability*), que diz respeito à capacidade de um modelo de fornecer razões inteligíveis sobre seu funcionamento, isto é, de tornar compreensível o caminho percorrido entre os dados de entrada e de saída. Não se trata de um artifício epistêmico, mas de uma condição elementar para a verificação de erros, a contestação de decisões e a reconstrução da cadeia de sentido que conduz a uma determinada classificação, pontuação de risco ou recomendação.

Embora frequentemente confundida com a ideia de interpretabilidade, a explicabilidade implica um movimento ativo do sistema: é ele que deve produzir ou permitir que se extraia uma explicação compreensível para humanos. O desafio está em compatibilizar esse imperativo de inteligibilidade com a complexidade crescente dos modelos de aprendizado profundo, que operam com milhões de parâmetros e múltiplas camadas de transformação não linear. Nesse contexto, surge o campo da *Explainable Artificial Intelligence (XAI)*, voltado à construção de métodos que favoreçam a transparência algorítmica, sem prejuízo do desempenho preditivo (Arrieta et al., 2020).

De acordo com a taxonomia proposta por Arrieta et al. (2020), há dois grandes eixos metodológicos no campo da XAI: a explicabilidade intrínseca e a explicabilidade *post hoc*. No primeiro caso, o próprio modelo é concebido de forma

transparente, como ocorre em regressões lineares, árvores de decisão ou modelos aditivos generalizados. No segundo, objetiva-se explicar sistemas que, por natureza, não são interpretáveis – a exemplo de redes neurais profundas ou máquinas de vetor de suporte –, por meio de técnicas que criam representações simplificadas de suas decisões (Arrieta et al., 2020; Ribeiro et al., 2016).

A literatura aponta, ainda, que a explicabilidade é uma exigência que varia conforme o público-alvo e os objetivos envolvidos: operadores técnicos demandam granularidade e precisão; usuários finais, clareza e linguagem acessível; e agências reguladoras, auditabilidade e reprodutibilidade (Doshi-Velez; Kim, 2017). Ignorar essa pluralidade conduz a modelos que, ainda que tecnicamente avançados, tornam-se ilegítimos do ponto de vista democrático, pois escapam à compreensão dos que por eles são afetados. Essa assimetria entre quem projeta e quem é impactado reproduz, no plano informacional, as desigualdades já presentes no plano social.

Não se defende, aqui, uma posição "tecnofóbica" ou contrária ao avanço científico. O desenvolvimento da inteligência artificial, se submetido a balizas éticas e normativas claras, pode contribuir para o aprimoramento de políticas públicas, em áreas como saúde e segurança, e da própria racionalidade administrativa. O problema reside no fato de que, sob o discurso da inovação, naturaliza-se a concentração de poder informacional nas mãos de poucas corporações privadas transnacionais – as chamadas *big techs* –, que operam sob lógicas opacas e com baixa sujeição a controles públicos e democráticos.

A arquitetura dessas plataformas frequentemente impede o conhecimento efetivo sobre o destino dos dados coletados e processados, ainda que formalmente haja manifestação de consentimento por parte do usuário. Trata-se, muitas vezes, de consentimentos viciados, obtidos em contextos de assimetria informacional e desprovidos de real possibilidade de controle posterior.

O desvio de finalidade – pelo qual dados autorizados para uso em uma determinada política são silenciosamente reutilizados em outras – revela o caráter insidioso de muitos sistemas de IA, que escapam à rastreabilidade. A sociedade, então, transforma-se em um campo experimental permanente para a coleta de dados comportamentais, em pesquisas empíricas cujas hipóteses e objetivos não são declarados, e cujos efeitos não estão sujeitos a escrutínio público.

5. Relativização de direitos fundamentais para fins de segurança pública

Refletir sobre a violência exige reconhecê-la como um fenômeno social multifacetado, resultante da articulação de fatores históricos, econômicos, políticos e culturais. A sociologia brasileira insiste na impossibilidade de reduzir a violência à responsabilidade individual dos sujeitos, o que evidencia que sua persistência

decorre de desigualdades estruturais e da reprodução sistemática da exclusão. Em relação à violência doméstica, em particular, verifica-se uma manifestação extrema de desigualdade de gênero, sustentada por estruturas históricas de dominação masculina e por um sistema social que naturaliza a subordinação feminina.

Federici (2017), em reforço, assinala que a violência doméstica opera como instrumento de disciplinamento dos corpos e das subjetividades, que reforça papéis sociais tradicionais e limita a autonomia feminina. Nesse sentido, tal violência não é apenas um fenômeno interpessoal, mas um mecanismo político de controle social que se reproduz no espaço privado, contribuindo para a manutenção de hierarquias e desigualdades estruturais.

Essa constatação permite compreender como a retórica da proteção à mulher pode ser mobilizada para legitimar políticas públicas que relativizam direitos fundamentais sob o argumento da segurança. Foucault (2005), ao analisar a racionalidade de governo nas sociedades contemporâneas, descreve como os dispositivos de segurança operam segundo a lógica da gestão de riscos, da normalização dos desvios e da intervenção permanente sobre a vida. No paradigma neoliberal, essa governamentalidade transforma experiências sociais em indicadores mensuráveis que orientam decisões estatais e de mercado. Embora se apresente como voltada à população em geral, sua aplicação incide com maior intensidade sobre segmentos previamente identificados como "necessitados de controle" ou "em situação de risco".

A conversão de experiências de violência de gênero em métricas estatísticas e perfis de risco exemplifica essa racionalidade, na medida em que subordina a proteção de direitos à gestão algorítmica de grupos vulnerabilizados.

Esse deslocamento dialoga com a crítica de Agamben (2004), para quem o estado de exceção se apresenta como forma legal daquilo que não possui forma legal, instaurando um vazio normativo que permite a suspensão de garantias sob aparência de juridicidade. Ao se tornar mecanismo permanente de governo, a exceção deixa de ser evento extraordinário e passa a operar de forma difusa, inclusive em regimes democráticos. A incorporação de sistemas de inteligência artificial à segurança pública pode materializar uma nova configuração dessa exceção: uma suspensão velada de direitos, justificada pela prevenção de danos futuros.

Nessa mesma direção, Bigo (2002) denuncia o fenômeno da "securitização", por meio do qual problemas sociais, como migração, pobreza ou saúde pública, são reconvertidos em ameaças à ordem e justificam o endurecimento de políticas repressivas. Essa lógica constrói populações inteiras como potenciais inimigos internos, e desloca o foco da proteção de direitos para a antecipação de condutas indesejadas.

Em acréscimo, a reflexão de Terestchenko (2011) sobre o chamado "bom uso" da tortura oferece um contraponto valioso para compreender como práticas atentatórias a direitos podem ser incorporadas ao repertório de ação de regimes

formalmente democráticos. O autor demonstra que, sob a retórica da necessidade e da proteção coletiva, medidas antes reputadas inaceitáveis passam a ser justificadas como instrumentos legítimos de defesa social, desde que envoltas em mecanismos discursivos que lhes confiram aparência de controle e legalidade. Essa lógica serve para legitimar a violência física extrema e encontra paralelos na gestão contemporânea da segurança pública por meio de tecnologias algorítmicas: a coleta e o uso de dados sensíveis sem consentimento são apresentados como preço a pagar pela prevenção de crimes graves, como se a excepcionalidade da medida se justificasse por si mesma.

Por derradeiro, Bauman (2013) descreve esse processo como a instauração de uma "vigilância líquida", caracterizada por sua difusão contínua e por sua capacidade de penetrar nas mais variadas esferas da vida cotidiana. Nesse novo arranjo, "indivíduos são constantemente rastreados, categorizados e avaliados, muitas vezes sem perceberem", o que contribui para a diluição da privacidade e legitima formas de intervenção cada vez mais invasivas.

Exemplos concretos dessa tensão emergem de iniciativas como o estudo desenvolvido pela *Vital Strategies* e pelo FrameNet Brasil, cerne deste trabalho. A partir de registros médicos de 13 mil mulheres atendidas no Recife-PE, foram identificados supostos padrões comportamentais que antecederiam o agravamento das violências, como mudanças nas rotinas de atendimento e relatos de sofrimento mental. Apesar da aparente intenção de proteger vidas e evitar o feminicídio, o modo como o estudo foi conduzido (com violações à privacidade das pacientes e a outros direitos) permite induzir um preocupante deslocamento do eixo protetivo para uma lógica de vigilância seletiva.

Os registros clínicos – originalmente destinados à promoção do cuidado – foram transformados em insumos para um sistema de predição algorítmica, que converte experiências íntimas e confidenciais em dados operacionais, dissociando-as do contexto humano que lhes confere sentido. Tal procedimento fragiliza o vínculo de confiança entre paciente e médico, mas também inaugura um precedente perigoso de apropriação institucional de informações sensíveis, submetendo-as a finalidades distintas daquelas para as quais foram legitimamente coletadas. Soma-se a isso a inexistência de mecanismos concretos de controle, rastreabilidade ou segurança que impeçam o vazamento dessas informações ou sua exploração para fins estranhos à proteção das vítimas, como uso comercial, profilagem mercadológica ou até mesmo discriminação indireta, o que agrava o cenário de vulnerabilidade e expõe as pacientes a novos riscos, para além da violência que já enfrentam.

De mais a mais, o perfil das mulheres que recorrem ao sistema público de saúde é composto por grupos historicamente mais expostos tanto à violência de gênero quanto à vulnerabilidade social. Quando sistemas de IA são treinados com

informações oriundas dessas bases, o recorte socioeconômico e racial predominante entre as usuárias tende a influenciar diretamente a "leitura de risco" realizada pelo algoritmo. Assim, qualquer viés presente na coleta ou no tratamento dessas informações pode gerar previsões que reforçam estigmas: por exemplo, associando bairros periféricos ou determinados perfis sociodemográficos a maior probabilidade de violência, mesmo que tal associação resulte de padrões históricos de exclusão e não de um risco inerente ao grupo (Lum; Isaac, 2020; Richardson et al., 2019).

A crítica de Valdivia, Hyde-Vaamonde e García Marcos (2023) à ferramenta EPV-R (Escala de Predicción de Violencia grave contra la Pareja – Revisada), utilizada no País Basco, oferece paralelo relevante. Os autores descrevem o caso "M", em que o algoritmo classificou como "baixo risco" uma situação que o juiz, examinando os mesmos elementos, entendeu como de risco elevado. A EPV-R se baseia em 20 indicadores psicométricos agrupados em cinco categorias e, a partir de um ponto de corte, propõe três níveis de risco. Contudo, apresenta número significativo de falsos negativos, o que compromete sua confiabilidade e pode privar vítimas de medidas protetivas urgentes.

A opacidade de seu funcionamento agrava o problema: magistrados não têm acesso às variáveis específicas nem à lógica algorítmica empregada, o que enfraquece o contraditório e a fundamentação das decisões. Embora concebida como instrumento de apoio rápido e objetivo, sua adoção, sem critérios claros e sem formação técnica adequada, leva o sistema a funcionar como "quase perito", deslocando a responsabilidade decisória para a máquina e sustentando-se mais na aparência de cientificidade do que em precisão comprovada.

Os autores ainda apontam vieses nos dados que alimentam esses sistemas, muitas vezes herdados de filtros institucionais seletivos. No caso basco, isso se expressa, por exemplo, na associação entre nacionalidade e risco, que reforça estigmas e práticas discriminatórias em ciclos de retroalimentação conhecidos como *feedback loops*. No Brasil, permanece sem esclarecimento público o critério para selecionar os 13 mil casos do projeto *Vital Strategies*/FrameNet Brasil, o que impede avaliar a representatividade dos resultados.

Por fim, a ausência de menção a qualquer consentimento prévio para o uso dos dados das vítimas, tanto no estudo espanhol quanto no brasileiro, revela um modelo de atuação que instrumentaliza corpos e experiências em nome da previsibilidade estatística, deslocando o foco de políticas públicas da escuta e do acolhimento para a gestão algorítmica da periculosidade.

6. Considerações finais

As discussões aqui empreendidas revelam as múltiplas camadas de complexidade envolvidas na adoção de tecnologias algorítmicas para subsidiar estudos e,

eventualmente, políticas públicas voltadas à prevenção de feminicídios. O ponto de partida foi a pesquisa conduzida pela organização *Vital Strategies* em parceria com o FrameNet Brasil, que, ao analisar os prontuários de saúde de 13 mil mulheres sem consentimento delas, concluiu pela existência de padrões estatísticos supostamente capazes de antecipar a escalada da violência doméstica. A apresentação dos resultados como um avanço no campo da prevenção, com promessas de detecção precoce e intervenções mais eficazes, embora receba adesão entusiasta em determinados setores, exige exame mais cauteloso à luz dos marcos normativos que regem a proteção de dados e os direitos das vítimas.

O artigo demonstrou que o uso de dados sensíveis para finalidades preditivas, sobretudo em contextos de vulnerabilidade extrema, não se limita a uma questão técnica. Trata-se de um campo de disputa sobre a forma como o poder se estrutura, se distribui e se exerce sobre os corpos. A tecnificação de decisões que afetam diretamente direitos fundamentais como privacidade, autonomia, acesso a serviços e não discriminação não pode ocorrer dissociada de mecanismos efetivos de controle social, transparência e responsabilização.

Nesse contexto, o deslocamento das políticas de proteção da mulher para formas de gestão estatística baseadas em dados biomédicos e comportamentais retoma a racionalidade de governo teorizada por Foucault, com o acréscimo da modelagem algorítmica da conduta, o que redefine as fronteiras entre prevenção e controle, público e privado. Tal arranjo desloca a intervenção estatal do campo da escuta e do cuidado para o da predição e do monitoramento contínuo, transformando experiências de violência em insumos para sistemas opacos, cuja atuação tende a reforçar hierarquias preexistentes e a reduzir a autonomia dos sujeitos à sua mensuração em métricas de risco.

O caso espanhol da EPV-R, cotejado ao estudo nacional, evidencia os riscos de se adotar classificadores de risco como critério orientador de decisões judiciais ou institucionais. A opacidade das ferramentas, a falta de transparência quanto aos dados utilizados, a ausência de mecanismos de contestabilidade e a inexistência de consentimento informado demonstram que a promessa de eficiência muitas vezes encobre a reprodução de estigmas e a precarização das garantias processuais e materiais das vítimas.

A confiança desmedida em soluções tecnológicas pode, ademais, desviar a atenção das reais causas da violência de gênero, que se enraízam em desigualdades históricas, relações assimétricas de poder, omissão institucional e cultura patriarcal. Substituir políticas de direitos por tecnologias de gestão de risco representa um retrocesso, ao deslocar o foco da responsabilização estatal para o controle biomédico das vítimas.

O objetivo não é interditar o debate sobre inovação, mas afirmar que sua adoção em áreas sensíveis deve se submeter a escrutínio rigoroso, com base em limites claros, salvaguardas eficazes e instrumentos democráticos de controle. Tecnologias têm intencionalidades, refletem interesses e produzem efeitos materiais sobre a vida das pessoas. Por isso, não podem ser naturalizadas nem delegadas à racionalidade técnica como se neutras fossem.

Referências bibliográficas

AGAMBEN, Giorgio. *Estado de exceção*. Trad. Iraci D. Poleti. São Paulo: Boitempo, 2004.

AMBROSIO, Gleiner Pedroso Ferreira; BARBOSA, André Luis Jardini. O paradigma da implantação da inteligência artificial na segurança pública brasileira: regulação versus eficiência. *Revista de Estudos Jurídicos da UNESP*, Franca, v. 28, n. 48, p. 73-92, 2024. Disponível em: [https://periodicos.franca.unesp.br/index.php/estudosjuridicosunesp/article/view/4398/3595]. Acesso em: 11.03.2025.

ANGWIN, Julia et al. *Machine Bias*. ProPublica, 2016.

ARRIETA, Alejandro Barredo et al. Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Information Fusion*, v. 58, 2020, p. 82-115. Disponível em: [https://doi.org/10.1016/j.inffus.2019.12.012]. Acesso em: 27.03.2025.

BAUMAN, Zygmunt. *Vigilância líquida:* diálogos com David Lyon. Trad. Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013.

BELIATO, Araceli Martins. Inteligência de Segurança Pública e defesa dos Direitos Humanos: lições do julgamento do Caso CAJAR vs. Colômbia pela Corte Interamericana de Direitos Humanos. In: BELIATO, Araceli Martins et al. (Orgs.). *Inteligência policial*. Leme: Mizuno, 2025b, p. 63-94.

BELIATO, Araceli Martins. Persecução penal e novas tecnologias. In: JORGE, Higor Vinicius Nogueira (Org.). *Direito processual penal para carreiras policiais*. São Paulo: JusPodivm, 2025a, p. 67-90.

BIGO, Didier. Security and Immigration: Toward a Critique of the Governmentality of Unease. *Alternatives,* v. 27, Special Issue, p. 63-92, 2002.

BUARQUE, Gabriela; EHRHARDT JÚNIOR, Marcos. Direito fundamental à proteção de dados pessoais: entre autodeterminação e proporcionalidade. *Revista de Direito, Governança e Novas Tecnologias*, n. 24, p. 73-96, jul.-dez. 2023. Disponível em: [https://revistas.unilasalle.edu.br/index.php/dialogos/article/view/12487]. Acesso em: 30.03.2025.

BUOLAMWINI, J.; GEBRU, T. Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning*

Research, v. 81, p. 77-91, 2018. Disponível em: [https://doi.org/10.1145/3287560.3287590]. Acesso em: 27.03.2025.

BURRELL, Jenna. How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society*, v. 3, n. 1, 2016. Disponível em: [https://doi.org/10.1177/2053951715622512]. Acesso em: 07.03.2025.

CHANG, Yan. Reflexões sobre a proteção penal de dados pessoais sob a Lei de Proteção de Informações Pessoais. *Revista Estudos Institucionais*, v. 9, n. 1, p. 15-33, jan.-abr. 2023. Disponível em: [https://www.estudosinstitucionais.com/REI/article/view/744]. Acesso em: 30.03.2025.

CORTE INTERAMERICANA DE DIREITOS HUMANOS (Corte IDH). *Caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" vs. Colombia.* Sentencia de 18 de octubre de 2023 (excepciones preliminares, fondo, reparaciones y costas). San José: Corte Interamericana de Direitos Humanos, 2023. Disponível em: [https://www.corteidh.or.cr/docs/casos/articulos/seriec_506_esp.pdf]. Acesso em: 16.03.2025.

COZMAN, Fabio Gagliardi; CORTESE, João Figueiredo Nobre. *Inteligência artificial em pleno verão*. [S.l.], 2019.

COZMAN, Fabio Gagliardi; NERI, Hugo. O que, afinal, é Inteligência Artificial? In: COZMAN, Fabio Gagliardi; PLONSKI, Guilherme Ary; NERI, Hugo (Orgs.). *Inteligência artificial*: avanços e tendências. São Paulo: Instituto de Estudos Avançados da Universidade de São Paulo, 2021.

DOSHI-VELEZ, F.; KIM, B. Towards a rigorous science of interpretable machine learning. *arXiv preprint*, arXiv:1702.08608, Cornell University, 2017. Disponível em: [https://arxiv.org/abs/1702.08608]. Acesso em: 28.03.2025.

ESTEVA, A. et al. A guide to deep learning in healthcare. *Nature Medicine*, v. 25, n. 1, p. 24-29, 2019. [https://doi.org/10.1038/s41591-018-0316-z].

FEDERICI, Silvia. *Calibã e a bruxa*: mulheres, corpo e acumulação primitiva. São Paulo: Elefante, 2017.

FERGUSON, A. G. The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement. Oxford: *Oxford University Press*, 2019. Disponível em: [https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=6306&context=law_lawreview]. Acesso em: 27.03.2025.

FOLHA DE SÃO PAULO. *IA lê prontuários e detecta violência contra mulher 92 dias antes de caso se agravar*. São Paulo, 21 dez. 2024. Disponível em: [https://www1.folha.uol.com.br/equilibrioesaude/2024/12/ia-le-prontuarios-e-detecta-violencia-contra-mulher-92-dias-antes-de-caso-se-agravar.shtml]. Acesso em: 03.03.2025.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. *Modelos de inteligências artificiais e a propensão ao autoritarismo algorítmico*. Renato Sérgio de Lima et al. (Orgs.). São Paulo: FBSP, 2025. (Informe de Análise nº 04). Disponível

em: [https://publicacoes.forumseguranca.org.br/items/661a8833-c041-4d-36-a1d1-d180b996a28c]. Acesso em: 10.03.2025.

FOUCAULT, Michel. *Em defesa da sociedade*: curso no Collège de France (1975-1976). Trad. Maria Ermantina Galvão. São Paulo: Martins Fontes, 2005.

HARARI, Yuval Noah. *21 lições para o século 21*. Trad. Paulo Geiger. 1. ed. São Paulo: Companhia das Letras, 2018.

KNUTH, Donald Ervin. *The art of computer programming*. v. 1. Fundamental algorithms. 3. ed. Boston, MA, 1997. Disponível em: [http://broiler.astrometry.net/~kilian/The_Art_of_Computer_Programming%20-%20Vol%201.pdf]. Acesso em: 20.03.2025.

KROLL, Joshua et al. Accountable algorithms. *University of Pennsylvania Law Review*, v. 165, 2017. Disponível em: [https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=9570&context=penn_law_review]. Acesso em: 12.03.2025.

LEPRI, Bruno et al. *Fair, Transparent, and Accountable Algorithmic Decision-making Processes*. *Philosophy & Technology*, v. 31, n. 4, p. 611-627, dez. 2018. Disponível em: [https://datapopalliance.org/wp-content/uploads/2020/09/Fair-Transparent-and-Accountable-Algorithmic-Decision-making-Processes.pdf]. Acesso em: 11.03.2025.

LUM, K.; ISAAC, W. *To predict and serve*? Significance, v. 17, n. 5, p. 14-19, 2020. [https://doi.org/10.1038/s41599-020-00593-9].

MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. *Pensar*, Fortaleza, v. 25, n. 4, p. 1-18, out.-dez. 2020.

MORAES, Alexandre de. *Direito constitucional*. 41. ed. São Paulo: Atlas, 2025.

MORAES, Maurício Zanoide de. Opacidade da IA como impeditivo de transparência e controle democrático da investigação criminal. *Colóquio Luso-Brasileiro Direito Penal, Tecnologia e IA*. Colégio da Trindade – Faculdade de Direito da Universidade de Coimbra, dias 26 e 27 de outubro de 2023. Youtube. Disponível em: [https://www.youtube.com/watch?v=0hnqgBHPkXw]. Acesso em: 11.03.2025.

MORAES, Maurício Zanoide de. *Processo criminal transformativo*: modelo criminal e sistema processual não violentos. Coord. da coleção Cláudio Brandão. 1. ed. Belo Horizonte, São Paulo: D'Plácido, 2022. (Ciência criminal contemporânea; v. 2).

MOTTA, Júlia. *IA auxilia médicos e detecta violência contra mulher 92 dias antes de caso se agravar.* Fórum, 21 dez. 2024. Disponível em: [https://revistaforum.com.br/saude/2024/12/21/ia-auxilia-medicos-detecta-violncia-contra-mulher-92-dias-antes-de-caso-se-agravar-171407.html]. Acesso em: 03.03.2025.

MURDOCH, Blake. Privacy and artificial intelligence: challenges for protecting health information in a new era. *BMC Medical Ethics,* n. 22, v. 122, 2021. [https://doi.org/10.1186/s12910-021-00687-3].

O TEMPO. *IA lê prontuários e detecta violência contra mulher 92 dias antes de caso se agravar*. Agências, Contagem-MG, 21 dez. 2024. Disponível em: [https://www.otempo.com.br/brasil/2024/12/21/ia-le-prontuarios-e-detecta-violencia-contra-mulher-92-dias-antes-de-caso-se-agravar]. Acesso em: 02.03.2025.

OBERMEYER, Ziad et al. Dissecting racial bias in an algorithm used to manage the health of populations. *Science,* v. 366, Issue 6464, 2019. Disponível em: [https://www.science.org/doi/10.1126/science.aax2342]. Acesso em: 13.03.2025.

OLIVEIRA, Letícia Lé. Inteligência Artificial e desigualdade social: o impacto do colonialismo digital nas políticas públicas. *Internet & Sociedade*, v. 5, n. 1, p. 148-167, jul. 2024.

PHAM, H. et al. DeepCare: A deep dynamic memory model for predictive medicine. In: *Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. New York: ACM, 2017. p. 1485-1494. [https://doi.org/10.1145/2783258.2788613].

RATCLIFFE, J. H. Policing and machine learning. *Policing*: A Journal of Policy and Practice, v. 13, n. 2, p. 215-221, 2019. [https://doi.org/10.1093/police/pay073].

RIBEIRO, Marco Tulio; SINGH, Sameer; GUESTRIN, Carlos. "Why Should I Trust You?": Explaining the Predictions of Any Classifier. In: *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. New York: ACM, 2016. p. 1135-1144. [https://doi.org/10.1145/2939672.2939778].

RICHARDSON, R.; SCHULTZ, J.; CRAWFORD, K. Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice. *New York University Law Review Online*, 2019. Disponível em: [https://ssrn.com/abstract=3370129]. Acesso em: 27.03.2025.

RUSSELL, Stuart; NORVIG, Peter. *Artificial intelligence:* a modern approach. 4. ed. Hoboken: Pearson, 2021.

SARLET, Ingo Wolfgang. O STF e a proteção dos dados pessoais. *Consultor Jurídico*, 3 mar. 2025. Disponível em: [https://www.conjur.com.br/2025-mar-03/o-stf-e-a-protecao-dos-dados-pessoais/]. Acesso em: 15.03.2025.

SARLET, Ingo Wolfgang. Proteção de dados pessoais: para além da privacidade e autodeterminação informacional. *Consultor Jurídico*, 16 jul. 2021. Disponível em: [https://www.conjur.com.br/2021-jul-16/direitos-fundamentais-

protecao-dados-alem-privacidade-autodeterminacao-informacional/?utm_source=chatgpt.com]. Acesso em: 15.03.2025.

SETZER, Valdemar W. Dado, informação, conhecimento e competência. *Departamento de Ciência da Computação*, Universidade de São Paulo. 25 maio 2015. Disponível em: [www.ime.usp.br/~vwsetzer]. Acesso em: 15.03.2025.

SOLOVE, Daniel J. The myth of the privacy paradox. *George Washington Law Review*, v. 89, n. 1, p. 1-51, 2020. [https://doi.org/10.2139/ssrn.3567521].

SOUSA, Natália; SUAREZ, Joana. Médicos quebram sigilo e denunciam mulheres por aborto. Profissionais de saúde se aproveitam da vulnerabilidade de pacientes e devem ser responsabilizados por isso. Terra/AzMina, 16 ago. 2023. Disponível em: [https://www.terra.com.br/nos/medicos-quebram-sigilo-e-denunciam-mulheres-por-aborto,362101de09f122ec9b370acf03b7baees9uikkt6.html]. Acesso em: 30.03.2025.

SOUSA, Susana Aires de. "Não fui eu, foi a máquina": teoria do crime, responsabilidade e inteligência artificial. In: RODRIGUES, Anabela Miranda (Coord.). *A inteligência artificial no direito penal*. Coimbra, Portugal: Almedina, 2020.

SUPERIOR TRIBUNAL DE JUSTIÇA. *Sexta Turma tranca ação penal por aborto ao ver quebra de sigilo profissional entre médico e paciente.* Brasília, DF, 14 mar. 2023. Disponível em: [https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2023/14032023-Sexta-Turma-tranca-acao-penal-por-aborto-ao-ver-quebra-de-sigilo-profissional-entre-medico-e-paciente.aspx]. Acesso em: 30.03.2025.

TELLES, Primonata Silva Brilhante. Inteligência artificial e polícia preditiva: limites e possibilidades. *Boletim Científico ESMPU*, Brasília, v. 20, n. 57, p. 247-268, jul.-dez. 2021. Disponível em: [https://escola.mpu.mp.br/publicacoescientificas/index.php/boletim/article/download/613/516/1896]. Acesso em: 11.03.2025.

TERESTCHENKO, Michel. *O bom uso da tortura*: ou como as democracias justificam o injustificável. Trad. Eduardo Brandão. São Paulo: WMF Martins Fontes, 2011.

TOPOL, E. J. High-performance medicine: the convergence of human and artificial intelligence. *Nature Medicine*, v. 25, n. 1, p. 44-56, 2019. [https://doi.org/10.1038/s41591-018-0300-7].

VAISHYA, R. et al. Artificial Intelligence (AI) applications for COVID-19 pandemic. *Diabetes & Metabolic Syndrome*: Clinical Research & Reviews, v. 14, n. 4, p. 337-339, 2020. [https://doi.org/10.1016/j.dsx.2020.04.012].

VALDIVIA, Ana; HYDE-VAAMONDE, Cari; GARCÍA MARCOS, Julián. Judging the algorithm: a case study on the risk assessment tool for gender-based violence implemented in the Basque Country. *Patterns*, v. 4, n. 6, 100838, 2023. [https://doi.org/10.1016/j.patter.2023.100838].

VIANEZ, Paula. *IA auxilia médicos a identificarem violência contra mulher 92 dias antes*. A Repórter, 23 jan. 2025. Disponível em: [https://areporter.com.br/ia-auxilia-medicos-a-identificarem-violencia-contra-mulher-92-dias-antes/]. Acesso em: 03.03.2025.

ZAVRŠNIK, A. Big Data, Crime and Social Control. *ERA Forum,* v. 20, p. 567-583, 2020. Disponível em: [https://link.springer.com/article/10.1007/s12027-020-00602-0]. Acesso em: 20.03.2025.

ZUBOFF, Shoshana. *A era do capitalismo de vigilância*: a luta por um futuro humano na nova fronteira do poder. Trad. George Schlesinger. Rio de Janeiro: Intrínseca, 2021.

Legislação

BRASIL. Conselho Nacional de Justiça. *Resolução nº 332 de 21.08.2020*. Dispõe sobre a ética, a transparência e a governança na produção e no uso de Inteligência Artificial no Poder Judiciário e dá outras providências. Brasília, DF, 2020. DJe/CNJ, nº 274, de 25.08.2020, p. 4-8. Disponível em: [https://atos.cnj.jus.br/atos/detalhar/3429]. Acesso em: 18.03.2025.

BRASIL. Conselho Nacional de Justiça. *Resolução nº 615, de 11 de março de 2025.* Estabelece diretrizes para o desenvolvimento, utilização e governança de soluções desenvolvidas com recursos de inteligência artificial no Poder Judiciário. Brasília, DF, 2025. Disponível em: [https://atos.cnj.jus.br/files/original1555302025031467d4517244566.pdf]. Acesso em: 05.08.2025.

BRASIL. *Decreto nº 11.491, de 12 de abril de 2023*. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001. Brasília, DF, 2023. Disponível em: [https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11491.htm]. Acesso em: 17.03.2025.

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 para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF, 2022. Disponível em: [https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm]. Acesso em: 06.08.2025.

BRASIL. *Lei nº 10.778, de 24 de novembro de 2003*. Estabelece a notificação compulsória, no território nacional, do caso de violência contra a mulher que for atendida em serviços de saúde públicos ou privados. Brasília, DF, 2003. Disponível em: [https://www.planalto.gov.br/ccivil_03/Leis/2003/L10.778.htm]. Acesso em: 06.03.2025.

BRASIL. *Lei nº 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet). Brasília, DF, 2014. Disponível em: [https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm]. Acesso em: 16.03.2025.

BRASIL. *Lei nº 13.709, de agosto de 2018*. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF, 2018. Disponível em: [http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm]. Acesso em: 16.03.2025.

BRASIL. *Lei nº 13.931, de 10 de dezembro de 2019*. Altera a Lei nº 10.778, de 24 de novembro de 2003, para dispor sobre a notificação compulsória dos casos de suspeita de violência contra a mulher. Brasília, DF, 2019. Disponível em: [https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13931.htm]. Acesso em: 06.03.2025.

BRASIL. *Lei nº 6.259, de 30 de outubro de 1975*. Dispõe sobre a organização das ações de Vigilância Epidemiológica, sobre o Programa Nacional de Imunizações, estabelece normas relativas à notificação compulsória de doenças, e dá outras providências. Brasília, DF, 1975. Disponível em: [https://www.planalto.gov.br/ccivil_03/leis/l6259.htm]. Acesso em: 16.03.2025.

CONSELHO FEDERAL DE MEDICINA. *Código de Ética Médica*: Resolução CFM nº 2.217, de 27 de setembro de 2018, modificada pelas Resoluções CFM nº 2.222/2018 e 2.226/2019. Brasília: Conselho Federal de Medicina, 2019.

UNIÃO EUROPEIA. *Regulamento (UE) 2016/679, de 27 de abril de 2016.* Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral de Proteção de Dados). Jornal Oficial da União Europeia, L 119, 4 maio 2016. Disponível em: [https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX%3A32016R0679]. Acesso em: 11.03.2025.

UNIÃO EUROPEIA. Regulamento (UE) 2024/1689, de 12 de julho de 2024. Estabelece regras harmonizadas sobre a inteligência artificial (AI Act) e altera determinados atos legislativos da União. *Jornal Oficial da União Europeia*, L 2.024/1689, 12 jul. 2024. Disponível em: [https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai]. Acesso em: 11.03.2025.

UNITED NATIONS (UN). High Commissioner for Human Rights. *The right to privacy in the digital age*. Geneva: UN, 4 Aug. 2022. Disponível em: [https://digitallibrary.un.org/record/3985679?ln=en&v=pdf]. Acesso em: 06.08.2025.

Recebido em: 31.03.2025.
Aprovado em: 28.07.2025.
Última versão da autora: 09.08.2025.



PESQUISA DO EDITORIAL



Área do Direito: Penal; Digital; Constitucional

Veja também Doutrina relacionada ao tema

- A política do policiamento preditivo: pressupostos criminológicos, técnicas algorítmicas e estratégias punitivas, de Daniel Edler Duarte e Luisa Cruz Lobato – *RBCCrim* 183/57-98;
- Inteligência artificial aplicada aos bancos de dados do CNJ no enfrentamento à violência contra a mulher: caminhos para prevenção, monitoramento e política pública, de Christiany Pegorari Conte e Thiago Rodovalho – *RIAD* 1/87-103; e
- Predição dos crimes de violência de gênero com algoritmos de aprendizagem de máquina, de Samuel M. Brasil Jr. e Flávio M. Varejão – *RT* 1058/143-163.

A coleta de dados em larga escala e as possibilidades críticas de direito comparado: sistema de dupla proteção

Bulk data collection and critical possibilities in compared law: double lock system

Samuel Andreatta[1]
Pontifícia Universidade Católica do Rio Grande do Sul, PUCRS, Brasil.
samuelandreatta@hotmail.com

DOI: [doi.org/10.5281/zenodo.17058401].

Área do Direito: Penal; Digital

Resumo: Esta pesquisa teórica tem o objetivo de demonstrar as nuances da coleta de dados em larga escala por meio da delimitação dos mecanismos de coleta de dados no ordenamento jurídico brasileiro, pela explicação da diferenciação entre coleta de dados individuais e em larga escala e pelas possibilidades normativas contidas na legislação inglesa. Concluiu-se que o Brasil, apesar de não possuir legislação específica para a coleta de dados em larga escala, realiza tal atividade, tampouco diferencia entre as garantias de coleta individual e coleta em massa. Ademais, foi possível perceber que o mecanismo de dupla

Abstract: This theoretical research has the aim of demonstrating the nuances of bulk data collection by delineating data collection mechanisms within the Brazilian legal framework, explaining the distinction between individual and large-scale data collection, and analyzing the normative possibilities contained in British legislation. It was concluded that Brazil, despite lacking specific legislation for large-scale data collection, carries out such activity, it also does not distinguish between guarantees for individual collection and mass collection. Furthermore, it was possible to observe that the dual protection

1. Doutorando e Mestre em Ciências Criminais pela Pontifícia Universidade Católica do Rio Grande do Sul (PUC/RS). Advogado.
Currículo Lattes: [http://lattes.cnpq.br/3023689561632480].
ORCID: [https://orcid.org/0000-0003-2862-1776].
E-mail: samuelandreatta@hotmail.com
O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001.

proteção contido na legislação inglesa pode servir como base de maneira a garantir um duplo juízo de admissibilidade da medida centrado na necessidade e na proporcionalidade. Por fim, denota-se o fato de que há uma admissão tácita de um novo espaço de jurisdição exercido por grandes empresas do setor tecnológico.

Palavras-chave: Tecnologia – Coleta de dados em larga escala – Criminologia crítica.

mechanism present in British legislation can serve as a basis to ensure a dual admissibility assessment of the measure, centered on necessity and proportionality. Finally, it is noted that there is a tacit acknowledgment of a new jurisdictional space exercised by big tech companies.

Keywords: Technology – Bulk data collection – Critical criminology.

Sumário: 1. Introdução. 2. Perspectivas iniciais e questões individuais: legislação pertinente. 3. O fornecimento de dados em larga escala. 4. Possibilidades de legislação comparada: o sistema de "proteção dupla". 5. Considerações finais. Referências. Legislação. Jurisprudência.

1. Introdução

A nova razão de mundo neoliberal, reforçada pelos processos de globalização, criou territórios jurídico-políticos, assentando e dissipando espaços de produção de verdade. A resignação, própria de um mundo unipolar, serviu para limitar as condições de emergência do discurso jurídico, fragilizando o modelo soberano que ainda impera na diferenciação política essencial – aquela que separa amigos e inimigos – como indica Schmitt (1992, p. 51). Essa nova forma "tecnopolítica" (Sabariego; Amaral; Salles, 2020) do capitalismo não reside apenas no espaço muito concreto da nuvem ou abaixo da superfície em cabos de fibra ótica transatlânticos, mas no tempo e nos fluxos de coleta de dados.

A ubiquidade das comunicações que uniformiza o tempo global, o que Virilio (1997, p. 85) nomeia de tirania da velocidade, gera novos mecanismos de requisição e fornecimento de dados. Acima de tudo, alimenta a ambição de acessibilidade total à informação ao demonstrar as possibilidades da dimensão de uma coleta de dados que faria Bentham tremer. Trata-se de uma matriz de pensamento que serve para nublar os limites entre a jurisdição estatal e a ingerência de plataformas na web. Essa jurisdição, admitida tacitamente, começa a tomar forma por meio de tentativas cada vez mais constantes de conexão direta entre empresas de tecnologia e agências punitivas.

A expansão da capacidade computacional alimenta o desejo de informação total, que é um dos objetivos explícitos da contrainsurgência (Harcourt, 2021), técnica de governo internalizada; é esse o ponto que foi denunciado por Snowden (2019) quando se refere à atividade da NSA. A reinvenção de parâmetros de legalidade,

instituída pela seção 215 do *USA Patriot Act*, que, à sua vez, permitiu a coleta e a interceptação de dados sem mandado judicial de empresas de telecomunicação, como indica Harcourt (2021, p. 159), serviu não só para expandir e legitimar a vigilância, mas também como denúncia da fragilidade do regime de proteção dos direitos humanos: a privacidade é o cordeiro sacrificial da virada neoliberal.

O objetivo deste trabalho é destrinchar as especificidades da requisição de dados em larga escala. O direcionamento desse esforço está situado no grande campo da teoria Crítica (Harcourt, 2020). Aqui, diante do processo de fragmentação das criminologias (Sozzo, 2006), adota-se o termo Criminologia crítica (Baratta, 2004) no sentido de uma crítica ao direito processual penal centrada na análise de legislação e jurisprudência de maneira a demonstrar (ou não) a existência de regime específico de coleta de dados em massa. O esforço leva em conta a interdisciplinaridade intrínseca da disciplina criminológica que abdica de qualquer "encerramento metodológico" (Amaral, 2020, p. 165).

A ideia de encerramento metodológico está também ancorada na suposta limitação da Criminologia Crítica no que diz respeito ao seu objeto. Essa posição está baseada em uma cisão, de cunho marxiano, que separa de maneira absoluta a teoria e prática. Ocorre que a visão pós-estruturalista possui uma visão ampla sobre a concepção de discurso, notadamente os vetores normativos também são espaços de produção de subjetividade. O espaço de atuação metodológico altera as pretensões da crítica, no sentido de que a pesquisa não ambiciona se deter na avaliação de tipo prescritivo. De fato, pretende-se exibir um panorama geral das fontes jurídicas diretas que atravessam o tema em caráter enumerativo, mas para responder a um problema geral de pesquisa e um problema específico.

O problema geral pode ser reduzido à seguinte pergunta: há regime específico de coleta de dados em larga escala no ordenamento jurídico brasileiro? Para adiantar a resposta, entende-se que não há regramento próprio, tampouco diferenciação especificada quanto à necessidade de tomar medidas próprias à dimensão das informações coletadas, que é intrínseca ao caráter intrusivo da medida, dada a inevitabilidade de atingir sujeitos que nada têm a ver com a investigação. Já o problema específico se debruça sobre as possibilidades que já estão sendo utilizados: A legislação comparada pode servir como inspiração diante da evidenciação dos mecanismos de admissibilidade dos pedidos de quebra de sigilo telemático em larga escala?

Dado esse cenário, diante da inexistência de mecanismos vigentes específicos à coleta em larga escala no âmbito do poder punitivo estatal, poderia a legislação inglesa, que possui regime jurídico próprio de requisição de dados em larga escala, servir tanto como norte principiológico quanto como exemplo procedimental? A resposta, descobrimos, não é maniqueísta. Concluiu-se que a legislação inglesa

poderia servir de inspiração para um regime jurídico centrado em uma dupla camada de verificação de admissibilidade da medida, onde os pressupostos de proporcionalidade e necessidade possam ser averiguados por duas instâncias. No entanto, a lei inglesa conta com os mesmos problemas de vagueza de motivações que podem ensejar uma expansão acelerada de mecanismos punitivos legitimados por uma regulamentação norteada pelo imperativo de defesa social.

Feitas as considerações iniciais, cabe observar que o presente trabalho não se estrutura pela oposição à violação de direitos fundamentais ou garantias processuais às medidas na requisição de dados em larga escala, o que poderia se chamar de "crítica imanente" (Harcourt, 2020), apesar de tal esforço ser imensuravelmente essencial. A pesquisa se concentra em três eixos de crítica geral: a delimitação dos mecanismos de coleta de dados, a explicação da diferenciação entre coleta de dados individuais e em larga escala e nas possibilidades normativas contidas na legislação inglesa.

2. Perspectivas iniciais e questões individuais: legislação pertinente

Os pedidos de requisição de dados telemáticos em larga escala no Brasil, para fins penais, carecem de legislação específica apropriada. Essa afirmação é reflexo da utilização dos mesmos mecanismos de quebra de sigilo diante de situações díspares; porém, antes de pormenorizar tal diferenciação, é necessário definir o termo "coleta de dados em larga escala". A intenção desta pesquisa não é realizar uma crítica fundamentada nas violações aos direitos fundamentais e aos ditames do direito e processo penal que seriam aplicáveis à coleta de dados em larga escala, mas identificar o fenômeno e apontar, a partir da teoria crítica, em uma visão de direito comparado, possibilidades de regulamentação inédita.

A sistematização do termo "coleta de dados em larga escala" comporta dois níveis: o primeiro, uma diferenciação entre os tipos de dados telemáticos; o segundo, uma diferenciação entre o fornecimento de dados de um indivíduo e o fornecimento de dados em larga escala de maneira a determinar uma conexão a um indivíduo (ou organização criminosa).

O termo genérico "dados", segundo o Marco Civil da Internet (Lei 12.965, de 23 de abril de 2014), pode ser destrinchado em três tipos distintos: registros de conexão, registro de acesso a aplicações na internet e comunicações privadas. Enquanto os dois primeiros podem ser encarados como dados cadastrais e de geolocalização, fornecidos pelo próprio usuário à plataforma, as comunicações privadas tratam dos dados que configuram as comunicações entre usuários ou atividades específicas da plataforma. As comunicações privadas demandam um regime mais

criterioso para seu fornecimento, pois as informações que as constituem são de caráter sensível (Brasil, 2014).

A Lei Geral de Proteção de Dados Pessoais – LGPD (Lei 13.709/2018) postula ainda outra diferenciação: dados pessoais e dados pessoais sensíveis. Novamente, a diferenciação parte do conteúdo que compreende essas informações. No caso dos dados pessoais, trata-se de "informação relacionada à pessoa natural identificada ou identificável" (Brasil, 2018a, artigo 5º, inc. I) e, no caso dos dados sensíveis, trata-se da correspondência a uma série de critérios ancorados em marcadores sociais. A obtenção de dados sensíveis, assim como a obtenção de comunicações privadas, demanda maior rigor na imprescindibilidade da medida. Mesmo que a aplicação da LGPD não seja direcionada a aspectos punitivos, a similaridade entre as duas legislações e a base principiológica do Regulamento Geral sobre a Proteção de Dados europeu (Regulation EU 2016/679), que inspirou a LGPD (Doneda, 2021), no que toca à distinção entre dados que compreendem uma noção mais intrusiva sobre o sujeito, deve ser reafirmada. Há diversas classificações possíveis sobre dados, como indica Lyon (2018, p. 72). No entanto, aqui vamos nos ater à nomenclatura genérica "dados", para descrever tanto os dados cadastrais quanto os dados sensíveis, quando esta diferenciação não for explicitada.

No segundo nível, precisamos diferenciar a coleta de dados da coleta de dados em larga escala. A quebra de sigilo em larga escala ocorre quando empresas de conexão ou de serviços online divulgam os registros de atividades de usuários que não foram previamente identificados pelas autoridades, baseando-se em critérios de busca genéricos ou aleatórios – como ter circulado por uma determinada área em certo período ou ter feito pesquisas por palavras específicas em *sites* de busca, como indicam Moura e Marchionatti (2020).

Há duas situações, que embora sejam distintas, nos parecem ser regradas pelo mesmo dispositivo legal: o artigo 22 e seus incisos do Marco Civil da Internet (Brasil, 2014). A primeira medida é o que poderia se chamar de quebra de sigilo direta individualizada. Tal medida é realizada, a título exemplificativo, quando o indivíduo X está sendo investigado e a autoridade competente realiza o pedido de quebra de sigilo telemático de registros de conexão. O juiz, posteriormente à verificação dos critérios do artigo 22, realiza a requisição dos dados do sujeito X, que são fornecidos. A segunda medida é a quebra de sigilo em larga escala ou em massa, na qual o indivíduo X também está sendo investigado, no entanto, se quer determinar se pessoa(s) relacionada(s) ao indivíduo X estava(m) em determinada área, a autoridade competente realiza o pedido de quebra de sigilo de registros de conexão que compreende determinada área; logo em seguida à verificação dos critérios do artigo 22, o juiz realiza a requisição de todos os registros de conexão da área e esses dados são

fornecidos, cabendo ao requerente pormenorizar tais dados e estabelecer um nexo com o indivíduo investigado.

Aqui não nos parece claro se esse pedido deve se restringir aos dados cadastrais (registros de acesso e conexão) ou se a amplitude de tal medida também abarcaria os dados de conteúdo (comunicações privadas). Muito embora a questão aludida seja de imensurável relevância, o que importa destacar é que resta evidente a existência de uma diferença na amplitude das duas medidas, especialmente na inevitabilidade de fornecimento de dados de indivíduos que não têm qualquer relação com o objeto da investigação, no caso de coleta em massa. Ainda, é nebulosa a afirmação de que a coleta de dados em larga escala é regida pela mesma fundamentação de uma coleta individualizada, todavia, nos parece que no caso de dados cadastrais seria possível afirmar que sim.

Assim, quando tratamos de "coleta de dados em larga escala", concluímos que não há uma especificação quanto ao tipo de dado passível de ser coletado em larga escala; ou seja, não se pode afirmar que haveria procedimento mais rigoroso para a coleta em massa de dados de comunicações privadas do que para a coleta de dados cadastrais. Ao mesmo tempo, diante da distinção das situações de coleta de dados, seria possível afirmar que o fornecimento de dados em larga escala não possui regime próprio positivado de fundamentação legal que possa, porventura, criar obrigações mais rigorosas para a aplicação da medida.

Por óbvio, os ditames das Ciências Criminais e os dispositivos positivados esparsos fornecem um arcabouço jurídico para a ponderação dessas medidas, a começar pela Constituição Federal e os direitos dos titulares de dados; a constitucionalidade da autodeterminação informativa e seu *status* como direito fundamental é amplamente reconhecida (Sarlet, 2021). Concorrentemente, é preciso denotar o fato de que os motivos relevantes de vulnerabilização desses direitos têm forte vinculação com os discursos de segurança nacional e com as novas linhas que as relações "tecnopolíticas" (Sabariego; Amaral; Salles, 2020) traçam sobre os regimes jurídico-políticos.

Em um exercício de imaginação, ao tratar de atividades de inteligência, poderíamos presumir que, seguindo uma fundamentação genérica de defesa social e a lógica constitucional de ponderação, a coleta massiva de dados de fato ocorre, possivelmente individualizada – dirigida a determinado sujeito ou organização criminosa –, mas a partir de um mecanismo onde não é possível, por meio de pesquisa, aferir a legitimidade da coleta pela própria natureza da atividade de inteligência. Tal cenário é de difícil verificação empírica, visto que a Lei de Acesso à Informação (Lei 12.527, de 18 de novembro de 2011) em seu artigo 4º, inc. III, classifica as informações sigilosas como aquelas que são imprescindíveis para segurança da sociedade e do Estado, e, logo, não passíveis de divulgação (Brasil, 2011).

Os espaços de admissibilidade desses pedidos nos levam à análise de uma gama ampla de dispositivos. Faz-se uma breve referência à lei que instituiu a Agência Brasileira de Inteligência em 1999 (Lei 9.883, de 7 de dezembro de 1999), pois a amplitude da questão da inteligência demanda maior explicação e excede o objeto do artigo[2]. De maneira geral, pode-se afirmar que a Lei não trata especificamente de coleta massiva de dados, apesar de fazer referência às competências de planejamento de ações e obtenção de análise de dados em seu artigo 4º, inc. I. O controle e a fiscalização da atividade de inteligência, como consta no *mandamus* do art. 6º da mesma lei, são exercidos pelos Poderes Legislativo e Judiciário, mas a legislação e a regulamentação dessa estrutura não fazem menção específica aos mecanismos de requisição de dados, à autoridade nacional de proteção de dados, tampouco elaboram quanto à existência de obrigações próprias que devem ser cumpridas pelo Poder Público nesses pedidos.

Seguindo a malha de dispositivos que atravessa a questão, podemos fazer menção à LGPD. A LGPD não é aplicável às atividades de investigação e repressão de infrações penais, apesar dos direitos ali elencados influenciarem nas garantias processuais penais que deverão ser observadas por meio da possibilidade de analogia. De forma transversal, a Lei de Interceptação Telefônica menciona os dados telemáticos, estabelecendo critérios para seu requerimento. O procedimento ocorre por meio de uma verificação concentrada no polo judicial quanto à admissibilidade da medida. É feito o requerimento pela autoridade competente e o Magistrado verifica se este cumpre as hipóteses legais. Apesar de aplicável aos dados telemáticos, a lei não adentra nos pormenores específicos do ambiente digital, tampouco o caso de pedidos em larga escala. O Código de Processo Penal (Brasil, 1941) estabelece os parâmetros de medidas de busca e apreensão para a coleta de elementos de convicção, e, na fase administrativa, atribui ao juiz das garantias a competência para decidir sobre requerimentos de busca e apreensão, afastamento do sigilo e modalidades de interceptação.

Aqui, vale ressaltar uma diferenciação que nos parece merecer maior cuidado. A jurisprudência realiza uma distinção entre a interceptação de dados e a quebra de sigilo de dados armazenados. A diferença prática necessita de maior elucidação sobre como dados são enviados na internet ou, em termos mais técnicos, o envio de pacotes por meio de aplicações de conteúdo e de conexão e a quebra de procedimentos criptográficos no envio de dados. Por meio de voto da Ministra Rosa Weber, em sede de repercussão geral no Recurso Extraordinário 1.301.250 do Rio de Janeiro, interposto pela Google Brasil Internet Ltda. e pela Google LLC contra acórdão

2. Para uma pormenorização do arcabouço jurídico de atividades de inteligência, ver Gonçalves (2010).

do Superior Tribunal de Justiça que negou provimento a superior recurso ordinário em mandado de segurança, temos esclarecida a diferenciação referida:

> "A determinação do Magistrado de primeiro grau, de quebra de dados informáticos estáticos, relativos a arquivos digitais de registros de conexão ou acesso a aplicações de internet e eventuais dados pessoais a eles vinculados, é absolutamente distinta daquela que ocorre com as interceptações das comunicações, as quais dão acesso ao fluxo de comunicações de dados, isto é, ao conhecimento do conteúdo da comunicação travada com o seu destinatário. Há uma distinção conceitual entre a quebra de sigilo de dados armazenados e a interceptação do fluxo de comunicações. Decerto que o art. 5º, X, da CF/88 garante a inviolabilidade da intimidade e da privacidade, inclusive quando os dados informáticos constarem de banco de dados ou de arquivos virtuais mais sensíveis. Entretanto, o acesso a esses dados registrados ou arquivos virtuais não se confunde com a interceptação das comunicações e, por isso mesmo, a amplitude de proteção não pode ser a mesma." (Brasil, 2021)

Ainda, segundo entendimento postulado no acórdão do Superior Tribunal de Justiça proferido em sede de Recurso Ordinário em Mandado de Segurança 61.302 do Rio de Janeiro:

> "Logo, a quebra do sigilo de dados armazenados, de forma autônoma ou associada a outros dados pessoais e informações, não obriga a autoridade judiciária a indicar previamente as pessoas que estão sendo investigadas, até porque o objetivo precípuo dessa medida, na expressiva maioria dos casos, é justamente de proporcionar a identificação do usuário do serviço ou do terminal utilizado" (Brasil, 2020a).

Por óbvio, quando se busca a identidade de determinado investigado não seria possível a individualização deste nos termos da Lei de Interceptação Telefônica. No entanto, quando se trata de investigado já identificado, a diferenciação do patamar de proteção entre esses dois tipos de dados se torna problemática.

A obtenção de dados arquivados pelos provedores de conexão e de aplicações na internet é diferente da captura desses mesmos dados em trânsito. Porém, diante da instantaneidade do armazenamento de comunicações em servidores de controladores e operadores, essa distinção ainda faz sentido? Um dado armazenado milésimos de segundo depois do envio não gozaria da mesma proteção de um dado em trânsito? Ou seja, deveríamos repensar os critérios de fornecimento de dados, mesmo aqueles armazenados, dada a velocidade do armazenamento. Qual seria o critério temporal adequado? Um pedido para o fornecimento de dados que abdica das exigências da Lei de Interceptação Telefônica poderia ser feito em 24 horas? Em uma hora? Em dez minutos? Não há indicação clara. O Marco Civil aborda

critérios de admissibilidade, mas que não possuem o mesmo rigor do procedimento de interceptação. A lei determina a possibilidade de obtenção de dados dos titulares mediante requerimento. Ela depende de ordem judicial, e um critério tríplice está positivado para determinar sua admissibilidade: fundados indícios da ocorrência do ilícito; justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e indicação do período ao qual se referem os registros.

Quanto a esta última exigência, o Superior Tribunal de Justiça, em interpretação restritiva dos dispositivos contidos no Marco Civil da Internet, entendeu, no HC 587.732/RJ, de relatoria do Ministro Nefi Cordeiro, que:

> "Apesar de o artigo 22, III, da Lei n. 12.965/2014 determinar que a requisição judicial de registro deve conter o período ao qual se referem, tal quesito só é necessário para o fluxo de comunicações, sendo inaplicável nos casos de dados já armazenados que devem ser obtidos para fins de investigações criminais." (Brasil, 2020b)

Tomemos como exemplo os serviços de mensageria privada. A autoridade policial que requer ao juízo a quebra de sigilo de investigado ou o representante do Ministério Público que requer a quebra de sigilo do réu/investigado (em caso de processo já em curso ou de investigação por órgão do *parquet*) intenciona por meio dessa obter dados estáticos que são armazenados nos servidores de determinado serviço diante do dever de guarda destes dados positivado em legislação. Já à medida que intenciona a interceptação telemática desses dados procura visualizar a transmissão de mensagens em curso, quando ocorre envio e subsequente recebimento. Nesse último caso, medidas técnicas para a quebra de criptografia no envio de pacotes ou a instalação de malware no alvo investigado ou réu podem ser opções viáveis. Ambas as opções apresentam problemáticas específicas quanto à fragilização da privacidade e da autodeterminação informativa, processo inquisitorial, extensão do controle governamental, meios de produção de prova, limites de investigação oculta e diversos outros atravessamentos possíveis. Mas o ponto que este trabalho pretende destacar é a constatação de que o imperativo de velocidade que emerge com as novas tecnologias fragiliza o estabelecimento de parâmetros que sustentam a diferença entre um dado em curso e um dado armazenado, gerando o risco de transformar a quebra de sigilo em interceptação por via reflexa.

A forma massiva de coleta de dados em larga escala, sobretudo por provedores de aplicação na internet, expõe como a distinção entre dados em trânsito e dados armazenados se torna difusa no cenário atual. A maneira com que as empresas geram novos circuitos de dados – ao armazená-los ininterruptamente – retira a efemeridade de uma comunicação instantânea – antes resguardada exclusivamente

pela proteção à interceptação –, transformando-a em um elemento "eterno" (por pelo menos seis meses) alocado em um banco de dados imediato e atualizado constantemente. Essa relação faz emergir a pergunta maior: as aplicações de internet já não superaram, elas mesmas, essa diferenciação? A capacidade de analisar dados em tempo real é um dos elementos essenciais da "algoritmização da vida" (O'Neil, 2020), uma das ferramentas mais perniciosas do governo exercido por essas plataformas.

3. O fornecimento de dados em larga escala

A problemática quanto à questão aqui tratada diz respeito à evidenciação dos mecanismos de admissibilidade dos pedidos de quebra de sigilo telemático em larga escala. O que tratamos até o momento, apesar de compartilhar características com os procedimentos de larga escala, são procedimentos vinculados a uma dimensão individual, nos quais a autoridade competente requer a medida cautelar. A verificação de necessidade da medida de obtenção de dados compete ao Juiz, que, ao confirmar a presença dos pressupostos necessários, envia a requisição para os provedores de aplicações ou de conexão, ou melhor, submete esse pedido aos mecanismos de *compliance* próprios das empresas, efetivamente reconhecendo uma nova jurisdição.

Os provedores de aplicação e conexão, ao receberem a medida, enviam (ou não) os dados requisitados. Ainda há uma terceira camada de verificação, aquela que implica a cooperação entre regimes jurídicos de países distintos. É importante lembrar, como indica o artigo 11, § 2º, do Marco Civil da Internet, que, mesmo que as empresas sejam sediadas no exterior, ao ofertar serviço ao público brasileiro, submetem-se ao regime jurídico deste país. Diversos servidores de empresas privadas, por razões específicas geopolíticas e econômicas, estão fora do Brasil, o que, na prática, substancia a pulverização do princípio da territorialidade. Como é sabido, na Ação Declaratória de Constitucionalidade 51, o Supremo Tribunal Federal asseverou que o juiz pode realizar a requisição de dados diretamente às empresas responsáveis por seu tratamento (Brasil, 2023b). A decisão implica na não aplicação de acordo de cooperação internacional em matéria penal o que, na prática, implicaria em um novo exame de admissibilidade da medida no país sede. O Acordo de Assistência Judiciária em Matéria Penal (Decreto 3.810, de 2 de maio de 2001), por exemplo, é o dispositivo que fundamentava os pedidos para empresas sediadas nos Estados Unidos, e a frustração de pedidos de dados atinentes ao dispositivo é reconhecida pelo Ministério da Justiça (Ofício 965/2018 em sede da Ação Declaratória de Constitucionalidade 51) como decorrente de ausência de *probable cause*, requisito específico para a quebra de sigilo na legislação americana (Brasil, 2018b).

O que importa destacar aqui é que a concessão do pedido de envio de dados é regida sob um espaço de veridição que compete com a questão da "soberania das plataformas" (Bratton, 2015, p. 26, tradução livre). Para Bratton, a soberania da plataforma é:

> "uma combinação ainda imatura de subjetividade política legalmente articulada (às vezes determinada pela posição geográfica e, às vezes, não) e uma soberania infraestrutural produzida em relação às infraestruturas de plataforma da computação em escala planetária, independentemente de serem de propriedade privada ou pública."

Há uma verdadeira inversão na lógica soberana de proteção do sujeito de direito ou do cidadão, que passa a ser reconhecido, tanto pelas plataformas quanto pela interação entre elas e agências estatais, como usuário. O usuário é consubstanciado não pela malha jurídica de garantias que limitam a intervenção punitiva, mas pela relação de poder estabelecida entre as plataformas e as agências punitivas concretamente centrada na propensão de determinado serviço a fornecer certo dado que, não custa lembrar, é gerado por ele mesmo.

Apesar de não eliminar os acordos de cooperação mútua, a decisão do Supremo Tribunal Federal reforça, no plano jurídico, que a requisição de dados deve ser regida pela manifestação da autoridade policial ou do Ministério Público e de subsequente ordem judicial dirigida à empresa. Na prática, as novas linhas territoriais traçadas pela globalização e o crescimento das *big techs* continuam a depender de decisões políticas que traçam novos territórios de disputa. A opção de uma plataforma por alocar seus servidores em determinado espaço é um dos fatores principais de viabilização ou impedimento das requisições de fornecimento.

É certo que mecanismos de cooperação diplomáticos continuarão, em certa medida, exercendo influência, mas a questão essencial está na percepção crítica de que o reconhecimento da constitucionalidade da requisição direta aos provedores indica um reconhecimento jurídico do deslocamento dos centros de poder, uma confiança tácita no *compliance* das empresas que são objeto da requisição.

Uma expansão do arcabouço legal brasileiro quanto à disponibilização de dados e à criação de outros organismos de verificação de admissibilidade poderia evitar a frustração no cumprimento das medidas, questão destacada pelo Ministério da Justiça e, ao mesmo tempo, limitar a ingerência do *compliance* nessas empresas e fornecer um mecanismo de garantia aos direitos do investigado ou réu, para que a vulnerabilização de direitos atinentes ao portador de dados seja precedida de verificação de imprescindibilidade robusta.

O Superior Tribunal de Justiça já se pronunciou quanto ao envio de dados em larga escala, em sede de recurso do Mandado de Segurança 61.302 do Rio de Janeiro.

O acórdão trata da constitucionalidade da coleta de dados em larga escala (por identificação geográfica) e da violação ao direito fundamental da privacidade. O tribunal entendeu que a coleta de dados em larga escala não demanda regime de observação de garantias mais rigoroso. A decisão é fundamentada em primeiro plano pelo princípio da ponderação, afirmando a inexistência de direito absoluto ao sigilo. Em segundo plano, a decisão, por meio de interpretação da gravidade do delito e tempo de investigações, reforça a necessidade da medida, argumentando por sua proporcionalidade. A decisão reflete a ampliação do espaço da fase pré-processual e indica a inversão dos valores de contenção do direito penal, que já é transversalmente fundamentada pelos métodos de investigação na coleta e interceptação de dados positivados na Convenção de Budapeste – Decreto 11.491, de 12 de abril de 2023 (Brasil, 2023a). Mas, acima de tudo, incorpora a lógica de acumulação de dados como um novo normal.

Os mecanismos que autorizam a coleta de dados em larga escala devem exigir diferentes tipos de juízos de admissibilidade mais rigorosos específicos? O questionamento gera dois desdobramentos. Primeiro, pressupõe uma admissão tácita; uma ótica realista (Fisher, 2009) que parte da impossibilidade de imaginar um horizonte político-jurídico mais amplo, ao menos neste artigo, que seria consubstanciado por uma aposta na total vedação de tais medidas. Tal posição é tática, pois a malha de relações que se desdobram na discussão mais ampla tecnopolítica da perniciosidade das "práticas de assujeitamento" (Foucault, 1995) constituiria um artigo em si. Assim, abdicamos de trilhar tal caminho por entender a dimensão teórico-crítica que está em aberto, e não por discordar das linhas de fuga que ela proporciona. Segundo, faz emergir uma constatação: a coleta, a organização, o gerenciamento e o governo de dados já acontecem por meio das plataformas e da relação entre empresas e Estado, o que torna tal diferenciação ultrapassada.

A teoria crítica é munida de um manancial de exemplos que exploram não só como os dados são coletados, mas como as subjetividades são produzidas, como sujeitos – jurídicos ou não – são construídos. Modelos de inteligibilidade como os *Dopplegänger* digitais (Harcourt, 2015), a hibridização do ciborgue (Haraway, 2009), o manifesto Hacker (Wark, 2004), a algoritmização da vida (Jesús et al., 2021), os sistemas ópticos (Foucault, 2014; Mathiesen, 2013), o capitalismo de vigilância (Zuboff, 2019), entre vários, podem ser usados para explicar o processo de coleta de dados. No entanto, aqui mencionaremos a ideia de filtragem colaborativa defendida por Galloway (2014), por conseguir sintetizar a modulação inédita que emerge com a nossa sociedade, a qual ele chama de sociedade de protocolo. Segundo o autor, a filtragem colaborativa é distinta dos outros modelos anteriores de coleta de dados, pois:

> "funciona por meio de um processo de interpelação (seleciona o interior dos conjuntos de dados ao invés do exterior), não é possível qualquer melhora no reservatório de dados. Então, a filtragem colaborativa assegura homogeneidade estrutural ao invés de heterogeneidade" (Galloway, 2014, p. 114, tradução livre).

A construção de bancos de dados de larga escala, altamente descritivos e ao mesmo tempo reducionistas, faz-nos perceber que a lógica de acumulação que alicerça o modelo de negócios dessas empresas está sendo incorporada pelas agências punitivas estatais. Assim, ao admitir a existência desse circuito de coleta massiva de dados pelas *big techs*, a posição essencialmente "jurídica", que deriva do entendimento da matriz de poder hobbesiana (Foucault, 2020), sustenta um discurso de demanda de maior intervenção do Estado por meio de regulamentação e seu próprio regime jurídico de coleta de dados em larga escala.

Nesse panorama, percebe-se que o Brasil ainda não possui legislação robusta e clara que evidencie os procedimentos que devem ser tomados na coleta massiva de dados, o que não constitui necessariamente uma lacuna, mas um alargamento de espaço de ingerência das empresas de tecnologia, visto que esse tipo de coleta já é realizado por elas. Assim, como forma de iluminar caminhos possíveis a serem trilhados, a legislação inglesa pode nos fornecer um exemplo de como esse regime poderia ser gerido.

4. Possibilidades de legislação comparada: o sistema de "proteção dupla"

O regime jurídico inglês é o da *common law*, mas procedimentos específicos podem servir como uma pedra de toque para a análise crítica de legislação que porventura venha a ser aplicada em nosso ordenamento. O procedimento de *double lock* ou "fechamento duplo" ou de "proteção dupla" contém, em sua própria nomenclatura, a perniciosidade de medidas de regulamentação do espaço tecnopolítico. O duplo fecho pode ser encarado como uma regulamentação que propaga a legitimidade e o reconhecimento das *big techs* como gerenciadoras da vida, reforçando a aquiescência ao circuito econômico sob o qual os dados são governados, fechando-nos ainda mais no circuito de extração de dados. O duplo fecho pode ser visto como a expansão de técnicas de vigilância do próprio Estado. Afinal, os dados necessariamente passam a circular em maior número de órgãos governamentais. E o duplo fecho pode funcionar como freio à ingerência das *big techs*, como limite das possibilidades do tratamento de dados. Esses três vetores não são mutuamente excludentes: funcionam de forma recíproca, estabelecendo tensões próprias de um mundo conectado e que admite novos espaços de produção jurídica.

O sistema de "proteção dupla" é um mecanismo de controle de mandados de busca e apreensão na realização de medidas investigativas de quebra de sigilo

telemático e de interceptação telefônica que regulamenta os mandados de busca e apreensão e interceptação de dados em caráter individual (*targeted warrants*) e de caráter coletivo (*bulk warrants*), ou o que convencionamos nomear de "coleta de dados em larga escala". O mecanismo foi instituído por meio do *Investigatory Powers Act* (Lei dos Poderes de Investigação) de 2016. O sistema de proteção dupla funciona a partir da verificação externa em duas instâncias da necessidade da medida de quebra de sigilo ou de interceptação de dados em massa e individualizados. A autoridade emite pedido de utilização do mecanismo de investigação para a quebra de sigilo ou interceptação que passa em primeiro grau por autoridades específicas determinadas pela lei e, em segundo grau, por um dos comissários Judiciais do *Investigatory Powers Commissioner's Office* (Escritório do Comissário de Poderes Investigativos). O comissário deve analisar a admissibilidade da medida, aprovando (ou não) a expedição do mandado e supervisionando a aplicação, a duração e a amplitude das medidas de vigilância (Reino Unido, 2016, 2022).

A interceptação de comunicações e a obtenção de registro de alvos específicos são também regidas por outra legislação, a *Regulation of Investigatory Powers Act* (Lei de Regulamentação de Poderes Investigativos). Cabe denotar tal diferença, pois o ordenamento jurídico brasileiro não possui legislação específica atinente à obtenção de coleta massiva de dados, tampouco mecanismo que garanta a proporcionalidade, a finalidade e a adequação dessas medidas.

O *Investigatory Powers Act* estabelece os limites sob os quais os poderes investigativos poderão interferir no direito à privacidade. Ainda que tenha saído da União Europeia, o Reino Unido reproduziu o Regulamento Geral de Proteção de Dados (RGPD) na sua legislação nacional, possibilitando alterações que independem de deliberação do parlamento europeu. Em sua lei específica, a *Data Protection Act* de 2018 (Lei de Proteção de Dados), a legislação se refere ao Regulamento Geral de Proteção de Dados tanto na definição de termos utilizados quanto no estabelecimento de princípios. A diferenciação, por exemplo, entre os termos *controller* e *processor* no *Data Protection Act* – que, por sua vez, são reproduzidos na nossa LGPD sob os termos controlador e operador – decorre de definições instituídas pela RGPD. Quanto à diferenciação entre dados armazenados e interceptação de dados, a introdução da lei explicita que as provisões ali contidas se aplicam para ambos os tipos de dados (Reino Unido, 2018).

Primeiramente, é importante destacar que a legislação estabelece que a requisição, a renovação e o cancelamento de pedidos de quebra de sigilo estão sujeitos a determinados critérios. Ainda, não é excessivo recordar que o *Investigatory Powers Act* trata de obtenção de dados da mais variada gama de sujeitos, inclusive aqueles que não têm relação com os interesses investigativos da inteligência, mas que estão em um *data set* que inclui mais dados para além daqueles relacionados ao objeto da

investigação, ou seja, o requerimento e a eventual requisição desses dados se referem a um grande número de dados que têm a probabilidade de conter informações desses sujeitos específicos, mas inevitavelmente conterá dados de sujeitos que nada têm a ver com a investigação.

Assim como o artigo segundo da nossa Lei de Interceptação Telefônica, o *Investigatory Powers Act* estabelece a preferência pela obtenção de informação por medidas menos intrusivas, caso possível. A lei estabelece a necessidade de observância da sensibilidade da informação e adequação do nível de proteção a ela depreendido, caso a informação requerida ou requisitada seja de caráter sensível. A lei também cita o interesse público, a integridade dos sistemas de telecomunicação, os interesses de segurança nacional e econômicos do Reino Unido, assim como a necessidade de proporcionalidade e referência as garantias do *Human Rights Act* de 1998.

Enquanto o art. 22 do Marco Civil da Internet estabelece que a parte pode requerer ao juiz os dados específicos e o artigo 3º da Lei de Interceptação estabelece as autoridades que podem requerer a interceptação, o artigo 18 da lei inglesa estabelece aqueles que podem realizar o pedido de obtenção de dados de investigações individualizadas. Na legislação inglesa, são nomeados como "autoridades interceptadoras": o chefe de um serviço de inteligência, o diretor-geral da agência nacional de crimes, o comissionário da polícia de Londres, o chefe de polícia da Irlanda do Norte, o comissionário aduaneiro, o chefe de defesa nacional e inteligência, além de autoridades internacionais específicas que possuem acordo de cooperação mútua. Ministros de Estado também podem emitir mandados em nome de uma autoridade interceptadora em caso de interceptações específicas em situações delimitadas por lei.

A aprovação dos mandados de quebra de sigilo e de busca e apreensão individualizada é estruturada pelo artigo 23 da legislação inglesa do *Investigatory Powers Act*. A aprovação dos pedidos de quebra de sigilo segue duas linhas gerais: ter motivos relevantes e proporcionalidade entre meios e fins. A definição do que é considerado como relevante é também parte da legislação, e é pormenorizada por três situações gerais descritas no artigo 20: interesse de segurança nacional; prevenção contra crimes graves; e defesa de interesses econômicos do Reino Unido, desde que se conectem com o campo da defesa nacional. Muito embora a gravidade do crime seja definida pela Seção 263, § 6, n. 9[3], não há definição positivada dos dois últimos

3. "Aquele pelo qual uma pessoa que atingiu a idade de 21 anos e não tem condenações anteriores poderia razoavelmente esperar ser sentenciada a prisão por um período de três anos ou mais, ou que envolve o uso de violência, resulta em ganho financeiro substancial ou é conduzido por um grande número de pessoas em busca de um propósito comum" (Reino Unido, 2016).

motivos. Não passa despercebida a vagueza dessas motivações. No entanto, o duplo grau de verificação da existência de relevância do pedido em sede distinta do Judiciário poderia, em tese, servir como modelo para o Brasil. Há um alinhamento à demanda de maior rigor na verificação de admissibilidade, dada a extensão da medida, assim como aos tipos de demanda consubstanciados pelo imperativo da eficiência, o que não significa abdicar da fragilidade e perniciosidade do termo.

A Subseção do artigo 23 também exige que o Comissário Judicial aplique os mesmos princípios que seriam aplicados por análise judicial e demanda um tratamento minucioso, de maneira a assegurar que o comissário não vá exceder seus deveres gerais em relação à privacidade, devendo agir como se estivera em sede judicial. Em caso de recusa, a resposta deve discriminar os motivos da negação do pedido e possibilitar recurso administrativo.

Há instâncias urgentes nas quais o pedido de quebra de sigilo individualizada pode ser aprovado sem a anuência do comissário judicial, instando a necessidade de controle posterior por esta figura, o que pode configurar a cessação completa ou parcial das medidas tomadas, assim como a destruição completa ou parcial do objeto dos pedidos.

O artigo 31 da legislação estabelece os critérios para autorização do pedido de quebra e busca e apreensão em relação ao indivíduo. Primeiro, ele delimita três categorias de mandado: de interceptação direcionado, de exame direcionado ou de assistência mútua. Esses mandados têm relação não apenas com uma pessoa ou organização. Em verdade, possuem um nível maior de abstração, pois podem estar adstritos a um grupo de premissas, no sentido de delimitar a coleta a partir de marcadores sociais ou preferências que ecoam os procedimentos já em curso pelas empresas de tecnologia. O artigo seguinte da lei estabelece o período de duração dos mandados e a possibilidade de renovação, estabelecendo períodos menores no caso de pedidos de urgência (cinco dias úteis) e maiores no caso de pedidos submetidos a maior prazo de deliberação por meio do sistema de dupla proteção (seis meses).

Aqui, no entanto, feitas essas considerações, nosso interesse é apontar o mecanismo chamado de *double lock*, ou duplo fecho, no requerimento massivo de informações, pois ele pode servir de modelo, indicar parâmetros possíveis para suprir a ausência de especificidade da legislação brasileira no tocante a tais questões ou despertar uma percepção crítica quanto a um eventual banimento dessas tecnologias diante da incongruência de poderes de tamanho alcance – essencialmente opacos – quando aplicados em regimes democráticos que prezam pela transparência.

A legislação possui regramento próprio para os pedidos de quebra de sigilo, assim como para os pedidos de interceptação de dados em larga escala situados nos artigos 136 a 226 IE do *Investigatory Powers Act*. A legislação enumera os pedidos

de coleta em larga escala em cinco categorias distintas: mandados de interceptação de dados em larga escala internacionais (*bulk interception warrants*), mandados de aquisição de dados em larga escala (*bulk acquisition warrants*), mandados de interferência em equipamentos em larga escala (*bulk equipment interference warrants*), mandados de aquisição de conjuntos de dados pessoais em massa (*bulk personal dataset warrants*) e mandados de aquisição de dados pessoais em massa de terceiros (*third party bulk personal datasets*). Aqui nos interessam duas categorias que permitem a coleta de dados em massa: os mandados de aquisição em larga escala, limitados pela apreensão de metadados (registros de conexão e de acesso), e os mandados aquisição de conjuntos de dados pessoais em massa, que permitem a interceptação e a apreensão de dados de conteúdo[4] que compreendem a atividade em determinada aplicação e comunicações privadas.

Muito embora os dispositivos contenham óbvias inclinações de expansão punitiva, como a provisão da alínea oitava do artigo 158, que possibilita que os dados possam sequer existir ao tempo do mandado, concentramo-nos na existência de pelo menos dois pontos relevantes: a diferenciação de pedidos de coleta de dados em larga escala aliada à sua pormenorização por meio de subcategorias e a existência de um duplo juízo de admissibilidade da medida. Em ambas as situações, é necessária a observância de maior rigor quanto à imprescindibilidade da medida, materializada pelo duplo grau exercido por um Comissário judicial, positivada nos artigos 159 e 208.

Assim como nos pedidos individuais, há uma série de critérios que deverão ser observados. Do mesmo modo que ocorre nos pedidos direcionados ou individuais, há a exigência de verificação de proporcionalidade da medida, mas, nesse caso, ela ocorre por meio de análise do secretário de Estado e, por óbvio, do comissário. Estão presentes também as mesmas motivações dos dispositivos que tratam dos pedidos individuais: interesse de segurança nacional, detecção e prevenção de crimes graves e proteção de interesses econômicos do Reino Unido, e o mesmo direcionamento no sentido de critérios de atuação: "aplicar os mesmos princípios que

4. Os mandados aquisição de conjuntos de dados pessoais em massa permitem a interceptação e apreensão de dados de conteúdo, categoria que é expressada pela nomenclatura "dados pessoais", à qual o artigo faz referência à definição do *Data Protection Act* de 2018 que, por sua vez, faz referência ao RGPD. Assim, dado pessoal significa: "qualquer informação relativa a uma pessoa singular identificada ou identificável ('titular dos dados'); uma pessoa singular identificável é aquela que pode ser identificada, direta ou indiretamente, em especial por referência a um identificador, como um nome, um número de identificação, dados de localização, um identificador online ou a um ou mais fatores específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular".

seriam aplicados por um tribunal no que toca o juízo de admissibilidade da medida." No entanto, a lei estabelece critérios adicionais, como a alínea 3 do artigo 161, que delimita que o pedido deve especificar os "propósitos operacionais" que motivam a coleta. Esses propósitos fazem parte de uma lista mantida pelos chefes do serviço de inteligência que, a cada três meses, deve ser submetida para análise de um comitê especial no parlamento.

O ponto nevrálgico da novidade possível trazida pela lei se situa na diferenciação entre mandados de coleta em larga escala (*Bulk personal dataset warrants*) específicos e gerais. Há, no artigo 203, a vedação genérica de coleta (ou coleta e exame) de conjunto de dados em larga escala gerais no que concerne às comunicações privadas, ou na nomenclatura da lei inglesa "dados protegidos" (*protected data*). A lei abre espaço para que esses dados protegidos possam ser coletados sob os ditames dos mandados de coleta em larga escala específicos, porém, mesmo que o secretário de Estado entenda pela autorização da medida, ele pode impor condições específicas, visto que tais informações são de caráter sensível.

Conclui-se que, apesar das motivações genéricas que fundamentam os pedidos, há três pontos que podem acrescentar ao debate jurídico pátrio no que diz respeito à coleta de dados: a existência de um regime próprio para a coleta de dados em larga escala, o duplo grau para a verificação de imprescindibilidade do pedido e a preocupação com os regimes de diferenciação entre dados protegidos e dados pessoais cadastrais.

Segundo o relatório da comissão do *Investigatory Powers Commissioner's Office*, no ano de 2022, foram autorizados mais de 330 mil pedidos de fornecimento de dados, individualizados e em massa (Reino Unido, 2022). Os dados demonstram um crescimento das autorizações em relação aos anos anteriores. Os procedimentos que fundamentaram seus pedidos sob a motivação de "prevenção/detecção" de crimes, constituem 81% dos pedidos, enquanto o resto é majoritariamente ocupado por pedidos que se relacionam à segurança nacional e prevenção de morte ou lesão grave.

Quanto à atuação concreta dos mecanismos de vigilância em massa, Murray et al. (2021) indicam que não há quase nenhum direcionamento voltado para os direitos humanos na coleta desses dados. O estudo também destaca a necessidade de independência entre os órgãos que constituem as fases de requerimento dos dados, assegurando a idoneidade do procedimento, assim como a análise pormenorizada exaustiva da necessidade da medida em duas instâncias. Os autores destacam a importância de um mecanismo que viabilize a autorização tanto na coleta de dados quanto no acesso a esses dados, asseverando também a necessidade de revisão judicial posterior.

5. Considerações finais

O Brasil não possui regime jurídico diferenciado para o fornecimento de dados em larga escala, mas aplica os mecanismos idênticos e observa as mesmas garantias atinentes à quebra de sigilo e à interceptação de dados que concernem ao indivíduo nos casos em que a quebra é direcionada a uma grande parcela da população (delimitada por geolocalização ou características que implicam uma grande massa homogeneizada), mas que, em verdade, é heterogênea.

Dessa forma, ao abordar o tema da "coleta de dados em larga escala", percebe-se que não há uma definição específica sobre quais tipos de dados podem ser coletados nesse formato. Em outras palavras, não se pode afirmar que existiria um procedimento mais restritivo para a coleta massiva de comunicações privadas em comparação à coleta de dados cadastrais. Ao mesmo tempo, considerando as diferentes situações em que a coleta ocorre, é possível concluir que o fornecimento de dados em grande volume não conta com um regime jurídico próprio que estabeleça exigências legais mais severas para viabilizar essa prática.

A vacuidade do argumento que diferencia dados em trânsito e dados armazenados, diante do avanço computacional exponencial, começa a surgir de maneira mais vívida, impondo novas problematizações quanto ao entendimento jurisprudencial assentado.

As proteções ao sigilo que abarcam as atividades de inteligência, aliadas à ausência material de possibilidades de verificação empírica, deixam o cenário de coleta de dados em larga escala feitas (ou não) sob justificativas de defesa social ainda mais problemáticas, pois impedem qualquer tipo de controle, anterior ou posterior. Os mecanismos que permitem a coleta de dados em larga escala devem exigir diferentes critérios de admissibilidade, com níveis específicos de rigor? Essa questão se desdobra em dois aspectos.

Primeiramente, parte-se de uma aceitação implícita da prática, adotando uma perspectiva realista que reconhece a impossibilidade, dentro dos limites deste artigo, de conceber um cenário político-jurídico mais amplo que proibisse totalmente tais medidas. Essa abordagem é estratégica, pois o conjunto de relações que compõem o debate tecnopolítico mais amplo sobre os impactos dessas práticas de controle demandaria uma análise aprofundada em um estudo próprio. Assim, optamos por não seguir esse caminho, não por discordância com as críticas existentes, mas por compreendermos que essa discussão teórico-crítica permanece em aberto.

Em segundo lugar, essa questão leva a uma constatação: a coleta, a organização, a gestão e o controle de dados em larga escala já ocorrem de forma contínua por meio das plataformas digitais e da interação entre empresas e Estado, tornando essa diferenciação um conceito ultrapassado.

Ao entender que esses mecanismos de maior alcance demandam maior tempo de deliberação e motivação robusta, os exemplos de direito comparado podem auxiliar a defender limites já existentes em outras partes do mundo para essas medidas. Mas, ao mesmo tempo, podem reforçar a expansão de mecanismos punitivos estatais na medida em que suas funções são deslocadas para as plataformas digitais.

Conclui-se que, apesar das motivações genéricas positivadas que sustentam os pedidos, há três aspectos que podem enriquecer a discussão jurídica nacional sobre a coleta de dados. O primeiro é a criação de um regime jurídico específico para a coleta de dados em grande escala, centrado na necessidade e na proporcionalidade da medida, assim como em sua revisão periódica. O segundo é a constituição de um mecanismo de controle externo dos pedidos; o sistema de *double lock* impõe um controle pormenorizado que se baseia em um duplo grau de análise para verificar a necessidade do pedido, realizado tanto pela autoridade competente quanto pelo comissário judicial. O terceiro é a atenção às distinções entre dados protegidos e dados pessoais cadastrais que, de fato, já se encontra presente na legislação brasileira, mas, neste espaço, aparece vinculada à coleta de dados em larga escala.

Por fim, não é exaustivo afirmar que a materialização da requisição de dados está regida sob um espaço de veridição que compete com a questão da soberania das plataformas, o que implica na admissão tácita de uma nova forma de jurisdição centrada no *compliance* dessas plataformas, e um deslocamento da posição de cidadão ou sujeito de direito para "usuário". Essa é a questão que vai além do tema de violações inevitáveis a direitos fundamentais: a percepção de que o regime jurídico de admissibilidade da coleta de dados não está submetido aos termos e condições da plataforma, mas na sua concreta atuação no fornecimento ou abstenção de fornecimento de dados, nas indicações de reconhecimento (ou não) de legitimidade dos pedidos e na produção de subjetividade que desterritorializa o sujeito.

Referências

AMARAL, Augusto Jobim. *Política da criminologia*. São Paulo: Tirant Lo Blanch, 2020.

BARATTA, Alessandro. *Criminología crítica e crítica del derecho penal*: introducción a la sociología jurídico-penal. Buenos Aires: Siglo XXI, 2004.

BRATTON, Benjamin. *The stack*: on software and sovereignty. London: MIT Press, 2015.

DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. In: DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JUNIOR, Otavio Luiz; BIONI, Bruno Ricardo (Coords.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021.

FISHER, Mark. *Capitalist realism*. London: Zero Books, 2009.

FOUCAULT, Michel. O sujeito e o poder. In: RABINOW, Paul; DREYFUS, Hubert. (Orgs.). *Foucault*: uma trajetória filosófica. Rio de Janeiro: Forense Universitária, 1995.

FOUCAULT, Michel. *Teorias e instituições penais*. Trad. Rosemary Costhek Abílio. São Paulo: Martins Fontes, 2020.

GALLOWAY, Alexander. *Protocol society* – How control exists after decentralization. Cambridge: MIT Press, 2014.

GONÇALVES, Joanisval Brito. Quem vigia os vigilantes? O controle da atividade de inteligência no Brasil e o papel do Poder Legislativo. *Revista de Informação Legislativa*, Brasília, ano 47 n. 187, jul.-set. 2010. Disponível em: [https://senado.leg.br/ril/edicoes/47/187/ril_v47_n187_p125.pdf]. Acesso em: 20.02.2025.

HARAWAY, Donna J. *Manifesto ciborgue*: ciência, tecnologia e feminismo-socialista no final do século XX. Belo Horizonte: Autêntica, 2009.

HARCOURT, Bernard. *A contrarrevolução*: como o governo entrou em guerra contra os próprios cidadãos. Coordenação de tradução: Augusto Jobim do Amaral e Jádia Timm Santos. São Paulo: Glac Edições, 2021.

HARCOURT, Bernard. *Critique and praxis* – A critical philosophy of illusions, values, and action. New York: Columbia University Press, 2020.

HARCOURT, Bernard. *Exposed* – Desire and obedience in the digital age. Cambridge: Harvard University Press, 2015.

LOPES, Marcus Vinícius Pimenta. *A participação ativa do acusado na persecução que utiliza a busca e a apreensão de elementos de prova digitais*. 2023. Tese (Doutorado em Direito) – Pontifícia Universidade Católica de Minas Gerais, Belo Horizonte, 2023. Disponível em: [https://bib.pucminas.br/teses/Direito_MarcusViniciusPimentaLopes_30465_Textocompleto.pdf]. Acesso em: 29.02.2025.

LYON, David. *The culture of surveillance*. Cambridge: Polity Press, 2018.

MATHIESEN, Thomas. *Towards a surveillant society* – The rise of surveillance systems in Europe. Sheffield: Waterside Press, 2013.

MOURA, Maria Thereza Rocha de Assis; MARCHIONATTI, Daniel. Quebra de sigilo em massa e proteção de dados de terceiros: como minimizar o impacto da medida sem prejudicar a ampla defesa. In: ARAS, Vladimir Barros; MENDONÇA, Andrey Borges de; CAPANEMA, Walter Aranha; SILVA, Carlos Bruno Ferreira da; COSTA, Marcos Antônio da Silva (Orgs.). *Proteção de dados pessoais e investigação criminal*. Brasília: Associação Nacional dos Procuradores da República, 2020. Disponível em: [https://anpr.org.br/images/2020/Livros/protecao_dados_pessoais_versao_eletronica.pdf]. Acesso em: 28.02.2025.

MURRAY, Daragh; FUSSEY, Pete; MCGREGOR, Lorna; SUNKIN, Maurice. *Effective oversight of large-scale surveillance activities* – A human rights perspective. AI Human Rights, 2021. Disponível em: [https://aihumanrights.blog/wp-content/uploads/2022/09/Effective_Oversight_of_Large_Scale_Surveillance_Activities_2-3.pdf]. Acesso em: 02.03.2025.

O'NEIL, Cathy. *Algoritmos de destruição em massa*: como o *big data* aumenta a desigualdade e ameaça a democracia. São Paulo: Rua do Sabão, 2020.

REINO UNIDO. Investigatory Powers Commissioner's Office (IPCO). *Annual Report of the Investigatory Powers Commissioner 2022*, London, 2022. Disponível em: [https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/Annual-Report-2022.pdf]. Acesso em: 28.03.2025.

SABARIEGO, Jesús; AMARAL, Augusto Jobim do; SALLES, Eduardo Baldissera Carvalho (Orgs.). *Algoritarismos*. Valência: Tirant Lo Blanch, 2020.

SARLET, Ingo Wolfgang. Fundamentos constitucionais: O direito fundamental à proteção de dados. In: BIONI, Bruno (Org.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021.

SCHMITT, Carl. *O conceito do político*. Petrópolis: Vozes, 1992.

SNOWDEN, Edward. *Eterna vigilância*. São Paulo: Planeta Brasil, 2019.

SOZZO, Máximo (Org.). *Reconstruyendo las criminologías críticas*. Buenos Aires: Ad Hoc, 2006.

VIRILIO, Paul. *El cibermundo*: la política de lo peor. Trad. Mónica Poole. Madrid: Ediciones Cátedra, 1997.

WARK, Mckenzie. *A hacker manifesto*. Cambridge: Harvard University Press, 2004.

ZUBOFF, Shoshana. *The age of surveillance capitalism*. New York: Public Affairs, 2019.

Legislação

BRASIL. Decreto 3.810, de 2 de maio de 2001. Promulga o Acordo de Assistência Judiciária em Matéria Penal entre o Governo da República Federativa do Brasil e o Governo dos Estados Unidos da América, celebrado em Brasília, em 14 de outubro de 1997, corrigido em sua versão em português, por troca de Notas, em 15 de fevereiro de 2001. Brasília, 02.05.2001. *DOU* 03.05.2001. Disponível em: [https://planalto.gov.br/ccivil_03/decreto/2001/d3810.htm]. Acesso em: 31.08.2024.

BRASIL. *Decreto 11.491, de 12 de abril de 2023*. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001. Brasília: Presidência da República, 2023a. Disponível em: [https://planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11491.htm]. Acesso em: 31.08.2024.

BRASIL. *Lei 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 n. 8.112, de 11 de dezembro de 1990; revoga a Lei n. 11.111, de 5 de maio de 2005, e dispositivos da Lei n. 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília: Presidência da República, 2011. Disponível em: [https://planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm]. Acesso em: 31.08.2024.

BRASIL. *Lei 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília: Presidência da República, 2014. Disponível em: [https://planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm]. Acesso em: 31.08.2024.

BRASIL. *Lei 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Presidência da República, 2018a. Disponível em: [https://planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm]. Acesso em: 31.08.2024.

BRASIL. Ministério da Justiça e da Segurança Pública. Ofício 965/2018. Cooperação jurídica internacional em matéria penal para fins de afastamento de sigilo telemático. Brasília: Ministério da Justiça e Segurança Pública, 2018b. Disponível em: [https://conjur.com.br/wp-content/uploads/2023/09/drci--stf.pdf]. Acesso em: 31.08.2024.

REINO UNIDO. UK Public General Acts. *Data Protection Act 2018*. Londres: Parliament, 23 maio 2018. Disponível em: [https://legislation.gov.uk/ukpga/2018/12/introduction]. Acesso em: 28.03. 2025.

REINO UNIDO. UK Public General Acts. *Investigatory Powers Act 2016*. Londres: Parliament, 29 mar. 2016. Disponível em: [https://legislation.gov.uk/ukpga/2016/25/introduction]. Acesso em: 28.02.2025.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Bruxelas: Jornal Oficial da União Europeia, 2016. Disponível em: [https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679]. Acesso em: 08.03.2025.

Jurisprudência

BRASIL. STF, ADC 51, rel. Min. Gilmar Mendes, j. 23.02.2023b. Disponível em: [https://portal.stf.jus.br/processos/detalhe.asp?incidente=5320379]. Acesso em: 31.02.2024.

BRASIL. STF, Repercussão Geral no RE 1.301.250/RJ, j. 06.05.2021, Manifestação da Ministra Rosa Weber. Disponível em: [https://conjur.com.br/wp-content/uploads/2023/09/stf-julgar-quebra-sigilo-telematico.pdf]. Acesso em: 31.02.2025.

BRASIL. STJ, RMS 61.302/RJ, rel. Min Rogerio Schietti Cruz, 3ª S., j. 26.08.2020a. Disponível em: [https://scon.stj.jus.br/SCON/pesquisar.jsp?b=ACOR&livre=%28%28ROMS.clas.+ou+RMS.clap.%29+e+%40num%3D%2261302%22%29+ou+%28%28ROMS+ou+RMS%29+adj+%2261302%22%29.suce.&O=JT]. Acesso em: 31.08.2024.

BRASIL. STJ, HC 587.732/RJ, rel. Min. Nefi Cordeiro, 6ª T., j. 20.10 2020b. Disponível em: [https://buscadordizerodireito.com.br/jurisprudencia/detalhes/94841421fb5e84a4d83e303949e6b211]. Acesso em: 31.08.2024.

Recebido em: 30.03.2025.
Aprovado em: 08.08.2025.
Última versão do autor: 08.08.2025.

PESQUISA DO EDITORIAL

Área do Direito: Penal; Digital

Veja também Doutrina relacionada ao tema

- Biometria, autodeterminação informativa e proteção de dados pessoais, de Adriana Espíndola Corrêa e Maria Fernanda Battaglin Loureiro – *RDCC* 36/47-74;
- Linhas gerais sobre a Lei 13.709/2018 (LGPD): objetivos, fundamentos e axiologia da lei geral de proteção de dados brasileira e a tutela de personalidade/privacidade, de Erick da Silva Regis – *RDPriv* 103/63-100;
- Os bancos de dados do Conselho Nacional de Justiça e seus reflexos na igualdade de gênero no âmbito do Poder Judiciário brasileiro, de Gabriela Lima Barreto e Maristela Eduardo Félix de Oliveira – *RDTec* 23; e
- Venda de informações biométricas, privacidade e indisponibilidade de direitos – Estudo de casos, de Patrícia Helena Marta Martins e Bruna Valeri Tavora – *BRTO* 60.

Técnicas antiforenses: obstrução da justiça ou garantia da defesa?

Antiforensic techniques: obstruction of justice or guarantee of defense?

Jamilla Monteiro Sarkis[1]
Pontifícia Universidade Católica de Minas Gerais, PUC Minas, Brasil.
jamilla.sarkis@gmail.com

Paola Alcântara Lima Dumont[2]
Faculdade Pitágoras, UNIMINAS, Brasil.
paolaa.dumont@gmail.com

DOI: [doi.org/10.5281/zenodo.17058406].

Área do Direito: Processual; Penal

Resumo: Este artigo, desenvolvido pelo método da revisão bibliográfica interdisciplinar, pretende investigar se a utilização de técnicas antiforenses

Abstract: This article is developed using the interdisciplinary bibliographical review method and aims to investigate whether the use of

1. Doutora em Direito pela Pontifícia Universidade Católica de Minas Gerais, em Estágio Pós-Doutoral na Pontifícia Universidade Católica do Rio Grande do Sul. Mestre em Direito pela Universidade Federal de Minas Gerais. Advogada e Professora. Vice-Presidente da Rede Ibero-Americana de Advocacia Criminal.
   Currículo Lattes: [http://lattes.cnpq.br/5388381867392010].
   ORCID: [https://orcid.org/0000-0002-2730-5950].
   E-mail: jamilla.sarkis@gmail.com
2. Mestre em Direito Público pela Pontifícia Universidade Católica de Minas Gerais. Especialista em Direito Penal Empresarial, Ciências Criminais e Direito Militar. Advogada e Professora Universitária.
   Currículo Lattes: [http://lattes.cnpq.br/3952748127831088].
   ORCID: [https://orcid.org/0000-0002-0559-3744].
   E-mail: paolaa.dumont@gmail.com

pela pessoa envolvida em fatos penais configura o crime de obstrução de justiça ou caracteriza exercício da garantia de defesa. Para tanto, realiza uma contextualização do problema a partir da virada tecnológica do processo e de sua adequação ao marco teórico do modelo constitucional de processo. Em seguida, analisa os conceitos e categorias de práticas antiforenses para, posteriormente, discutir o enquadramento das ferramentas antiforenses como condutas de obstrução de justiça ou como forma de exercício da defesa. Ao final, conclui que o catálogo de garantias da defesa deve ser ampliado, à medida que se incrementam os métodos de obtenção de prova a partir dos recursos tecnológicos.

Palavras-chave: Técnicas antiforenses – Obstrução de justiça – Garantia de defesa.

antiforensic techniques by the person involved in criminal proceedings constitutes the crime of obstruction of justice or the exercise of the guarantee of defense. To this end, it contextualizes the problem based on the technological turn of the process and its adaptation to the theoretical framework of the constitutional model of the process. It then analyzes the concepts and categories of antiforensic practices in order to later discuss the framing of antiforensic tools as conduct that obstructs justice or as a form of exercising the defense. Finally, it concludes that the catalog of defense guarantees should be expanded as the methods of obtaining evidence from technological resources increase.

Keywords: Antiforensic techniques – Obstruction of justice – Guarantee of defense.

Sumário: 1. Introdução. 2. Aperfeiçoamento da processualidade democrática à tecnologia. 3. Técnicas antiforenses: conceitos e categorias. 4. Seriam as técnicas antiforenses uma forma de obstrução da justiça? 5. Seriam as técnicas antiforenses uma garantia da defesa? 6. Considerações finais. Referências.

1. Introdução

O volume de dispositivos digitais em uso no Brasil – *smartphones*, *smartwatches*, *tablets* e *notebooks* – já superou o número de pessoas que habitam o país. A pesquisa mais recente sobre o tema, realizada em 2024 pelo Fundação Getulio Vargas[3], contabilizou mais de dois dispositivos digitais por habitante, dos quais mais da metade corresponde a aparelhos telefônicos.

Com o mundo e a vida, em todos os seus aspectos, ao alcance das teclas, é seguro afirmar que significativa parcela das evidências capazes de relacionar uma pessoa a fatos penais consiste em elementos probatórios digitais – imagens, vídeos, conversas em *chats*, *e-mails* e outros – armazenados em qualquer dos (vários) dispositivos digitais a que se tenha acesso.

O crescente protagonismo dessas provas digitais impacta, de maneira definitiva, a disciplina do Processo Penal e suscita "problemas relacionados a tutelas

3. Os resultados compõem a 35ª edição da Pesquisa Anual do Centro de Tecnologia de Informação Aplicada (FGVcia) sobre o Mercado Brasileiro de TI e Uso nas Empresas estão disponíveis em: [https://bit.ly/43ycPJw]. Acesso em: 20.03.2025.

constitucionais clássicas – privacidade, proteção das comunicações e devido processo legal" (Prado, 2024, p. 48).

Este artigo foca em um desses problemas: a necessária garantia dos direitos de defesa como contramedidas à sofisticação tecnológica dos métodos de obtenção de prova empregados pelas agências de segurança pública na investigação, processamento e julgamento de crimes.

Uma dessas contramedidas consiste no emprego de ferramentas antiforenses, cujos potenciais de excluir, alterar ou tornar anônimos vestígios digitais têm ensejado três espécies de repercussão processuais penais: a imposição de prisão preventiva, a imputação da figura típica de obstrução de justiça ou o incremento da pena na primeira fase da dosimetria (Sarkis, 2024).

Para a proposta do presente trabalho, adota-se como objeto a segunda espécie, consistente na imputação do crime previsto na Lei 12.850/2013[4], e que dá origem à seguinte pergunta: as práticas antiforenses caracterizam atos de obstrução de justiça ou constituem garantia da defesa?

Metodologicamente, o artigo promove, a partir do emprego do método dedutivo, uma revisão bibliográfica interdisciplinar[5], que articula obras jurídicas com trabalhos desenvolvidos no âmbito das Ciências da Computação e das subáreas da Engenharia Elétrica (tais como a Engenharia da Computação e a Engenharia de Informação).

Para a revisão bibliográfica, a coleta do material científico passou pelo acesso às bibliotecas do Senado Federal, do Supremo Tribunal Federal (STF), do Superior Tribunal de Justiça (STJ), do Instituto Brasileiro de Ciências Criminais (IBCCrim) e da Advocacia-Geral da União (AGU). Além disso, a pesquisa se valeu do acesso a periódicos com fatores de impacto assegurados pela plataforma Google Acadêmico, mecanismo que indexa conteúdos acadêmicos a partir de bases de dados nacionais e internacionais e adota, como critérios de relevância, quantidade de citações do trabalho, seus autores e meio de publicação, entre outros.

A partir desses elementos, o percurso a ser desenvolvido passa: *(a)* pela contextualização do problema, que será promovida a partir do conceito de virada

4. Exemplo de caso recente e de repercussão midiática se deu no âmbito da operação batizada "El Patrón". Um advogado foi denunciado, em concurso com seus clientes, por ter, supostamente, orientado a esposa a apagar os dados armazenados em nuvem por seu marido, que estava preso e tivera apreendido seu aparelho celular. Mais informações sobre a situação concreta podem ser obtidas em: [https://bit.ly/4hYJHyz]. Acesso em: 20.03.2025.

5. Como estratégia metodológica, a interdisciplinaridade apresenta a vantagem, entre outras, de proporcionar trocas generalizadas de informações e de críticas, contribuindo, dessa forma, para uma reorganização do meio científico e para fornecer à sociedade uma transformação institucional (Japiassú, 1976).

tecnológica e pela importância de sua adequação ao modelo constitucional de processo – marco teórico adotado nesta pesquisa; *(b)* pela compreensão interdisciplinar sobre os conceitos e categorias de práticas antiforenses; *(c)* pela discussão sobre o enquadramento das ferramentas antiforenses como condutas de obstrução de justiça ou como forma legítima de exercício da defesa.

Ao final, espera-se demonstrar que, na mesma medida em que são incrementados os métodos de obtenção de prova a partir dos recursos tecnológicos, deve ser ampliado o catálogo de garantias fundamentais para assegurar, às pessoas envolvidas em fatos penais, contramedidas que viabilizem o exercício de sua defesa.

2. Aperfeiçoamento da processualidade democrática à tecnologia

Ao longo das últimas décadas, o sistema jurídico sofreu importantes rupturas pragmáticas. Foram introduzidas mudanças que impactaram os fundamentos e propósitos de atuação das instituições a partir de sua inserção no ambiente digital (Lessig, 2009, p. 09), quando informações reais assumiram formas intangíveis e passaram a ser acessadas, democraticamente, por qualquer pessoa e em todos os lugares do mundo.

Os efeitos desse movimento, conhecido como virada tecnológica (Nunes, 2020, p. 15), transcendem sua mera aplicação instrumental. Impactam, de maneira concreta, o campo processual, seja pela mudança dos institutos jurídicos, seja pelo dimensionamento de uma nova racionalidade para a sua implementação, seja pela criação de novos institutos.

Efetivamente, a virada tecnológica não guarda relação exclusiva com a informatização (ou digitalização) judicial (por exemplo, o processo eletrônico) ou com o emprego de tecnologias no exercício das mais diversas carreiras jurídicas (por exemplo, o fluxo de comunicação via *e-mail* ou aplicativos de comunicação).

É fato que as novas tecnologias podem ser usadas para melhorar, refinar, agilizar, otimizar e turbinar as formas tradicionais de atividades forenses (Susskind, 2019, p. 34). Esse conceito de eficiência e melhoria do desempenho profissional no âmbito jurídico se adequa ao termo "automação", que envolve a inclusão de novas tecnologias em velhas práticas de trabalho. Foi esta a tônica que dominou tanto a teoria quanto a prática da interlocução entre Direito e tecnologia pelas últimas cinco décadas (Susskind, 2019, p. 34).

Todavia, muito além da mera "automação", a virada tecnológica no Direito tem potencial para revolucionar os hábitos tradicionais da atividade jurídica e de apresentar mudanças radicais, criando coisas novas, em vez de coisas velhas de novas formas (Susskind, 2019, p. 34). Trata-se, pois, da verdadeira "transformação", que passa a demandar profunda mudança nos institutos processuais e na prática jurídica.

Na fase da "transformação", porém, as interações entre tecnologia e processo originam conflitos e viabilizam novas formas de interação entre os sujeitos e instituições. Afinal, com a criminalidade se voltando aos espaços virtuais e com o incremento do controle exercido pelas agências de segurança pública nos ambientes digitais (Sarkis, 2024), parece natural que as atividades de persecução penal também sofram os reflexos da virada tecnológica.

Os métodos de obtenção de provas, em especial, são submetidos a uma verdadeira revolução a partir da tecnologia: se outrora estavam limitados a alguns aspectos da vida pessoal, como os assuntos conversados em certa ligação telefônica ou os depósitos feitos em determinada conta bancária, agora conseguem abranger absolutamente todas as esferas privadas – inclusive, aquelas que estão no nível mais íntimo e sequer são exteriorizadas, como as vontades, medos, anseios e desejos.

Muito além de carne e osso, os corpos "dataficados" (Mendes, 2024, p. 84)[6] são compostos por meios de prova digitais: senhas, impressões digitais, reconhecimento facial, biometria, geometria de mãos e orelhas, forma de íris e retina, traços vocais e faciais, marchas e frequência de digitação são algumas das fontes a partir das quais é possível extrair indícios de materialidade ou autoria delitiva.

Por isso, não se mostra mais razoável acreditar que o sistema processual e suas atuais codificações – entre elas, o Código de Processo Penal – que foram pensadas dentro de um contexto alheio às tecnologias "consigam resolver a contento e em conformidade com o devido processo constitucional democrático a obtenção de direitos por cada cidadão" (Nunes, 2023, p. 407).

O processo, na perspectiva da virada tecnológica, precisa ser pensado a partir do papel de protagonismo de cidadãos e cidadãs e dos direitos que lhes são assegurados no âmbito do modelo constitucional de processo, esquema caracterizado pela abertura e pelo vínculo total à moldura da Constituição e que condiciona a confecção, a leitura e a interpretação de todo esse sistema de proteção às diretrizes democráticas.

Concebido por Italo Andolina e Giuseppe Vignera (1990, p. 14), o modelo constitucional de processo é composto por três características gerais: a expansividade, a variabilidade e a perfectibilidade.

---

6. Sobre o termo "dataficação", Carlos Helder Mendes (2024, p. 84) escreve: "Não é demais salientar que a dataficação, pela razão numérica, traduz em *bits* qualquer evento, de modo a possibilitar o alcance da percepção do sujeito. Ou seja, percepção como aspecto subjetivo do ser atrelado a si e às suas circunstâncias. Percepção sobre si e sobre o mundo, percepção e fatos a partir do que se enxerga, escuta e fala alcançáveis por *softwares* tecnológicos de apreensão de informação, metodologia de vigilância e, por fim, métodos invasivos de investigação".

A expansividade é a característica que permite ao modelo constitucional condicionar a forma dos procedimentos judiciais a serem desenvolvidos pelo legislador infraconstitucional; enquanto isso, a variabilidade indica sua capacidade de assumir diversas formas, a fim de adaptar à Constituição as figuras processuais e possibilitar sua aplicação a escopos definitivos; já a perfectibilidade designa a possibilidade de que o modelo constitucional seja constantemente aperfeiçoado pela legislação ordinária.

Com a proposta de conferir maior dinamismo à implementação concreta dos princípios constitucionais – outrora vistos pela perspectiva estática e formal –, o modelo constitucional de processo considera a complexidade da atividade decisória, motivo pelo qual "permite ao intérprete esboçar um verdadeiro e próprio esquema geral de processo, capaz de formar o objeto de uma exposição unitária" (Andolina; Vignera, 1990, p. 13, tradução nossa).

Entre os princípios relacionados na Constituição da República de 1988, o contraditório, a ampla defesa, o direito à prova, a isonomia, o devido processo legal, a fundamentação das decisões e o juízo natural são direitos que permitiram a construção de um procedimento jurisdicional legítimo.

É interessante notar, nesse sentido, que a dinâmica do modelo constitucional de processo permite a adequação às suas diversas espécies – processos jurisdicionais civil, penal, trabalhista, militar, eleitoral, constitucional e legislativo. Para a disciplina do Processo Penal, seria possível trabalhar o modelo constitucional de processo para além de uma perspectiva civilista, desde que destacadas as suas especificidades e demarcada a sua dependência em relação aos direitos fundamentais (Barros, 2009, p. 332).

As particularidades do Processo Penal o tornam um microssistema com direitos fundamentais específicos e tratamento diferenciado em comparação ao Processo Civil, "justamente em razão dos direitos fundamentais que visa tutelar, notadamente a liberdade dos cidadãos" (Barros, 2009, p. 332).

Reconhecidas, pois, as características particulares de cada espécie processual, restaria preservada a concepção de um esquema geral, retirado da Constituição, e que permite a consolidação do processo como direito fundamental a partir da principiologia que lhe sustenta.

Concretamente, na medida em que adota uma base principiológica uníssona que se funda em um esquema geral, o modelo constitucional de processo torna-se uma entidade de modelo único e tipologia plúrima, expressão que manifesta a ideia de que, se há apenas um paradigma constitucional de processo, também existe no sistema uma pluralidade de procedimentos jurisdicionais (Andolina; Vignera, 1990, p. 15).

É como esquema único de tipologia plúrima que o modelo constitucional de processo reconhece, na Constituição, sua base uníssona de princípios – entre eles, os que definem o processo como direito fundamental – e, a partir deles, se expande, se especializa e se aperfeiçoa.

Diante dessas características, exige o modelo constitucional de processo que seus intérpretes – independentemente do poder ao qual se vinculam – o compreendam "tanto a partir dos princípios-bases como, também, de acordo com as características próprias daquele processo" (Barros, 2009, p. 335), tudo isso sem que se afaste da máxima dependência entre o processo e os direitos fundamentais.

Nas especificidades do Processo Penal, o próprio texto constitucional o reconhece como microssistema em razão da magnitude do direito fundamental que pretende amparar: a liberdade (Barros, 2009, p. 336). Os exemplos de direitos fundamentais relacionados à liberdade, próprios do microssistema do Processo Penal, não se limitam ao sentido de ir e vir, abrangendo também a presunção de inocência, a não autoincriminação, a intimidade, a privacidade e a inviolabilidade.

Cumpre ressaltar que, mesmo refletindo a preocupação com o combate à criminalidade quando atribui maior rigor no combate aos crimes hediondos e equiparados (artigo 5º, XLIII), a Constituição da República de 1988 não dispensa a necessidade de uma interpretação subordinada ao modelo constitucional de processo. Não prevê, pois, exceções aos direitos fundamentais.

Mas, mesmo com o reconhecimento do microssistema processual penal pela Constituição, permanece a dificuldade de compatibilizá-lo: "são épocas difíceis" para o constitucionalismo essas em que o sentimento de Constituição é aniquilado pela continuidade e prevalência de práticas típicas da ordem autoritária" (Carvalho Netto, 2004, p. 25).

As matrizes teóricas díspares e contraditórias do vigente Código de Processo Penal acabam por exigir um esforço ainda maior para sua interpretação em conformidade com a Constituição, como se depreende do modelo constitucional de processo. Por isso, qualquer proposta relacionada aos direitos fundamentais precisa, necessariamente, partir da premissa constitucional e democrática de sua prevalência, com vistas à liberdade da pessoa envolvida em fatos penais.

É necessário, nesse sentido, que o microssistema processual penal se expanda a fim de condicionar à Constituição a atuação do legislador infraconstitucional; que se varie para adaptar à Constituição as medidas de cunho processual penal; e que se aperfeiçoe para permitir a constante promoção de melhorias das leis e decisões ambientadas ao modelo constitucional de processo.

Para os objetivos deste artigo, o último aspecto – da perfectibilidade – tem especial relevância. Os impactos gerados pelos fenômenos da tecnologia no Processo Penal devem levar à perfectibilidade (ou aperfeiçoamento) de direitos e garantias

fundamentais que compõem a base principiológica uníssona do modelo constitucional de processo, cujos desenvolvimento e vigência tornam-se cada vez mais necessários no ambiente digital.

No item a seguir, será analisado um conjunto de práticas – denominadas antiforenses – que, diante do potencial de oferecer às pessoas inseridas no contexto virtual ferramentas para o exercício de direitos e garantias fundamentais, têm sido percebidas como nocivas ou, até mesmo, criminosas.

3. Técnicas antiforenses: conceitos e categorias

Existem diversas definições para as técnicas antiforenses. Dos múltiplos conceitos relacionados ao termo (Conlan; Baggili; Breitinger, 2016), é curioso perceber um aspecto comum: a conotação negativa atribuída a essas ferramentas.

A primeira referência sobre o tema conceitua as técnicas antiforenses como método de "ocultar uma tentativa de invasão do sistema" (Shirani, 2002). Essa definição é seguida por muitas outras, sempre com tom de reprovabilidade.

Alguns exemplos são: "tentativa de limitar a identificação, coleta, agrupamento e validação de provas digitais" (Peron; Legary, 2005); "tentativas de afetar negativamente a existência, a quantidade e/ou a qualidade das provas digitais de uma cena de crime, ou tornar o exame dessas provas difícil ou impossível de ser realizado" (Rogers, 2006); "coleção crescente de técnicas que frustram as ferramentas forenses, as investigações e os investigadores" (Garfinkel, 2007); "métodos utilizados para impedir o processo de investigação digital conduzido por investigadores forenses legítimos" (Albano et al., 2011); ou "métodos científicos são usados para simplesmente frustrar os esforços forenses em todos os estágios forenses" (Dahbur; Mohammad, 2012); "uma série de contramedidas adotadas para frustrar ou se esquivar de investigações forenses" (Jain; Chhabra, 2014):

> "qualquer técnica, ferramenta de *hardware* ou *software* capaz de impedir ou retardar a análise forense de um portador de dados e afetar, negativamente, a existência, a quantidade, a autenticidade ou a qualidade das provas digitais disponíveis em um dispositivo" (Mason; Sheldon; Dries, 2017).

"Invalidar", "comprometer", "dificultar", "frustrar", "impossibilitar", "impedir", "disfarçar", "falsificar", "esquivar" e "retardar" são alguns dos verbos selecionados para atribuir significado às ações antiforenses. Seu papel, nesse sentido, seria de antagonismo em relação à atividade de investigação desempenhada sobre provas digitais.

Essa característica parece ser confirmada pela origem etimológica do termo "antiforense": o prefixo "anti" tem origem no grego antigo e denota a ideia de

oposição ou contrariedade; já por "forense", termo relacionado às ideias de "foro" e "justiça", se compreende a ciência aplicada pelas agências de segurança pública na solução de crimes.

Tanto conceitual quanto etimologicamente, as características negativas implicadas às técnicas antiforenses desestimulam sua utilização e esvaziam suas potencialidades: é como se qualquer obstáculo à obtenção de provas digitais por parte das agências de investigação constituísse uma ação ou omissão reprovável, ruim ou maléfica.

Essa ideia, todavia, não se coaduna com os pressupostos até então desenvolvidos neste artigo. Em uma noção aperfeiçoada pelo marco teórico do modelo constitucional de processo, as técnicas antiforenses podem contribuir, efetivamente, com a afirmação dos direitos de defesa das pessoas envolvidas em fatos penais diante do contexto da virada tecnológica.

Para tanto, propõe-se uma reformulação no conceito de técnicas antiforenses, no sentido de que sejam definidas como aquelas que garantem, às pessoas usuárias do ambiente digital, o exercício afirmativo do direito de se defenderem da produção de provas digitais em seu desfavor.

Essa definição incorpora, ao mesmo tempo, a ideia de oposição representada pelo prefixo "anti-" – aqui lido como a oposição da pessoa envolvida no fato penal à produção de provas em desfavor – e o objeto da expressão "forense" – notadamente as provas digitais.

O conceito aqui proposto também se adéqua à perspectiva de soberania digital (Floridi, 2020, p. 369), pensamento multidimensional (Belli, 2021) que se refere à capacidade dos sujeitos de exercerem – com autonomia estratégica – controle e poder sobre as infraestruturas digitais que acessa e seus dados.

São diversas as categorias de técnicas antiforenses e, a esse respeito, também inexiste consenso na literatura especializada.

Em pesquisa qualitativa a respeito das diferentes formas a partir das quais os autores e autoras que escreveram sobre o tema categorizaram as técnicas antiforenses, concluiu-se pela existência de três grandes categorias: a exclusão (ou destruição e eliminação), a alteração (ou ocultação, codificação, reorganização e substituição) e o anonimato (ou ofuscação, contracepção, codificação, codificação, criptografia e prevenção) de provas digitais (Gül; Kugu, 2017).

A exclusão seria a mais óbvia das técnicas antiforenses, caso os arquivos eletrônicos seguissem a mesma lógica dos não eletrônicos (Mason; Sheldon; Dries, 2017, p. 325). Bastaria, por exemplo, eliminar um documento impresso em papel para que as informações que ali constassem deixassem de existir em absoluto.

No contexto digital, porém, a eliminação definitiva de um arquivo caracteriza processo bem mais complexo. Apesar de aparentemente intuitivo, o ato de

selecionar um arquivo eletrônico e determinar seu apagamento não resulta, necessariamente, em sua exclusão definitiva (Bhat; Quadri, 2012, p. 18). Isso porque, ao excluir um arquivo ou movê-lo para o ícone "Lixeira", o documento apenas muda de lugar, mas continua a existir.

E, mesmo ao determinar a exclusão permanente (ou o esvaziamento da "Lixeira") dos arquivos, seus conteúdos permanecem intactos e apenas deixam de ocupar um espaço no sistema. Oportunamente, o sistema ocupará esse espaço vazio e os dados do arquivo excluído passarão a ser subscritos (ou substituídos) pelos dados de novos arquivos (Reardon; Basin; Capkun, 2013, p. 309).

Pensando nisso, diversos utilitários de limpeza efetiva e permanente foram desenvolvidos e estão disponíveis – inclusive, gratuitamente e com diferentes níveis de sofisticação e dificuldade – para usuários e usuárias de computadores. Essas ferramentas, no formato de *softwares*, funcionam a partir da gravação de padrões de combinação pseudoaleatórios de números 1 e 0 em todos os setores do disco rígido do computador.

Tais combinações, por seu turno, criam dados sem nenhum conteúdo ou significado, que substituem os dados dos arquivos excluídos, impedindo sua recuperação (Mason; Sheldon; Dries, 2017, p. 325).

Na prática, os *softwares* de limpeza nem sempre impedem a recuperação dos arquivos deletados, agindo, muitas vezes, somente no sentido de dificultá-la (Jain; Chhabra, 2014, p. 414).

Em teste operado com um dos mais populares aplicativos da categoria – o Eraser –, foi promovida a exclusão de dois arquivos idênticos de formas diferentes: uma, apenas encaminhando o documento para a "Lixeira" e, depois, deletando-o permanentemente; outra, com o uso do Eraser. Em seguida, um *software* profissional – o FTK Forensic – procedeu à tentativa de recuperação de dados – e constatou que a limpeza dos arquivos feita pelo Eraser foi muito mais eficiente quando comparada à mera exclusão do documento na "Lixeira". Todavia, até mesmo os arquivos apagados pelo Eraser tiveram alguns resíduos recuperados, ainda que com maior grau de dificuldade em relação ao outro método.

Pela possibilidade de recuperação da íntegra ou de parte dos arquivos excluídos, pode-se afirmar que a destruição mais eficiente e garantida de dados é aquela promovida por meio da eliminação física do disco rígido ou da unidade em estado sólido, quebrando-o ou queimando-o, ou por sua desmagnetização (Mason; Sheldon; Dries, 2017, p. 328).

Por outro lado, a alteração de provas digitais consiste na capacidade de transformar – ou "camuflar" (Wani, 2021, p. 99) – um arquivo, substituindo o original por uma nova versão. As muitas as possibilidades de alteração da prova digital se devem a uma de suas características mais particulares: são elementos de fácil manipulação

e adulteração, característica que impacta sua autenticidade e, consequentemente, sua confiabilidade (Brighi; Ferrazzano, 2021; Prado, 2024).

Exatamente por isso, as ferramentas antiforenses que mudam os dados e, em particular, os metadados cruciais de cada arquivo são bastante eficazes. Alguns exemplos são: Kali, *software* capaz de alterar a extensão dos arquivos; TimeStomp, que incide sobre os registros de data e hora de criação ou modificação do arquivo, copiando para ele os metadados de outro documento que está salvo no mesmo local; Rename Exper, que atribui aos arquivos títulos randômicos compostos por letras e números; Transliterator, que substitui a grafia original do título de um arquivo nomeado em algarismos romanos pelos correspondentes no alfabeto cirílico.

Existem outras formas de alteração relacionadas a arquivos eletrônicos, mas duas merecem destaque por serem muito adotadas nos últimos anos (Ferreira et al., 2020): a esteganografia e a criptografia.

A esteganografia consiste em uma prática utilizada há séculos para incrementar a segurança das comunicações, e que explora as limitações humanas, ocultando informações relevantes dentro de outros arquivos.

Seu emprego é promovido, geralmente, pela alteração nos valores dos *pixels*, que constituem o menor elemento de um arquivo de imagem ao qual se pode atribuir uma cor (Englander, 2014, p. 310) e são capazes de esconder informações imperceptíveis ao olhar humano.

Já a criptografia consiste em uma forma de ocultar informações a partir de sua alteração direta por códigos secretos (Bock, 2021, p. 16). Esses métodos estão cada vez mais complexos e acessíveis – inclusive, são integrados automaticamente na maioria dos sistemas operacionais, tais como Windows, Linux, Android e iOS (Wani, 2021, p. 99).

Por fim, o anonimato consiste em um esforço da pessoa usuária em relação aos seus próprios dados (Sarkis, 2024). Esse esforço antecede até mesmo a criação ou a disponibilização desses dados e é viabilizado por instrumentos como VPN e The Onion Routing (Tor), duas ferramentas que têm o mesmo modelo de comunicação por tunelamento e usam a tecnologia de criptografia para garantir a integridade dos dados.

Alguns dos principais *softwares* de VPN são o ExpressVPN, o CyberGhost e o TunnelBear. Todos funcionam a partir da criação de um túnel criptografado na rede pública (como a internet) que conecta o dispositivo às pessoas usuárias (como o computador ou o *smartphone*) a um servidor remoto operado pela empresa de VPN.

Como incremento da segurança da conexão, o Tor é uma tecnologia que opera no processo de roteamento por diversas camadas, nas quais os dados são criptografados em três etapas. Com isso, possibilita o isolamento de cada *website* visitado e

impede rastreamentos, apagando automaticamente todos os *cookies* e registros do histórico de navegação. Além disso, mascara o número IP de seus usuários e obsta sua identificação e localização.

Além da utilização de *softwares* de VPN, alguns esforços mais simples e que exigem menos capacitação técnica por parte da pessoa usuária podem contribuir para um acesso digital anônimo. Um exemplo seria a criação de contas de e-mail ou de perfis em redes sociais sem o nome completo ou outro dado de identificação de quem os acessará.

Medidas como esta têm o potencial de reduzir o campo de abrangência investigativa por meio do tratamento de dados abertos, "que podem ser encontrados livremente, à disposição do público (acesso público) e sem limites geográficos" (Camargo, 2022, p. 79) – método conhecido como OSINT ou Inteligência de Fontes Abertas.

Compreendidos os conceitos e as categorias das práticas antiforenses, bem como conhecidos seus empregos e suas potencialidades, passa-se à discussão central do presente artigo: afinal, essas práticas caracterizam atos de obstrução de justiça e, portanto, são criminosas, ou trata-se apenas de técnicas que possibilitam o exercício dos direitos de defesa?

4. Seriam as técnicas antiforenses uma forma de obstrução da justiça?

O crime de obstrução de justiça[7] foi tipificado no Brasil em decorrência direta da ratificação da Convenção de Palermo das Nações Unidas contra o Crime Organizado Transnacional.

Mencionado diploma prevê o compromisso de cada Estado-parte em adotar medidas legislativas hábeis a conferir o caráter de infração penal às condutas de obstrução praticadas no âmbito de organizações criminosas transnacionais e é fruto da tendência de sujeição do Direito interno às diretrizes internacionais.

No Brasil, a criminalização da obstrução de justiça ocorreu à margem da estruturação, da conceituação e da tipificação do crime de organização criminosa. O Projeto de Lei do Senado que deu origem à Lei 12.850/2013 pouco tratou da obstrução ou de suas características específicas, cabendo à ciência jurídico-penal definir seus contornos.

O primeiro dos contornos necessários trata do objeto de proteção da norma penal incriminadora. É preciso, nesse aspecto, diferenciar a obstrução de justiça

7. A Lei nº 12.850/2013, em seu artigo 2º, § 1º, comina penas de três a oito anos de reclusão e multa a quem impede ou, de qualquer forma, embaraça a investigação de crime que envolva organização criminosa (Brasil, 2013).

dos tipos penais que tutelam a Administração da Justiça, a exemplo do crime de fraude processual[8].

Os delitos contra a Administração da Justiça se dividem em duas espécies: aqueles que atentam contra os meios de que o Estado dispõe para desenvolver a persecução; e aqueles que comprometem, diretamente, os resultados que o Estado visa a alcançar com a aplicação da lei e a realização da justiça (Feldens; Teixeira, 2020, p. 28).

A tipificação da obstrução de justiça busca proteger a persecução penal, sendo classificada como instrumento à disposição da Administração da Justiça. As ações que não atentam, imediatamente, contra os mecanismos persecutórios não violam o objeto de proteção do crime de obstrução, já que não realizam o conteúdo material do injusto, como a utilização de outros meios para manter oculta a prática de crime.

Sendo assim, o objeto material sobre o qual recai a ação delituosa será a investigação de infração penal envolvendo organização criminosa, em razão da leitura limitada do tipo, que não se estende à fase judicial do processo penal.

Já o segundo contorno necessário guarda relação com a consumação e o resultado do delito. Consuma-se a obstrução de justiça quando efetivo o impedimento ou a continuidade do curso da investigação criminal. A lei não faz referência a quaisquer atos com potencial para impedir ou embaraçar a investigação, limitando-se a punir o resultado dessas ações.

Na modalidade "impedir investigação penal que apura organização criminosa", imperiosa a ocorrência do resultado de impedir o andamento das investigações, ou seja, pressupõe-se que o impedimento de fato se concretize e que dele resulte a impossibilidade do desenvolvimento da investigação.

Por outro lado, na modalidade "embaraçar investigação penal que apura organização criminosa", exige-se apenas a demonstração de dificuldades concretas à investigação regular. É preciso que o embaraço gere transtornos e demande medidas supletivas e conservativas por parte das Autoridades, sob pena de se punir meras intenções que sequer podem ser comprovadas (Bitencourt; Busato, 2013, p. 93).

O tipo penal da obstrução de justiça, nesse sentido, merece críticas. Cezar Bitencourt e Paulo Busato (2014, p. 85) definem a norma incriminadora como excessivamente aberta, vaga e imprecisa. Essa circunstância, na perspectiva da pessoa envolvida em fatos penais, é eivada de insegurança jurídica, afinal, desconhece-se o limite entre o que pode ou não ser feito para exercer o direito de defesa.

8. O Código Penal, em seu art. 347, comina penas entre três meses e um ano de detenção, além de multa, a quem inovar artificiosamente, na pendência de processo civil ou administrativo, o estado de lugar, de coisa ou de pessoa, com o fim de induzir a erro o juiz ou o perito.

Na disciplina do Direito Penal, inexiste consenso nas discussões acerca de eventuais limites aos direitos de defesa e suas consequências – em regra, conectadas ao estudo dos tipos penais que criminalizam condutas comissivas ou omissivas praticadas pela pessoa envolvida no fato penal com a finalidade defender-se contra a incriminação.

De acordo com Ivan Zonta (2023), os posicionamentos sobre o tema se dividem: alguns autores se posicionam a favor da imputação do crime à pessoa envolvida no fato penal; outros, contra essa possibilidade em decorrência do direito de defesa; ainda, há um terceiro grupo que defende uma posição intermediária, admitindo a imputação em alguns casos.

Como representantes da primeira corrente, Cezar Roberto Bitencourt e Paulo Busato (2014, p. 83) defendem que a pessoa envolvida em fatos penais e que integra organização criminosa tem o direito de se defender, inclusive por meio da criação de transtornos ou dificuldades às investigações que constituiriam um *post factum* impunível.

Por outro lado, Luiz Flávio Gomes (2012) é um dos penalistas que defendem a abrangência do direito de defesa para qualquer conduta de inatividade ou omissão. Para o autor, fundamentalmente, trata-se do direito de não falar, de não falar a verdade, de não confessar, de não apresentar provas contra si e de não participar da produção de provas em seu desfavor.

No aspecto penal material, Gomes (2012, p. 611) entende que a única conduta comissiva a ser praticada pela pessoa imputada, sem gerar repercussões contrárias ao seu interesse, seria a de mentir, ou seja, declarar algo inverídico. Tal conduta não é criminalizada pelo ordenamento jurídico brasileiro e, diante disso, sua prática – apesar de não caracterizar um direito – não gera responsabilização penal[9].

Diferente disso seria a situação em que a pessoa abandona o campo da inatividade e passa a agir, comissivamente, com o intuito de obstar a produção da prova: por exemplo, quem oculta o cadáver de uma vítima de homicídio ou dissimula a origem de valores que são provenientes de infração penal.

Para o autor, considerando o fato de que tais condutas reverberam sobre o direito de terceiros, não poderiam ser reconhecidas como exercício da não

9. No mesmo sentido, veja-se: "Como forma de se efetivar o direito público e subjetivo contra a autoincriminação involuntária, afigura-se tolerável, inclusive, a mentira irrogada pelo indivíduo sobre quem recai a pretensão punitiva estatal. Essa conclusão é extraída pela inexistência de tipificação do crime de perjúrio no Direito Penal brasileiro, bem como pelo fato de tal conduta – apesar de imoral (ou até mesmo, eventualmente, injusta e passível de reparação civil) – poder se configurar, em tese e *a priori*, uma dirimente já que tratar-se-ia de inexigibilidade de conduta diversa, podendo até mesmo ser classificada como estado de necessidade exculpante" (Torres; Lopes, 2021, p. 260).

autoincriminação e devem constituir crimes autônomos (como, de fato, o são a ocultação de cadáver[10], a lavagem de dinheiro[11] e, no caso da aplicação das técnicas antiforenses, a invasão de dispositivo informático[12]).

Assim como Gomes (2012), para quem o limite ao direito de defesa seria a prática de condutas comissivas que recaem sobre direitos de terceiros, Luciano Feldens e Adriano Teixeira (2020, p. 15) pontuam que as ações defensivas, alinhadas a uma postura reativa, não requerem a adoção de comportamentos colaborativos, ainda que a resistência de cooperação gere prejuízos à investigação, ao processamento e ao julgamento de crimes.

Por outro lado, as condutas que ferem a administração da justiça – seja em relação aos seus meios, seja em relação aos seus resultados – deveriam ser objeto de tutela penal.

Estariam, portanto, fora do âmbito de proteção dos direitos de defesa; segundo Feldens (2021, p. 41), qualquer utilização antifuncional do Direito, que instrumentalizasse de maneira capciosa as formas jurídicas com a intenção de prejudicar o funcionamento do Estado, no exercício de suas atividades.

Assim, enquanto os comportamentos da pessoa alicerçados em posições jurídico-fundamentais não estão sujeitos à ilegalidade, não se encontraria no Direito legitimidade para a ação de quem se vale de meios tipicamente ilícitos e desencontrados de sua função constitucional (Feldens, 2021, p. 43-45).

Para Fernanda Tórtima (2021, p. 187), seria possível considerar o afastamento da tipicidade de obstrução sobre condutas comissivas ou omissivas praticadas pela pessoa envolvida nos fatos penais, desde que atendidos dois requisitos: a plena disponibilidade sobre os objetos materiais da obstrução e a não afetação do direito de terceiros.

Essa parece ser a mais ponderada das alternativas: admite que a pessoa envolvida em fatos penais exerça seu direito de defesa, desde que o faça sobre objetos que estejam no seu campo de disponibilidade e que não afetem interesses de outras pessoas.

10. O Código Penal, em seu art. 211, comina penas entre um e três anos de reclusão e multa a quem destruir, subtrair ou ocultar cadáver ou parte dele.
11. A Lei 9.613/1998, em seu art. 1º, comina penas de três a dez anos de reclusão e multa a quem ocultar ou dissimular a natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos ou valores provenientes, direta ou indiretamente, de infração penal.
12. O Código Penal, em seu art. 154-A, comina penas entre um e quatro anos de reclusão e multa a quem invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita.

Nas hipóteses em que o direito de defesa fosse exercido por ferramentas antiforenses, seria atípica a imputação da obstrução de justiça quando o dispositivo ou os arquivos a serem excluídos, alterados ou tornados anônimos estivessem ao seu dispor – isto é, não fossem obtidos de forma ilícita, como por meio da invasão a dispositivo informático, por exemplo – e fossem de sua propriedade ou titularidade – ou seja, não pertencessem a terceiros que pudessem ser prejudicados por sua exclusão, alteração ou anonimato.

Atendidos, portanto, os critérios da disponibilidade dos objetos e de sua propriedade, prevaleceria o direito de defesa sobre a incriminação da obstrução de justiça. Resta discutir, todavia, se as práticas antiforenses constituem formas legítimas de se exercer as garantias de defesa, seja no plano ético, seja no plano do Direito Processual Penal.

5. Seriam as técnicas antiforenses uma garantia da defesa?

A cada desenvolvimento tecnológico, uma nova plataforma de investigação penal é estabelecida,[13] e nem sempre existirá uma tutela adequada de garantias defensivas em contrapartida.

Exatamente por isso, surge a necessidade de se ampliar o rol de direitos fundamentais disponíveis às pessoas envolvidas nos fatos penais, na mesma proporção em que se estendem, em seu desfavor, as atividades de investigação tecnológicas.

Vistas como garantias capazes contribuir para o exercício da garantia de defesa, as práticas antiforenses asseguram às pessoas usuárias do ambiente digital – por meio da exclusão, da alteração e do anonimato de elementos digitais – a possibilidade de, em paridade com as agências públicas de segurança, contar com os avanços tecnológicos para a promoção de seus interesses.

Como métodos que garantem às pessoas o direito de defesa contra a obtenção de provas digitais em seu desfavor, a exclusão revela-se prática que, apesar de aparentemente simples, é de difícil emprego eficaz.

Com o desenvolvimento das tecnologias forenses, as agências de segurança pública possuem meios de recuperar grande parte dos dados apagados de dispositivos eletrônicos e, por esse motivo, somente a destruição total do disco rígido dos dispositivos poderia garantir que os dados ali constituídos seriam irresgatáveis.

A alteração, por seu turno, se mostrou uma técnica com diversas possibilidades, algumas mais e outras menos seguras, sendo a criptografia – método aderido pelos próprios sistemas operacionais – a mais popular delas.

13. "Trata-se da confirmação da Lei de Zimmermann, onde 'o fluxo natural de tecnologia tende a se deslocar na direção de tornar mais fácil a vigilância, e a capacidade dos computadores de nos rastrearem dobra a cada dezoito meses'" (Mendes, 2024, p. 89).

Já o anonimato se apresenta como método muito útil ao ingresso à internet, de modo a impedir – ou pelo menos dificultar – a identificação da pessoa usuária e de sua localização.

Com relação às críticas direcionadas às práticas antiforenses, verificam-se dois principais argumentos: um de ordem filosófica, que faz alusão à ilegitimidade das práticas antiforenses a partir de uma perspectiva ética. Questiona-se, nesse sentido, se seria ético – ou "correto", ou "justo" – permitir o uso de estratégias que impedem ou dificultam o acesso das autoridades a provas com potencial incriminador e, com isso, prejudicam o direito coletivo à segurança pública.

Por outro lado, em uma perspectiva processual penal, o segundo argumento está conectado à cadeia de custódia das provas, entre elas, as digitais. O ponto de reflexão, nesse contexto, está atrelado aos efeitos que a utilização dos métodos antiforenses gera sobre a autenticidade da prova digital, a ponto de comprometer sua admissibilidade.

Pela ótica filosófica, verifica-se uma tentativa, por parte de quem pesquisa as técnicas antiforenses, de transpor sistemas éticos tradicionais (principalmente a ética eudaimonista das virtudes) para o campo da tecnologia.

A ética das virtudes remonta à Grécia Antiga e tem como principal expoente Aristóteles e sua *Ética a Nicômaco*. No pensamento aristotélico, as virtudes intelectuais (compreendidas como a correição dos meios) e morais (compreendidas como a correição dos fins) são indispensáveis para que as pessoas sejam boas e, com isso, vivam bem.

Seria, portanto, a partir de bons hábitos que o caráter virtuoso se constituiria, tornando-se condição imprescindível para atingir a eudaimonia, tendo em vista que "a virtude e o homem bom como tais são a medida de todas as coisas" (Aristóteles, 1991).

Nessa perspectiva filosófica, que supõe uma instância humana intelectivo-moral irredutível (Brochado, 2023, p. 404), ideias como ação e correição estão intrinsecamente conectadas aos conceitos de virtudes e bondades. Uma ação seria correta, portanto, se estivesse em conformidade com aquilo que se espera de uma pessoa virtuosa naquelas circunstâncias; a bondade do caráter seria precedente à correção moral (Hobuss, 2011, p. 15).

Entre as virtudes da alma identificadas por Aristóteles, uma tem importante relevo para o presente estudo: a justiça. Na perspectiva da ética das virtudes, a justiça é boa tanto para quem é justo quanto para quem vive na comunidade da qual a pessoa justa faz parte.

Partindo dessa premissa ético-aristotélica e considerando a justiça como virtude de impactos pessoal e social, atrelada à bondade e à felicidade, é que se questiona: haveria, então, um dilema entre a virtude da justiça e o direito de empregar

meios antiforenses para garantir seu direito de defesa? Seria eticamente inadequada a proposta de assegurar a garantia de defesa com o auxílio das técnicas antiforenses? O exercício de práticas antiforenses por parte da pessoa que quer exercer sua garantia de defesa caracteriza uma prática injusta e, por isso, pouco virtuosa?

As respostas para essas perguntas devem ser negativas, diante da impossibilidade do dilema proposto.

Em um âmbito geral, é impossível se separar, analiticamente, aquilo que é "bom" ou "mau", no que concerne ao direito (Adeodato, 2023, p. 107). A afirmação pode parecer demasiadamente incisiva, mas precisa ser considerada, porque, ainda que as pretensas "certezas éticas" sobre aquilo que é "bom" ou "mau" sejam instintivas, porquanto condições antropológicas humanas, não estão apoiadas em dados empíricos e, por isso, dão margem a uma constante luta pelas "verdades" defendidas por cada um (Adeodato, 2023, p. 108).

No âmbito das técnicas antiforenses, a impropriedade desse pretenso dilema se fundamenta em duas circunstâncias empíricas bastante robustas: a primeira se justifica na medida em que não existem parâmetros ou diretrizes éticas para as práticas forenses digitais por parte das agências de segurança pública – e, diante dessa ausência, qualquer problematização semelhante em face das práticas antiforenses é incoerente.

A segunda circunstância é a impropriedade da utilização de fórmulas éticas para a supressão de direitos fundamentais consagrados pelo Estado de Direito e que compõem a base principiológica uníssona do modelo constitucional de processo.

A falsidade do dilema entre o "bom" e o "mau" em matéria de tecnologia é objeto de críticas, em especial nas pesquisas relacionadas à Inteligência Artificial (IA).

Existe uma teia de mitos, que ora trata a IA como uma panaceia definitiva, capaz de resolver e superar todos os problemas da humanidade; ora a considera uma catástrofe absoluta, que destruiria milhões de empregos e dominaria os seres humanos como animais de estimação (Floridi, 2016). A IA, nesse conflito, vive períodos que, metaforicamente, comparam-se a verões – com promessas e expectativas quentes e passageiras – e invernos – quando a realidade passa a mostrar aquilo que, de fato, a IA é ou não capaz de fazer (Floridi, 2020).

Quando o assunto são as técnicas forenses e antiforenses, o maniqueísmo constatado no campo da IA também se aplica. Valendo-se da metáfora com as estações do ano, as estratégias forenses encontram-se em permanente estado de verão, enquanto as antiforenses representam um longo e tortuoso inverno.

Além disso, apesar de toda a literatura antiforense se manifestar – ainda que brevemente – sobre os supostos conflitos éticos ocasionados por sua utilização, são

poucos os trabalhos científicos que questionam a falta de diretrizes éticas para as atividades forenses no ambiente digital, rotineiramente vistas como práticas novas e em constante melhoria.

Ocorre que as perícias digitais não são, exatamente, uma novidade: estão em atividade há mais de trinta anos, desde a criação da primeira empresa de computação forense – a AccessData[14] – no final da década de 1980 (Ferguson et al., 2020).

Ainda nos anos 1990, a Associação dos Chefes de Polícia do Reino Unido (Association of Chief Police Officers – ACPO) produziu o primeiro guia de boas práticas para a utilização de provas digitais e segurança da informação[15].

Em 2005, o Comitê Técnico ISO/IEC (parceria entre a International Organization for Standardization e a International Electrotechnical Commission) reuniu-se para aprovar técnicas de segurança da informação e para a gestão da segurança informática, as quais foram incorporadas no Brasil pela Associação Brasileira de Normas Técnicas (ABNT) na norma brasileira (NBR) 27002.

Veja-se que o fato de as tecnologias forenses estarem em crescimento exponencial – assim como ocorre com a IA[16] – apenas corrobora a necessidade de diretrizes éticas. O fato de as agências de segurança pública investirem cada vez mais em tecnologias de obtenção de provas digitais deveria suscitar um incremento ético, nos mesmos ritmo e rigor (Ferguson et al., 2020).

Contudo, quando comparados os princípios éticos que deveriam guiar as práticas forenses com as práticas de fato promovidas pelas agências de segurança pública, é possível perceber que essa não é a realidade:

14. A partir de 2008, a AccessData passou a ser Exterro, empresa desenvolvedora do *software* FTK, mencionado anteriormente.

15. A última versão do documento, atualizada em 2012, está disponível em: [https://bit.ly/3JvF7JP]. Acesso em: 23.03.2025.

16. Ao descrever o crescimento exponencial da IA, Francesca Rossi (2019, tradução nossa) consigna: "Na vida cotidiana, não estamos acostumados com o crescimento exponencial, mas com o crescimento linear: se cada um de nossos passos tiver um metro de comprimento, depois de darmos cem passos, teremos nos movido cem metros (supondo que estejamos indo em linha reta). Em uma caminhada exponencial, por outro lado, cada passo tem o dobro do comprimento do anterior (portanto, um metro para o primeiro passo, dois metros para o segundo, quatro metros para o terceiro, oito metros para o quarto e assim por diante). [...] Portanto, para resumir, graças às técnicas de aprendizado de máquina, a IA é capaz de resolver com grande precisão até mesmo problemas para os quais a "receita" é desconhecida. Problemas tão complexos ou vagos que não é possível definir as etapas exatas para chegar a uma solução em todos os casos possíveis".

Quadro 1 – Mapeamento comparativo entre princípios éticos e diretrizes investigativas

PRINCÍPIOS ÉTICOS	ALINHADO ✓ OPOSTO ×	DIRETRIZES INVESTIGATIVAS
Delinear o escopo da investigação	×	Investigar exaustivamente
Respeitar a privacidade das pessoas investigadas	×	Registrar todas as informações de forma abrangente
Ampliar o rol de investigados apenas se houver evidências do envolvimento de outras pessoas	×	Investigar todas as pessoas que possam ser relevantes
Marcar e excluir informações privadas	×	Marcar materiais sensíveis e mantê-los registrados
Documenta todas as ações	✓	Registrar todas as informações intangíveis
Facilitar auditorias	✓	Fornecer os registros das informações coletadas
Reportar todas as informações investigativas	✓	Registrar todos os passos da investigação
Ser transparente sobre a extensão das investigações e informações coletadas	✓	Permitir à defesa o acesso e inspeção das informações
Submeter investigadores e investigadoras a treinamentos regulares	✓	Garantir que investigadores e investigadoras sejam preparados para atuar
Manter a integridade e a confidencialidade das evidências coletadas	✓	Manter a integridade das informações
Considerar o bem-estar de investigadores e investigadoras	-	Não há diretriz correspondente.

Fonte: traduzido livremente a partir de Ferguson et al. (2020, p. 275).

O comparativo acima serve como indicativo do motivo de não serem os princípios éticos imediatamente incorporados nas práticas forenses por parte das agências de segurança pública: um "código de ética" para as perícias digitais limitaria, sobremaneira, suas práticas e sua abrangência.

Por conseguinte, restringiria os poderes e atividades do Estado, que depende da coleta e do processamento de informações para sua sobrevivência (Bolzan de Morais, 2018, p. 887). Considerando, então, que os parâmetros éticos limitariam a abrangência das agências de segurança pública, seu estabelecimento constituiria verdadeiro obstáculo indesejado.

Os debates sobre técnicas antiforenses, portanto, não podem se limitar às definições de "bom" ou "mau", "certo" ou "errado", "justo" ou "injusto". Essas dicotomias éticas, na vigência de uma processualidade democrática, acabam por tirar o foco do que realmente importa – sua utilização em garantia do direito de defesa.

Todo o conteúdo ético que recai, impropriamente, sobre as técnicas antiforenses acaba por ofuscar um grande mérito: a capacidade de potencializar a fiabilidade das provas digitais. Isso porque, a partir do momento em que as evidências eletrônicas ficam sujeitas aos fenômenos da exclusão, alteração ou anonimato, aumentam os desafios para sua obtenção de forma autêntica e íntegra (Mason; Sheldon; Dries, 2017, p. 325).

A fiabilidade probatória "refere-se ao esquema de ingresso do elemento probatório no procedimento em cujo âmbito, posteriormente, este elemento poderá ser objeto de avaliação" (Prado, 2019, p. 88). Para assegurá-la, é necessário um dispositivo – a cadeia de custódia – que o coloque "sob proteção de interferências capazes de falsificar o resultado da atividade probatória" (Prado, 2014, p. 86).

Como premissas da fiabilidade do elemento probatório, a autenticidade seria o princípio a partir do qual se determina que "o mesmo [elemento probatório] que se encontrou na cena do crime [seja] o mesmo que se está utilizando para tomar a decisão judicial" (Prado, 2019, p. 95); já a integridade constitui a garantia de que os elementos probatórios submetidos à apreciação judicial estão resguardados em sua completude (Domingos, 2019, p. 197) e preservados contra quaisquer alterações, correspondendo – exatamente – à maneira como foram coletados (Lopes Jr.; Rosa, 2015).

A formação e a preservação dos elementos probatórios, assim, devem ser cercadas de cautelas, ou seja, "trata-se de perseguir a melhor qualidade da decisão judicial e reduzir ao máximo os riscos de incriminação imprópria" (Prado, 2019, p. 95), com a finalidade de assegurar que a prova não foi adulterada, não sofreu diminuição ou alteração de suas características (Badaró, 2017, p. 525).

Efetivamente, a confiabilidade do elemento probatório pressupõe sua autenticidade e sua integridade, e deve ser regrada, formalizada, documentada e validada (Sombrio, 2021, p. 216) pela cadeia de custódia. Para o Direito Processual Penal brasileiro, o procedimento adotado para a cadeia de custódia – disposto nos artigos 158-A e seguintes do Código de Processo Penal – envolve a manutenção e a

documentação da história cronológica do vestígio, permitindo o rastreamento de sua posse e manuseio, desde o reconhecimento até o descarte.

Quando o elemento probatório é digital, contudo, algumas de suas características singulares (Taruffo, 2014, p. 83) afetam sua autenticidade e sua integridade, motivo pelo qual demandam maior rigor que o normalmente associado às evidências em formato físico.

Ao analisar uma prova material física – como um documento em papel, por exemplo –, circunstâncias como as propriedades químicas da tinta utilizada na escrita podem determinar se mais de um utensílio foi adotado (como duas ou mais canetas) e a época em que o documento foi produzido (Schafer; Mason, 2017, p. 21)

Quando a prova está em ambiente eletrônico, contudo, conceitos como "original" e "cópia" não se sustentam. No meio digital, o próprio ato de trabalhar em um documento cria, automaticamente, inúmeras cópias desse documento, que podem se manter salvas e registrar versões anteriores mesmo quando o documento estiver concluído (Schafer; Mason, 2017, p. 22).

Se os dados digitais são, intrinsecamente, maleáveis e mutáveis, assim também serão as evidências deles originadas. Essa característica expõe toda a sua fragilidade e explica o motivo pelo qual os documentos eletrônicos merecem um tratamento diferenciado em relação aos físicos (Teppler, 2014, p. 217).

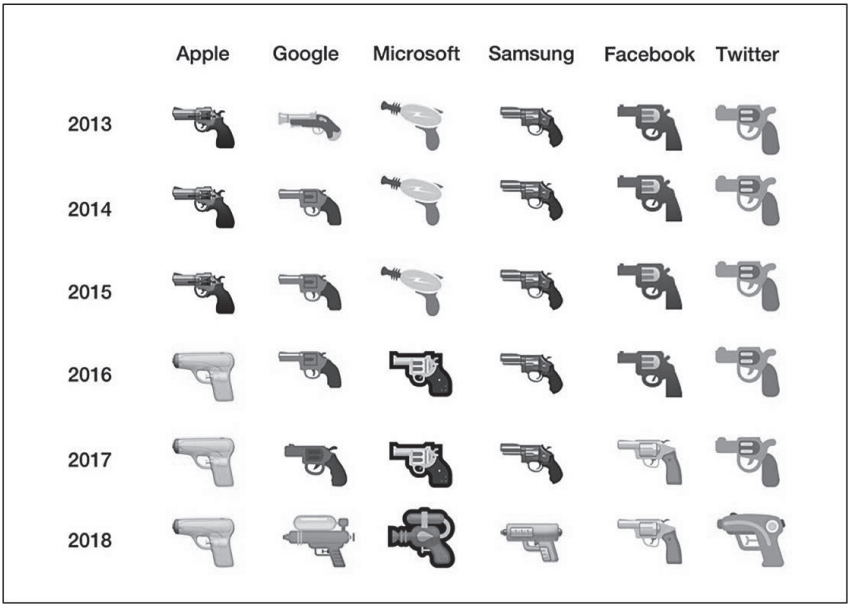
Devem os documentos digitais ser compreendidos como um processo pelo qual partes de dados ininteligíveis são distribuídas, armazenadas, processadas e tornadas legíveis para uma pessoa humana (Schafer; Mason, 2017, p. 22-23). No ambiente digital, o documento não ocupa lugar algum – na verdade, nem sequer existe sem uma aplicação (*software*) que o recria com o dispositivo (*hardware*) sempre que a pessoa usuária do dispositivo o inicia.

Além disso, no meio eletrônico, um mesmo documento pode se mostrar de formas diferentes pois a ele não se aplica um conceito de representação única e definitiva. Os autores exemplificam essa afirmação a partir dos *emojis*, que são ideogramas usados em mensagens eletrônicas semelhantes aos *emoticons*.

Em 2016, a Apple alterou a forma do *emoji* que representava uma arma na mão de alguém para um *emoji* cuja imagem é de uma pistola de água.

Porém, até o ano de 2018, quando uma mensagem que continha esse *emoji* fosse enviada para um dispositivo que não fosse da Apple, a imagem recebida pelo usuário não seria a divertida pistola de água, mas uma ameaçadora arma de fogo – fator capaz de alterar todo o contexto de mensagens como "traga sua << *emoji* de arma >> para a nossa reunião" ou "retire o que disse, senão verá a minha << *emoji* de arma >>". A Figura 1 ilustra essa diferença:

Figura 1 – Progressão temporal dos *emojis* de arma em diferentes dispositivos



Fonte: Burge (2018).

Com base nas características das provas digitais, pode-se elencar, entre os fatores que dificultam sua autenticidade e integridade, as possibilidades de exclusão, alteração ou anonimato das evidências (Mason; Stanfield, 2017, p. 196-197).

Essas situações podem ter relação com o emprego de técnicas antiforenses: imagine-se, por exemplo, um caso no qual existiam suspeitas plausíveis de que provas digitais (*e-mails* apreendidos) possam ter tido seus registros de data e hora de envio modificados, sendo essa informação imperiosa para o deslinde do processo.

Em contextos como esse, as análises periciais demandam maiores dedicação e qualidade, motivo pelo qual, em última instância, acabam por produzir resultados ainda mais confiáveis.

No mesmo ponto, os desafios resultantes do emprego de técnicas antiforenses geram reflexões cuidadosas sobre a natureza da prova eletrônica e incentivam o constante aperfeiçoamento da cadeia de custódia e das práticas periciais (Mason; Sheldon; Dries, 2017, p. 338). Agem, nesse aspecto, para "neutralizar a possível suspeita da alteração do dado, reduzir o risco da perda da originalidade do dado e com isso garantir confiabilidade e integridade" (Mendes, 2020, p. 150).

Um exemplo prático de potencialização da cadeia de custódia que evita a incidência de métodos antiforenses sobre provas digitais pode ser visualizado na fase de apreensão. A fim de que a fiabilidade dos elementos apreendidos seja preservada,

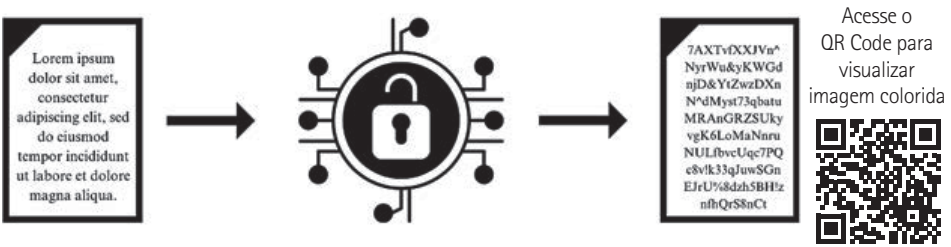
é necessária a cópia (ou espelhamento) integral (*bit to bit*) do conteúdo do dispositivo a ser periciado (Paiva, 2022, p. 133).

Deve-se, ainda, efetuar a extração do código de verificação *hash*, algoritmo matemático que mapeia todos os dados, que se alteram com qualquer intervenção, ainda que mínima, promovida sobre o arquivo original (Badaró, 2021, p. 08).

A Figura a seguir demonstra, de forma simplificada, como atua a função *hash*. Na primeira imagem, o arquivo está em seu formato original (no caso, um texto). Na segunda, é submetido ao algoritmo *hash*. Por fim, após passar pela função *hash*, o arquivo é criptografado.

Qualquer alteração no texto (primeira imagem) implicaria, imediatamente, a mudança do arquivo criptografado (terceira imagem).

Figura 2 – Função *hash*



Fonte: elaborado pelas autoras.

Tanto a necessidade de cópia integral das provas digitais, quanto da inclusão de algoritmo *hash*, são recomendações da ABNT, na NBR ISO/IEC 27037:2013, que contribuem para a sua confiabilidade, na medida em que asseguram a autenticidade e a integridade dos elementos probatórios.

Referido procedimento é suficiente para garantir que a prova digital não será adulterada no momento da perícia – já que a análise será feita sobre os elementos copiados, e não sobre os originais –, para assegurar que os elementos originais não serão modificados e para possibilitar que tais provas originais permaneçam disponíveis para novas perícias (Lopes, 2025, p. 180).

Esse incremento qualitativo precisa ser percebido em toda a sua relevância, que é proporcional ao protagonismo das provas científicas – entre elas, as perícias digitais – no contexto probatório. Afinal, as provas técnicas tendem à sobrevalorização epistêmica, isto é, a ser valoradas pelo que declaram, e não pelo que, de fato, comprovam (Prado, 2019, p. 88-89).

O controle de qualidade da prova, naquilo que toca aos seus parâmetros de obtenção, produção e manutenção, seria fundamental para garantir respaldo epistemológico à decisão judicial que lhe tenha como base. Trata-se, em síntese, do "exercício de uma 'prova sobre a prova', isto é, na comprovação (demonstração) da

correção do procedimento de obtenção e preservação dos elementos probatórios" (Prado, 2019, p. 90).

Na mesma medida, a cadeia de custódia – incrementada em decorrência das possibilidades de exclusão, alteração e anonimato antiforenses – é fundamental para a efetivação do modelo constitucional de processo. Em seu aspecto de expansividade, o modelo constitucional de processo se realiza pelo tratamento expresso da irregularidade probatória, disposto no artigo 5º, LVI, da CF/1988, e que norteia todo o direito probatório brasileiro, inclusive naquilo que se refere à cadeia de custódia (Lopes, 2025, p. 177).

Por isso, em relação à cadeia de custódia, as técnicas antiforenses não apresentam nada além de benefícios. Robustecem o controle processual sobre a prova – reflexo da orientação constitucional – e permitem a fiscalização sobre sua qualidade, fator que deve ser de interesse, inclusive, das agências de segurança pública.

6. Considerações finais

A cada desenvolvimento tecnológico, uma nova plataforma de investigação oculta será estabelecida, e nem sempre existirá uma tutela adequada de direitos individuais em contrapartida.

Exatamente por isso, surge a necessidade de se ampliar o rol de direitos fundamentais disponíveis às pessoas envolvidas nos fatos penais, na mesma proporção em que se estendem, em seu desfavor, as práticas processuais.

Para tanto, considerando a necessidade do próprio Direito Processual Penal de se adaptar à processualidade democrática, o modelo constitucional de processo se mostra uma metodologia capaz de proporcionar a adoção de uma base principiológica uníssona, cuja dinâmica prevê a expansão, a especialização e o aperfeiçoamento do ordenamento jurídico diante da adesão aos direitos fundamentais.

A partir do modelo constitucional de processo penal, é possível ultrapassar a sujeição do indivíduo ao Estado, posicionando o indivíduo e o órgão de acusação em paridade. Essa paridade, no aspecto das garantias de defesa, tem o potencial de tutelar os direitos individuais, ressalvada a vedação às práticas que constituem ilícitos penais quando violadoras do direito de terceiros.

Por tudo isso, o direito de defesa deve alcançar sua plenitude para que se adéque à processualidade democrática no contexto da virada tecnológica. É preciso garantir à pessoa envolvida em fatos penais o direito de se proteger das diversas formas desenvolvidas pelo Estado – inclusive por métodos ocultos de investigação empregados na Era Digital – para obter sua inculpação.

As técnicas antiforenses, nesse sentido, têm o potencial de contribuir para o exercício da defesa. Por meio da exclusão, da alteração e do anonimato de elementos

digitais, a pessoa pode, em paridade com as agências públicas de segurança, contar com os avanços tecnológicos para a promoção de seus interesses.

Obviamente, por se tratar de ferramentas que dificultam ou impossibilitam a atividade investigativa pelo Estado, as técnicas antiforenses são alvo de críticas. Entretanto, quando submetidas ao filtro do modelo constitucional de Processo Penal, constata-se que nenhum dos questionamentos se sustenta.

No aspecto ético-filosófico, a legitimidade das práticas antiforenses nem sequer pode ser contestada, porque inexiste igual medida voltada à atuação forense exercida pelos órgãos do Estado.

Assim também ocorre em relação ao aspecto probatório processual, porquanto as técnicas antiforenses consistem em mecanismo de reforço à cadeia de custódia, capazes de incrementar significativamente a qualidade da prova em seus aspectos de integralidade, autenticidade e confiabilidade – circunstância esta que deve (ou deveria) interessar a todos impactados pela dinâmica probatória.

Com base nas discussões estabelecidas, conclui-se que a criminalização das técnicas antiforenses como atos de obstrução de justiça, sem considerar seu papel na consagração do direito de defesa, resulta em insegurança jurídica e fragiliza os direitos fundamentais.

Portanto, é imprescindível que o sistema jurídico amplie e adapte as garantias de defesa para acompanhar as inovações tecnológicas, assegurando que as práticas antiforenses não sejam tratadas como obstruções à justiça, mas como instrumentos legítimos de exercício das garantias defensivas.

Referências

ADEODATO, João Maurício. *Introdução ao estudo do direito*: retórica realista, argumentação e erística. Rio de Janeiro: Forense, 2023.

ALBANO, Pietro; CASTIGLIONE, Aniello; CATTANEO; Giuseppe; DE SANTTIS, Alfredo. A novel anti-forensics technique for the android OS. *International Conference on Broadband and Wireless Computing, Communication and Applications – IEEE*, Barcelona, 2011. *Proceedings* [...] Barcelona: [s.n.], Oct. 2011.

ANDOLINA, Italo; VIGNERA, Giuseppe. *Il modelo constituzionale del processo civile italiano*: corso di lezioni. Torino: G. Giappichelli Editore, 1990.

ARISTÓTELES. *Ética a Nicômaco*. 4. ed. São Paulo: Nova Cultural, 1991.

BADARÓ, Gustavo Henrique Righi Ivahy. A cadeia de custódia e sua relevância para a prova penal. In*:* SIDI, Ricardo; LOPES, Anderson Bezerra (Orgs.). *Temas atuais da investigação preliminar no processo penal*. Belo Horizonte: D'Plácido, 2017.

BARROS, Flaviane de Magalhães. O modelo constitucional de processo e o processo penal: a necessidade de uma interpretação das reformas do processo penal a partir da Constituição. In: MACHADO, Felipe Daniel Amorim; CATTONI DE OLIVEIRA, Marcelo Andrade (Coords.). *Constituição e processo*: a contribuição do processo ao constitucionalismo democrático brasileiro. Belo Horizonte: Del Rey, 2009.

BELLI, Lucas. CyberBRICS: A Multidimensional Approach to Cybersecurity for the BRICS. In*:* BELLI, Lucas (Ed.). *CyberBRICS*: Cybersecurity Regulations in the BRICS Countries. Cham: Springer International Publishing, 2021.

BHAT, Wasim Ahmad; QUADRI, Syed Mohammad Khurshaid. After-deletion data recovery: myths and solutions. *Computer Fraud & Security*, n. 4, p. 17-20, apr. 2012.

BITENCOURT, Cezar Roberto; BUSATO, Paulo César. *Comentários à Lei de Organização Criminosa*: Lei 12.850/2013. São Paulo: Saraiva, 2014.

BOCK, Lisa. *Modern Cryptography for Cybersecurity Professionals*: Learn how you can leverage encryption to better secure your organization's data. Birmingham: Packt Publishing, 2021.

BOLZAN DE MORAIS, José Luis. O Estado de Direito "confrontado" pela "revolução da internet"! *Revista Eletrônica do Curso de Direito da Universidade Federal de Santa Maria*, v. 13, n. 3, p. 876-903, 2018.

BRIGHI, Raffaella; FERRAZZANO, Michele. Digital forensics: best practices and perspective. In: CAIANIELLO, Michele; CAMON, Alberto (Ed.). *Digital forensic evidence*: towards common European standards in antrifraud administrative and criminal investigations. Milão: CEDAM, 2021.

BROCHADO, Mariah. *Inteligência artificial no horizonte da filosofia da tecnologia*: técnica, ética e direito na era cybernética. São Paulo: Dialética, 2023.

BURGE, Jeremy. Google Updates Gun Emoji. *Emojipedia*, 24.04.2018. Disponível em: [https://bit.ly/46o8VS6]. Acesso em: 24.06.2023.

CAMARGO, Rodrigo Oliveira de. *Tratamento de dados, persecução penal e a garantia do direito de defesa*. Tese (Doutorado em Ciências Criminais) – Programa de Pós-Graduação em Ciências Criminais, Escola de Direito, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2022.

CARVALHO NETTO, Menelick de. A hermenêutica constitucional sob o paradigma do Estado Democrático de Direito. In: CATTONI DE OLIVEIRA, Marcelo (Coord.). *Jurisdição e hermenêutica constitucional no Estado Democrático de Direito*. Belo Horizonte: Mandamentos, 2004.

CONLAN, Kevin; BAGGILI, Ibrahim; BREITINGER, Frank. Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy. *Digital Investigation*, v. 18, p. 66-75, aug. 2016.

DAHBUR, Kamal; MOHAMMAD, Bassil. Toward understanding the challenges and countermeasures in computer anti-forensics. In*:* ALJAWARNEH, Shadi (Ed.). *Cloud Computing Advancements in Design, Implementation, and Technologies*. [S.l.]: IGI Global, 2013.

DOMINGOS, Fernanda Teixeira Souza. As provas digitais nos delitos de pornografia infantil na internet. In*:* SALGADO, Daniel de Resende; QUEIROZ, Ronaldo Pinheiro (Orgs.). *A prova no enfrentamento à macrocriminalidade*. 3. ed. Salvador: JusPodivm, 2019.

ENGLANDER, Irv. *The architecture of computer hardware, systems software & networking*: an information technology approach. Hoboken: John Wiley & Sons, 2014.

FELDENS, Luciano. *O direito de defesa*: a tutela jurídica da liberdade na perspectiva da defesa penal efetiva. 2. ed. Porto Alegre: Livraria do Advogado, 2021.

FELDENS, Luciano; TEIXEIRA, Adriano. *O crime de obstrução de justiça*: alcance e limites do art. 2º, § 1º, da Lei 12.850/2013. São Paulo: Marcial Pons, 2020.

FERGUSON, Ian; RENAUD, Karen; WILFORD, Sara; IRONS, Alastair. PRECEPT: a framework for ethical digital forensics investigations. *Journal of Intellectual Capital*, v. 21, n. 2, p. 257-290, 2020.

FERREIRA, William; FERREIRA, Cristiane; CRUZ JÚNIOR, Gelson da; SOARES, Fabrizzio. A review of digital image forensics. *Computers & Electrical Engineering*, v. 85, p. 66-85, jul. 2020.

FLORIDI, Luciano. Should we be afraid of AI? *Aeon Essays*, 2016. Disponível em: [https://bit.ly/43rlJs6]. Acesso em: 19.07.2023.

FLORIDI, Luciano. The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. *Philosophy & Technology*, v. 33, n. 3, p. 369-378, 2020.

GARFINKEL, Simson. Anti-forensics: Techniques, detection and countermeasures. In: ARMISTEAD, Leigh; Edith Cowan University. *2nd International Conference on i-Warfare and Security*. Reading: Academic Conferences Limited, 2007.

GOMES, Luiz Flávio. Princípio da não-autoincriminação: significado, conteúdo, base jurídica e âmbito de incidência. In: LIMA, Joel Corrêa de; CASARA, Rubens R. R. (Coords.). *Temas para uma perspectiva crítica do Direito*: homenagem ao Professor Geraldo Prado. Rio de Janeiro: Lumen Juris, 2012.

GÜL, Murat; KUGU, Emin. A survey on anti-forensics techniques. *2017 International Artificial Intelligence and Data Processing Symposium (IDAP)*. Malatya: IEEE, 2017.

HOBUSS, João. Sobre ética e virtudes. In*:* HOBUSS, João (Org.). *Ética das virtudes*. Florianópolis: Editora da UFSC, 2011

JAIN, Anu; CHHABRA, Gurpal Singh. Anti-forensics techniques: An analytical review. *2014 Seventh International Conference on Contemporary Computing* (IC3). Noida: IEEE, 2014.

JAPIASSU, Hilton. *Interdisciplinaridade e patologia do saber*. Rio de Janeiro: Imago, 1976.

LESSIG, Lawrence. *Code*: version 2.0. New York: Basic Books, 2009.

LOPES JR., Aury; ROSA, Alexandre Morais da. A importância da cadeia de custódia para preservar a prova penal. *Revista Consultor Jurídico*, 16.01.2015. Disponível em: [https://bit.ly/3QvtK7l]. Acesso em: 29.06.2023.

LOPES, Marcus Vinícius Pimenta. *Busca e apreensão de elementos digitais*. São Paulo: Ed. RT, 2025.

MASON, Stephen; SHELDON, Andrew; DRIES, Hein. Proof: the technical collection and examination of electronic evidence. In*:* MASON, Stephen; SENG, Daniel (Ed.). *Electronic Evidence*. 4. ed. London: Institute of Advanced Legal Studies, 2017.

MASON, Stephen; STANFIELD, Allison. Authenticating electronic evidence. In*:* MASON, Stephen; SENG, Daniel (Ed.). *Electronic Evidence*. 4th ed. London: Institute of Advanced Legal Studies, 2017.

MENDES, Carlos Hélder C. Furtado. *Prova penal digital*: direito à não autoincriminação e contraditório na extração de dados armazenados em dispositivos informáticos. São Paulo: Tirant lo Blanch, 2024.

MENDES, Carlos Hélder Carvalho Furtado. *Tecnoinvestigação criminal*: entre proteção de dados e a infiltração por *software*. Salvador: JusPodivm, 2020.

NUNES, Dierle. Virada tecnológica no direito processual (da automação à transformação): seria possível adaptar o procedimento pela tecnologia? In*:* NUNES, Dierle; LUCON, Paulo Henrique dos Santos; WOLKART, Erik Navarro. *Inteligência artificial e direito processual*: os impactos da virada tecnológica no direito processual. Salvador: JusPodivm, 2020.

NUNES, Dierle. Virada tecnológica no direito processual: fusão de conhecimentos para geração de uma nova justiça centrada no ser humano. *Revista de Processo*, v. 344, p. 403-429. 2023.

PAIVA, Stanley Gusmão de. Técnicas avançadas de extração de dados. *Revista Brasileira de Execução Penal*, Brasília, v. 3, n. 2, p. 129-146, jan./jun. 2022.

PERON, Christian; LEGARY, Michael. Digital anti-forensics: emerging trends in data transformation techniques. E-CRIME COMPUT. EVID. *Proceedings* [...]. West Lafayette: Center for Education and Research in Information Assurance and Security (CERIAS), 2005.

PRADO, Geraldo. *A cadeia de custódia da prova no processo penal*. São Paulo: Marcial Pons, 2019.

PRADO, Geraldo. Investigação criminal digital e processo penal. In: ABELLÁN, Marina Gascón; MATIDA, Janaina (Coords.). *Melhorar a prova*. São Paulo: Marcial Pons, 2024.

PRADO, Geraldo. *Prova penal e sistema de controles epistêmicos*: a quebra da cadeia de custódia das provas obtidas por métodos ocultos. São Paulo: Marcial Pons, 2014.

REARDON, Joel; BASIN, David; CAPKUN, Srdjan. SoK: Secure data deletion, 2013 IEEE Symposium on Security and Privacy. *Proceedings* [...] IEEE, 2013.

ROGERS, Marcus. Anti-forensics: the coming wave in digital forensics. Center for Education and Research in Information Assurance and Security (CERIAS). *Proceedings* [...] West Lafayette: CERIAS, 2006.

ROSSI, Francesca. *Il confine del futuro*: possiamo fidarci dell'intelligenza artificiale? Milano: Feltrinelli Editore, 2019.

SARKIS, Jamilla Monteiro. Direito da pessoa imputada ao anonimato digital. *Revista Brasileira de Direito Processual Penal*, v. 10, n. 3, 2024.

SARKIS, Jamilla Monteiro. *Não autoincriminação*: uma (re)leitura constitucional na era tecnológica da cyber-surveillance. São Paulo: Tirant lo Blanch, 2024.

SCHAFER, Burkhard; MASON, Stephen. The characteristics of electronic evidence. In*:* MASON, Stephen; SENG, Daniel (Ed.). *Electronic Evidence*. 4th ed. London: University of London Press, Institute of Advanced Legal Studies, 2017.

SHIRANI, Behzad. *Anti-forensics*. [Presentation on] High Technology Crime Investigation Association Conference 2002.

SOMBRIO, Débora Normanton. Nem tudo é prova: a cadeia de custódia como método de controle de fixação dos fatos no Processo Pena. In*:* SARKIS, Jamilla Monteiro; SANTIAGO NETO, José de Assim; PAULA, Leonardo Costa de (Orgs.). *Tudo e um pouco mais da inquisitoriedade no Processo Penal*: estudos em homenagem ao Professor Leonardo Marinho. Curitiba: Observatório da Mentalidade Inquisitória, 2021.

SUSSKIND, Richard. *Online courts and the future of justice*. Oxford University Press, 2019.

TARUFFO, Michele. *A prova*. São Paulo: Marcial Pons, 2014.

TEPPLER, Steven. Testable reliability: a modernized approach to ESI admissibility. *Ave Maria Law Review*, v. 12, n. 2, p. 213-255, Summer 2014.

TORRES, Henrique Abi-Ackel; LOPES, Luciano Santos. A proibição da autoincriminação involuntária no processo penal brasileiro: uma análise de precedente do Superior Tribunal de Justiça (*Habeas Corpus* 425.044/RJ). In: ESPIÑERA, Bruno; COLAVOLPE, Luís Eduardo; MATTOS FILHO, Maurício (Orgs.). *A prova e o processo penal constitucionalizado*: estudos em homenagem ao Ministro Sebastião Reis. Belo Horizonte: D'Plácido, 2021.

TÓRTIMA, Fernanda. O limite ao direito do investigado de destruir provas que o incriminem. In: ESPIÑERA, Bruno; COLAVOLPE, Luís Eduardo; MATTOS FILHO, Maurício (Orgs.). *A prova e o processo penal constitucionalizado*: estudos em homenagem ao Ministro Sebastião Reis. Belo Horizonte: D'Plácido, 2021.

WANI, Mohamad Ahtisham. Privacy preserving Anti-Forensic Techniques. In*:* GIRI, Kaiser J.; PARAH, Shabir Ahmad; BASHIR, Rumaan; MUHAMMAD, Khan (Ed.). *Multimedia Security*: Algorithm Development, Analysis and Applications. Singapore: Springer, 2021 (Series Algorithms for Intelligent Systems),

ZONTA, Ivan Navarro. *Obstrução de justiça e direito de defesa*. São Paulo: Tirant lo Blanch, 2023.

Recebido em: 30.03.2025.
Aprovado em: 18.08.2025.
Última versão das autoras: 18.08.2025.

PESQUISA DO EDITORIAL

Área do Direito: Processual; Penal

Veja também Doutrina relacionada ao tema

- Dado informático como fonte de prova penal confiável(?): apontamentos procedimentais sobre a cadeia de custódia digital, de Carlos Hélder C. Furtado Mendes – *RBCCrim* 161/131-161;
- "Eu sei o que vocês fizeram no verão passado": o uso de *software* de espionagem como meio de obtenção de prova penal, de Eduardo Bolsoni Riboli – *RBCCrim* 156/91-139; e
- *Standards* probatórios: remédio ou veneno? É uma questão de lugar!, de Vitor Paczek Machado e Carlos Hélder C. Furtado Mendes – *RBCCrim* 171/351-388.

Entrevistas

Entrevista com a Professora Dra. Heloisa Estellita

Interview with Professor Dr. Heloisa Estellita

Rodrigo Oliveira de Camargo[1]
ORCID: [https://orcid.org/0000-0003-2340-9901].
rodrigo@rodrigodecamargo.com.br

Carlos Helder Furtado Mendes[2]
ORCID: [https://orcid.org/0000-0001-5256-1297_].
helder@madeiraadvogados.com.br

DOI: [doi.org/10.5281/zenodo.17058418].



Professora da Escola de Direito da Fundação Getulio Vargas, onde integra a coordenação do Grupo de Ensino e Pesquisa em Direito Penal Econômico e da Empresa. Financiada pela Fundação Alexander von Humboldt e pela CAPES, fez pesquisas de Pós-Doutorado na Ludwig-Maximilians-Universität, de Munique; na Universidade de Augsburg; na Universidade

1. Doutorando em Ciências Criminais pela PUCRS. Bolsista Capes. Mestre em Ciências Criminais pela PUCRS (2011). Professor de Direito Penal e Processo Penal da ULBRA/Torres. Coordenador Estadual do IBCCRIM, no Estado do Rio Grande do Sul. Membro da Comissão Especial de Prevenção à Corrupção da OAB/RS. Autor de artigos e capítulo de livro sobre Direito Penal, Processo Penal e *Compliance* Anticorrupção. Advogado.
ORCID: [https://orcid.org/0000-0003-2340-9901].
E-mail: rodrigo@rodrigodecamargo.com.br
2. Doutor e Mestre em Ciências Criminais pela PUC-RS. Especialista em Direito Penal Econômico pela Universidade de Coimbra/IBCCRIM (2017). Especialista em Ciências Penais pela Uniderp (2017). Bacharel em Direito pelo UNDB – Centro Universitário/MA (2015). Advogado.
Lattes: [http://lattes.cnpq.br/3034060693231004_].
ORCID: [https://orcid.org/0000-0001-5256-1297_].
E-mail: helder@madeiraadvogados.com.br

Humboldt de Berlim (Alemanha); e na Universidade Pompeu Fabra (Barcelona, Espanha; CAPES Print). Doutora em Direito Penal pela Universidade de São Paulo. Mestre em Direito pela Universidade Estadual Paulista. Especialista em Direito Penal Econômico e Europeu (Universidade de Coimbra).

A presente entrevista, conduzida por Rodrigo Oliveira de Camargo e Carlos Helder Furtado Mendes, para o dossiê temático "Proteção de Dados Pessoais e Ciências Criminais", da *Revista Brasileira de Ciências Criminais*.

1. A partir da sua experiência como pesquisadora nas universidades de Munique, Berlim e Barcelona, como a proteção de dados pessoais tem sido debatida no contexto europeu, especialmente no campo penal? Quais aprendizados podem ser transpostos, com as devidas cautelas, para o caso brasileiro?

Na Europa, o debate sobre proteção de dados no campo penal iniciou-se no século passado. Com a Diretiva UE 2016/680, que regula especificamente o tratamento de dados por autoridades competentes em matéria penal, ele se tornou mais padronizado no ambiente europeu. Trata-se de reequilibrar a proteção de direitos fundamentais com o avanço geométrico do acesso das autoridades de persecução penal a dados pessoais. Uma tarefa urgente para o Brasil.

2. Considerando sua atuação no Tribunal Penal Internacional (TPI) e na Assembleia dos Estados-Partes, quais os principais desafios enfrentados por tribunais internacionais na harmonização entre o combate à criminalidade transnacional e a proteção de dados pessoais dos investigados e vítimas?

O principal desafio está na ausência de marcos normativos no âmbito do próprio Estatuto de Roma. Não obstante, desde sua instalação, o TPI tem cuidado de forma robusta da proteção de dados dos investigados, acusados, vítimas e testemunhas. Um tratamento que contrasta bastante com a publicidade processual opressiva que vemos no Brasil.

3. O Direito Penal Econômico tem lidado cada vez mais com a gestão e a análise massiva de dados. Como garantir, nesse contexto, a proteção de dados pessoais sem comprometer a efetividade das investigações?

A chave está na construção de medidas de proteção proporcionais e tecnicamente adequadas. O tratamento de dados deve estar ancorado em autorização legal, finalidades legítimas, mecanismos de transparência, minimização e descarte

Camargo, Rodrigo Oliveira de; Mendes, Carlos Helder Furtado. Entrevista com a Professora Dra. Heloisa Estellita. *Revista Brasileira de Ciências Criminais*. vol. 211. ano 33. p. 261-265. São Paulo: Ed. RT, nov./dez. 2025.
DOI: [doi.org/10.5281/zenodo.17058418].

de material impertinente, análise de risco e, especialmente, limitações robustas ao compartilhamento. É muito importante a promulgação de uma LGPD Penal e, também, de revisão legislativa, para que as medidas investigativas massivas atendam aos standards de proteção de dados.

4. Na sua avaliação, os métodos de coleta de dados pessoais em investigações financeiras e empresariais – muitas vezes utilizados com base em mecanismos de cooperação internacional – têm respeitado os princípios do devido processo legal e da proporcionalidade?

Quando há previsão legal, como no caso do sigilo bancário e mesmo do fiscal, há maior respeito aos princípios. O problema é em toda a área não coberta por autorização legal, na qual, inobstante a ausência de autorização do legislador, as agências de investigação têm avançado significativamente. Um exemplo é a atuação do Coaf e mesmo a obtenção de dados financeiros de provedores de aplicações. Nessa seara, cumpre ao Judiciário conter o avanço e ao Legislativo prover diplomas legais regulando a matéria de forma clara e determinada.

5. A ampliação das formas de vigilância no setor privado, muitas vezes amparada por contratos e políticas internas, pode influenciar as práticas estatais de persecução penal? Há um risco de "naturalização" do controle extrajudicial de dados?

Sim. O compartilhamento crescente de dados do setor privado com autoridades públicas – muitas vezes sem ordem judicial – contribui para a erosão dos direitos fundamentais à imagem, à vida privada e à autodeterminação informativa. Muito embora ele já se encontre sob a égide da LGPD, o desconhecimento dessa nova esfera de proteção de direito fundamental ainda faz com que haja uma certa promiscuidade no compartilhamento de dados do setor privado com agências de investigação e persecução penal. Para coibir essa prática, são necessárias, de um lado, a educação dos operadores jurídicos quanto ao regime de proteção de dados e, de outro, a atuação firme do Poder Judiciário coibindo a informalidade e o abuso.

6. No contexto da produção probatória em crimes econômicos complexos, como a senhora avalia o uso de fontes abertas e dados estruturados obtidos via sistemas automatizados? Em que medida isso tensiona os limites das garantias processuais?

O uso de fontes abertas e ferramentas automatizadas pode ser útil, mas sua validade probatória depende de critérios de transparência, autenticidade, integridade

e contextualização. O risco está na opacidade dos *outputs* gerados por algoritmos e na ausência de contraditório sobre os critérios de busca, seleção e classificação dos dados.

7. Como interpretar, à luz do garantismo penal, os projetos de lei que buscam regular o tratamento de dados pessoais para fins de segurança pública e investigação penal? Há riscos de flexibilização indevida dos direitos fundamentais?

Há, principalmente, duas propostas de regulamentação que vão em sentido diametralmente opostos. De um lado, o Anteprojeto de LGPD Penal, elaborado por uma comissão de juristas ao presidente da Câmara, em 2020, que está alinhado com o *standard* protetivo do ambiente europeu; e o PL 1.515/2022, que apenas atende aos interesses dos órgãos de investigação e persecução penal, e que, portanto, não desempenha a função de garantia do direito constitucional à autodeterminação informacional. O PL 1.515 deveria ser arquivado e o Anteprojeto deveria ser apresentado como PL, discutido, aperfeiçoado, aprovado e sancionado pelo Presidente da República.

8. Considerando sua atuação como parecerista e assessora de órgãos de governo, como o Ministério da Justiça e o STF, quais seriam os critérios mínimos para uma regulamentação legítima e proporcional sobre o uso de dados em investigações penais?

Há duas medidas urgentes: a) legislar na matéria de forma clara e exaustiva, por meio de uma lei geral de proteção de dados em matéria penal que estabeleça os parâmetros de tratamento para todo o sistema, já que a persecução penal (entendida em sentido amplíssimo) é toda baseada em tratamento de dados e de forma ubíqua; b) atualizar toda a legislação autorizativa de intervenções nesse direito (interceptações, acesso a dados armazenados etc.), para incluir dispositivos específicos, adequando-a à proteção da autodeterminação informacional, inclusive regulando, se o caso, novas formas de intervenção (como a infiltração *online*, por exemplo).

9. Em sua visão, como a formação jurídica no Brasil – especialmente nos cursos de Direito Penal e Processual Penal – pode incorporar criticamente o tema da proteção de dados pessoais como uma dimensão transversal da dogmática penal?

Acho que deveria ser ministrada como parte regular dos cursos de Direito e, também, como formação específica na Pós-Graduação. Idealmente, a matéria

deveria ser abordada a partir da teoria constitucional dos direitos fundamentais, passando pelos institutos gerais da proteção de dados, até chegar aos detalhes próprios da matéria penal e, especialmente, do processo penal.

10. Por fim, que papel o Direito Penal, especialmente em sua vertente econômica, deve desempenhar na construção de limites democráticos frente à expansão da vigilância algorítmica e à crescente integração entre setores público e privado na coleta de dados?

A tarefa de salvaguardar os direitos fundamentais e as facetas da democracia afetadas pela vigilância digital também é tarefa do Direito Penal, todo ele, inclusive o Econômico. Nesse sentido, é digno de registro o fato de que nossa tutela penal contra a vigilância digital é muito lacunosa. Não temos tipos penais voltados ao compartilhamento ilegal de dados pessoais, nem mesmo normas incriminadoras punindo graves violações de segurança cibernética. Essas são as fronteiras atuais em que têm ocorrido violações gravíssimas de direitos fundamentais e ameaça à democracia. Nesse sentido, sem prejuízo do caráter de *ultima ratio* do Direito Penal, entendo que seja necessário legislar também nessa matéria.



PESQUISA DO EDITORIAL



Área do Direito: Penal

Veja também Doutrina relacionada ao tema

- Dados pessoais no processo penal: tutela da personalidade e da inocência diante da tecnologia, de Flaviane de Magalhães Barros Bolzan de Morais, Leonardo Augusto Marinho Marques e Jamilla Monteiro Sarkis – *RBCCrim* 190/117-156;
- O reconhecimento facial na segurança pública e a proteção de dados pessoais como garantia fundamental, de Beatriz Daguer, Luiz Antonio Borri e Rafael Junior Soares – *RDTec* 16;
- Valoração da prova digital: entre a desconfiança e a crença, de Luíza Guimarães Campos Batista Gomes e André Ricardo Godoy de Souza – *RePro* 359/175-207; e
- Vigiar e Punir 4.0: efeitos das tecnologias de policiamento preditivo e reconhecimento facial no brasil e a perpetuação do racismo estrutural, de Fernanda Mateus Rosa da Silva – *RDTec* 16.

Camargo, Rodrigo Oliveira de; Mendes, Carlos Helder Furtado. Entrevista com a Professora Dra. Heloisa Estellita. *Revista Brasileira de Ciências Criminais*. vol. 211. ano 33. p. 261-265. São Paulo: Ed. RT, nov./dez. 2025.
DOI: [doi.org/10.5281/zenodo.17058418].

Entrevista com o Professor Dr. Geraldo Prado

Interview with Professor Dr. Geraldo Prado

Rodrigo Oliveira de Camargo[1]
ORCID: [https://orcid.org/0000-0003-2340-9901].
rodrigo@rodrigodecamargo.com.br

Carlos Helder Furtado Mendes[2]
ORCID: [https://orcid.org/0000-0001-5256-1297_].
helder@madeiraadvogados.com.br

DOI: [doi.org/10.5281/zenodo.17058439].



Professor Emérito da Escola da Magistratura do Estado do Rio de Janeiro (EMERJ), ex-Professor Associado da Universidade Federal do Rio de Janeiro (UFRJ) e Pesquisador Integrado do *Ratio Legis* – Centro de Investigação e Desenvolvimento em Ciências Jurídicas da Universidade Autónoma de Lisboa, o Professor Dr. Geraldo Prado é referência internacional em temas como

1. Doutorando em Ciências Criminais pela PUCRS. Bolsista Capes. Mestre em Ciências Criminais pela PUCRS (2011). Professor de Direito Penal e Processo Penal da ULBRA/Torres. Coordenador Estadual do IBCCRIM no Estado do Rio Grande do Sul. Membro da Comissão Especial de Prevenção à Corrupção da OAB/RS. Autor de artigos e capítulo de livro sobre Direito Penal e Processo Penal e *Compliance* Anticorrupção. Advogado.
ORCID: [https://orcid.org/0000-0003-2340-9901].
E-mail: rodrigo@rodrigodecamargo.com.br
2. Doutor e Mestre em Ciências Criminais pela PUC-RS. Especialista em Direito Penal Econômico pela Universidade de Coimbra/IBCCRIM (2017). Especialista em Ciências Penais pela Uniderp (2017). Bacharel em Direito pelo UNDB-Centro Universitário/MA (2015). Advogado.
Lattes: [http://lattes.cnpq.br/3034060693231004_].
ORCID: [https://orcid.org/0000-0001-5256-1297_].
E-mail: helder@madeiraadvogados.com.br

prova penal, garantismo processual e interseções entre direito, política e economia. Com trajetória que articula a prática jurisdicional, a crítica institucional e a investigação acadêmica transnacional, suas reflexões se destacam pela profundidade analítica e pelo rigor teórico.

A presente entrevista, conduzida por Rodrigo Oliveira de Camargo e Carlos Helder Furtado Mendes para o dossiê temático da Revista Brasileira de Ciências Criminais, busca explorar, à luz da proteção de dados pessoais como direito fundamental, as tensões entre segurança pública, investigação penal e garantias constitucionais.

1. Como sua formação em História das Ideias e Cultura Jurídicas, desenvolvida em Coimbra, influencia sua leitura crítica das transformações normativas recentes sobre proteção de dados pessoais no Brasil, como a Emenda Constitucional 115/2022 e a promulgação da Convenção de Budapeste?

Antes mesmo do período de estudos pós-doutorais, em Coimbra, sob supervisão e diálogo com o Prof. Dr. Rui Cunha Martins, minhas pesquisas no âmbito do saber processual penal se caracterizavam por forte influência criminológica e por abertura às contribuições teóricas da história dos sistemas de justiça criminal, além de modestos aportes sociológicos e filosóficos.

Creio que é possível notar essa influência – que, no campo da criminologia está ancorada nos saberes das criminologias críticas – pela maneira como abordei os sistemas processuais penais (Sistema Acusatório), os poderes de intromissão na esfera das comunicações (Limite às Interceptações Telefônicas e a Jurisprudência do Superior Tribunal de Justiça) e os acordos penais (Transação Penal), cobrindo o período de 1998 a 2003.

Em 2010, em Coimbra, pude aprofundar as investigações de caráter multidisciplinar, incluindo aportes da esfera da economia e, principalmente, a base teórica das histórias das ideias, fatores que proporcionaram melhor compreensão das disputas narrativas no próprio campo jurídico entre teses "hegemônicas" e teses "insurgentes", disputas que transferiam para as teorias jurídicas desigualdades e assimetrias epistemológicas visíveis na relação entre Estados e internamente, em cada Estado, entre os grupos sociais que o integram.

Creio que um honesto olhar retrospectivo leva à conclusão de que é a partir de 2010, dos estudos em Coimbra, que o tema do "Poder" adquire centralidade e maior consistência teórica no meu pensamento, apesar de estar em semente desde o início dos anos 1990.

É com ferramentas teóricas e com visão de mundo extraídas dessa experiência – de um mundo desigual, com forte presença e domínio das *Big Techs* – que tanto a

Camargo, Rodrigo Oliveira de; Mendes, Carlos Helder Furtado. Entrevista com o Professor Dr. Geraldo Prado. *Revista Brasileira de Ciências Criminais*. vol. 211. ano 33. p. 267-274. São Paulo: Ed. RT, nov./dez. 2025.
DOI: [doi.org/10.5281/zenodo.17058439].

proteção de dados como as várias normativas acerca do "mundo digital", incluindo a Convenção de Budapeste, passam a ser analisadas por mim.

2. De que modo sua experiência como Desembargador do TJ-RJ e posterior atuação acadêmica alteraram sua percepção sobre os limites e riscos do uso de dados pessoais em investigações criminais?

Fui magistrado de janeiro de 1988 a abril de 2012 (antes fui advogado e promotor de justiça). No exercício da magistratura, no TJ do Rio de Janeiro, fui promovido a desembargador em dezembro de 2006.

Leciono Direito Processual Penal desde 1987 e, após ter sido professor em instituições privadas (UNIG, UGF, Universidade Veiga de Almeida e Universidade Cândido Mendes), em 2004 ingressei na Faculdade Nacional de Direito (UFRJ). Encerrei meu ciclo na UFRJ como professor associado em 2020, o que me permitiu aprofundar as ligações acadêmicas com Universidades portuguesas.

Assim, as atividades na Academia e no Poder Judiciário foram quase concomitantes e tenho clareza de que se beneficiaram uma da outra. Fui melhor juiz – ou me senti dessa maneira – por causa da Universidade; fui melhor pesquisador e professor graças à atuação como magistrado. Tudo isso, certamente, teve o alto custo do sacrifício familiar.

Como minha vida é contemporânea à ditadura empresarial-militar, à transição de 1985-1988 (nessa época eu estava no Ministério Público ou recém-ingresso na magistratura) e à nossa instável democracia atual, posso afirmar que a proteção de dados sempre esteve no meu horizonte de preocupação.

Na atualidade, o que a revolução digital permite ou possibilita é a concentração e o processamento massivo desses dados, em especial com emprego de aplicações de inteligência artificial, que potencializam, em condições nunca experimentadas, os poderes de controle social.

A definição de perfis pessoais, predições comportamentais mais precisas, hipervigilância e induzimento a práticas e comportamentos desejados pelos detentores do poder estão viabilizados em um nível global nunca experimentado. No exercício cotidiano da magistratura apenas é possível notar pequenos fragmentos desse exercício de poder. Aos juízes e juízas, na prática judicial, é muito difícil perceber a dimensão global do problema e, em cada caso concreto, refletir sobre a macroprojeção das microdecisões proferidas diariamente.

Em geral, somente vendo de fora – e a Universidade é um desses "lugares de fora" – é que é possível dar-se conta das amplas consequências muitas vezes perversas desse exercício manipulado do poder.

É importante também ter em conta que não é a primeira vez que a sociedade ocidental se depara com grandes sistemas ideológicos instrumentalizadores da

dominação. Foi assim na Europa, no período de ascensão das práticas inquisitoriais que viabilizaram grande parte dos Estados territoriais modernos, com forte influência nas dimensões do simbólico e do imaginário exercida pelas doutrinas da Igreja Católica.

Embora não inédito, o atual processo de dominação ideotecnológica é muito perigoso para a sobrevivência das sociedades humanas e da própria vida no planeta dado o seu imenso poder de destruição.

3. Como o senhor analisa a expansão dos mecanismos de vigilância e extração de dados no campo penal à luz da tradição garantista do processo penal brasileiro?

É duvidoso falar em "tradição garantista do processo penal brasileiro". Nossa Constituição de 1988 é de fato garantista, mas a tradição de nossas práticas penais é autoritária, e o texto constitucional por si só não foi capaz de gerar o *breakdown* a que já me referi em tantas ocasiões. A Constituição se mostrou frágil para romper com o autoritarismo que está presente na nossa sociedade e, em consequência, no sistema de justiça criminal.

As práticas jurídico-penais inconstitucionais beneficiam-se muito dessa "expansão dos mecanismos de vigilância e extração de dados", acentuando e aprofundando com muita eficiência o controle social.

Convém observar que não se trata apenas do incremento da hipervigilância digital. Isso vem combinado, como mencionei na resposta anterior, com dispositivos de limitação cognitiva que são difundidos e largamente usados para converter o indivíduo em vigilante dele próprio.

Grupos de *WhatsApp* e *Telegram*, a plataforma *X*, a *Discord* e outros, condicionam comportamentos e facilitam a dominação de vastos setores da sociedade, incluindo suas classes médias, estabelecendo novas formas de servidão voluntária.

A hipervigilância e o acesso e ao massivo processamento de dados otimizam as condições de sufocamento das dissidências, de silenciamento do pensamento divergente e constrangem práticas sociais alternativas, praticamente instituindo um sistema penal digital autoritário sobreposto ao sistema penal oficial.

4. A investigação defensiva, tal como promovida por iniciativas como o Núcleo de Investigação Defensiva (Nidef), poderia constituir um contraponto legítimo à extração unilateral de dados pelas forças estatais? Quais os desafios éticos envolvidos nesse processo?

A investigação defensiva, que consiste em um dispositivo jurídico que permite às defesas de suspeitos e imputados buscar, com respaldo normativo, informações

sobre fato que seja objeto de investigação criminal, é decorrência lógica de um sistema jurídico-penal fundado na paridade de armas, isto é, no equilíbrio funcional entre os sujeitos, compensando a natural desigualdade entre o aparelho de persecução estatal e advogados e instituições dedicadas à defesa, como é o caso da Defensoria Pública.

Não se trata da única modalidade de investigação particular (em sentido *lato*), e é aquela que pode diminuir a assimetria cognitiva entre interessados e partes na persecução penal.

Não diria que se trata de um "contraponto à extração unilateral de dados pelas forças estatais", mas de um necessário mecanismo de verificação e controle de atividades probatórias sofisticadas e em constante evolução, que cada vez mais são dependentes da atuação de especialistas.

O contraditório em matéria de prova de matriz digital exige que ambas as partes – acusação e defesa – estejam preparadas para discutir temas da ciência da computação que são determinantes para se considerar certo meio de prova habilitado processualmente.

A professora italiana Serena Quattrocolo fala em uma "transparência de percurso", no tocante à prova digital, em contraposição à sua ordinária opacidade, transparência essa que exige conhecimento multidisciplinar que não está ao alcance dos juristas.

Por essa razão, é fundamental que a defesa penal disponha de recursos técnicos que lhe permitam entender a prova digital, em todas as suas etapas, e, consequentemente, a explicar ao julgador, como também é fundamental para o Ministério Público.

O Nidef, da Defensoria Pública do Rio de Janeiro, cumpre esse importante papel. Vale lembrar que os especialistas, independentemente de atuarem a requerimento das partes, têm o dever de agir conforme a verdade do objeto de estudo, empregando as boas práticas e advertindo os aspectos adequados e inadequados de cada situação examinada.

É possível que o resultado da análise do especialista, confirmando a integridade da prova digital, sirva para que a defesa estabeleça estratégias processuais convenientes e realistas, distintas, por exemplo, da impugnação da perícia oficial.

5. Em que medida a ideia de liberdade informática – especialmente sob o marco da LGPD – pode e deve impactar a admissibilidade e valoração da prova penal?

Garantir a liberdade e a privacidade dos indivíduos no tratamento de seus dados pessoais, assegurar o livre desenvolvimento da personalidade, na perspectiva da

dignidade da pessoa humana, impõem barreiras à admissibilidade e à valoração de provas digitais que no seu processo de aquisição e preservação contravenham esses valores, independentemente da consideração a respeito do significado de "verdade" em tese representado em uma prova digital declarada ilícita.

6. O senhor tem discutido as relações entre direito e economia. Como o senhor enxerga a crescente mercantilização dos dados pessoais na engrenagem do sistema penal contemporâneo?

Com algo bastante perigoso, quase uma "transmissão onerosa dos órgãos alheios".

O que se percebe na prática, dada a sofisticação das tecnologias hoje disponíveis, é que são incrementadas as situações de erro judiciário pela via da manipulação maliciosa de dados de terceiros.

7. Que riscos reais os métodos ocultos de investigação representam para a integridade dos sistemas informáticos e para o devido processo legal? Há como mitigar esses riscos?

Estamos agora em uma fase das provas digitais que ultrapassa as chamadas provas *offline*, ou seja, o acesso a dados digitais hospedados em algum sítio (nas nuvens etc.) ou dispositivo (relógios digitais, aparelhos de telefone celular, computadores portáteis ou de mesa etc.) para as provas *online*, que resultam da interação de agentes informáticos com o mundo digital das pessoas suspeitas ou investigadas.

A infiltração digital e o uso de *softwares* espiões introduzem agentes da investigação no próprio ambiente digital alvo, com possibilidade de intervenção e manipulação de arquivos e dados em geral.

Trata-se de situação de risco elevado pela evidente possibilidade de manipulação maliciosa do ambiente digital, com inserção e/ou apagamento intencional de dados visando confirmação de hipóteses acusatórias ou exculpatórias.

Daí que, por um lado, é incabível a incidência de presunções de fé pública ou de integridade da coleta e extração de dados, impondo-se sempre ao Estado demonstrar a correção de sua atuação; e, por outro, a mitigação dos riscos passa pela previsão – idealmente na lei – de um terceiro controlador dessas atividades no que toca à sua integridade.

Seria um terceiro em relação à polícia e ao Ministério Público, e penso que o ideal é que seja um perito nomeado pelo juiz criminal.

Camargo, Rodrigo Oliveira de; Mendes, Carlos Helder Furtado. Entrevista com o Professor Dr. Geraldo Prado. *Revista Brasileira de Ciências Criminais*. vol. 211. ano 33. p. 267-274. São Paulo: Ed. RT, nov./dez. 2025.
DOI: [doi.org/10.5281/zenodo.17058439].

8. A adesão à Convenção de Budapeste, somada à colaboração com organismos internacionais, pode colocar em xeque a soberania digital brasileira? Como compatibilizar essa agenda com o princípio da proteção de dados?

Pela aplicação do princípio *pro homine*. Entre normas que na prática se revelem contraditórias ou incompatíveis, deve prevalecer a regra que proteja, de forma mais abrangente, a liberdade e a dignidade da pessoa humana.

9. A proteção de dados pessoais como direito fundamental deveria ser incorporada de forma transversal na formação jurídica? Como reformular os currículos à luz dessas novas exigências democráticas?

A resposta está dada na pergunta em si. Os currículos devem ser reformulados, e isso não deve estar restrito ao ensino superior. Em virtude do atual estágio de transformação digital, essa reformulação e a transversalidade devem ser contempladas já no ensino médio, priorizando debates sobre todos os valores democráticos envolvidos.

10. Qual deveria ser, na sua visão, o papel das ciências criminais na reconstrução do pacto democrático em tempos de vigilância algorítmica e processamento automatizado de dados?

O mesmo de sempre, idealmente. As ciências criminais, como as percebo, têm compromisso com o Estado de Direito, com a proteção da liberdade e com o respeito à dignidade de todas as pessoas.

Portanto, esse é seu papel, que deve desempenhar limitando, no nível da dogmática jurídica e na prática do sistema penal, os poderes selvagens estatais e não estatais.

Camargo, Rodrigo Oliveira de; Mendes, Carlos Helder Furtado. Entrevista com o Professor Dr. Geraldo Prado. *Revista Brasileira de Ciências Criminais*. vol. 211. ano 33. p. 267-274. São Paulo: Ed. RT, nov./dez. 2025.
DOI: [doi.org/10.5281/zenodo.17058439].

PESQUISA DO EDITORIAL

Área do Direito: Penal

Veja também Doutrina relacionada ao tema

- Biometria, autodeterminação informativa e proteção de dados pessoais, de Adriana Espíndola Corrêa e Maria Fernanda Battaglin Loureiro – *RDCC* 36/47-74;
- Linhas gerais sobre a Lei 13.709/2018 (LGPD): objetivos, fundamentos e axiologia da lei geral de proteção de dados brasileira e a tutela de personalidade/privacidade, de Erick da Silva Regis – *RDPriv* 103/63-100; e
- Venda de informações biométricas, privacidade e indisponibilidade de direitos – Estudo de casos, de Patrícia Helena Marta Martins e Bruna Valeri Tavora – *BRTO* 60.

Camargo, Rodrigo Oliveira de; Mendes, Carlos Helder Furtado. Entrevista com o Professor Dr. Geraldo Prado. *Revista Brasileira de Ciências Criminais*. vol. 211. ano 33. p. 267-274. São Paulo: Ed. RT, nov./dez. 2025.
DOI: [doi.org/10.5281/zenodo.17058439].

Direito Por Quem o Faz

Análise jurisprudencial dos Tribunais Superiores no campo da proteção de dados pessoais em âmbito penal

Case law analysis of the Superior Courts in the field of personal data protection in criminal matters

Raissa de Cavassin Milanezi[1]
Pontifícia Universidade Católica do Paraná, PUCPR, Brasil.
raissadcm@gmail.com

DOI: [doi.org/10.5281/zenodo.17080246].

Área do Direito: Digital; Penal

Resumo: A proteção de dados foi eleita como um direito fundamental, o que lhe confere eficácia direta e vinculativa na perspectiva da dogmática constitucional. Assim, apesar da ausência de legislação específica sobre proteção de dados no âmbito penal, os Tribunais brasileiros enfrentam o desafio de interpretar demandas jurídicas com base nesse novo paradigma, pois os dados constituem a matéria-prima da sociedade e, portanto, da atividade jurisdicional. Este trabalho tem como objetivo analisar, em termos de estado da arte, como os Tribunais Superiores (STJ e STF) vêm tratando do tema da proteção de dados em âmbito penal. A pesquisa utilizou o método dedutivo, com procedimento teórico e técnica bibliográfica, buscando identificar avanços e lacunas no tratamento jurisprudencial da matéria.

Abstract: Data protection has been established as a fundamental right, granting it direct and binding effectiveness within the framework of constitutional dogmatics. Thus, despite the absence of specific legislation on data protection in the criminal sphere, Brazilian Courts face the challenge of interpreting legal claims under this new paradigm, since data constitutes the raw material of society and, consequently, of judicial activity. This study aims to analyze, in state-of-the-art terms, how the Higher Courts (STJ and STF) have addressed the issue of data protection in the criminal context. The research employed the deductive method, with a theoretical approach and bibliographic technique, seeking to identify advances and gaps in jurisprudential treatment of the matter. The results indicate that,

1. Mestra em Direito na PUC/PR. Advogada. Conselheira Estadual na OAB/PR. Professora de Direito Penal e Digital da Unibrasil.
ORCID: [https://orcid.org/0000-0003-1108-8266].
E-mail: raissadcm@gmail.com

Os resultados indicam que, embora a proteção de dados tenha recebido atenção crescente em outros campos do direito, ainda há pouco desenvolvimento no âmbito penal. Essa lacuna aponta para a necessidade de um aprofundamento teórico e legislativo, assegurando uma interpretação da matéria penal que se harmonize com o direito fundamental à proteção de dados.

Palavras-chave: LGPD penal; Direito fundamental à proteção de dados; Convenção de Budapeste; Jurisprudência penal.

although data protection has gained increasing attention in other branches of law, there is still limited development in the criminal sphere. This gap highlights the need for deeper theoretical and legislative engagement, ensuring that the interpretation of criminal law aligns with the fundamental right to data protection.

Keywords: Criminal LGPD; Fundamental right to data protection; Budapest Convention; Criminal jurisprudence.

Sumário: 1. Introdução. 2. Proteção de dados em âmbito penal. 3. Jurisprudência no campo da proteção de dados pessoais em âmbito penal. 3.1. Jurisprudência do STJ. 3.2. Jurisprudência do STF. 4. Considerações finais. Referências. Legislação. Jurisprudência.

1. Introdução

A revolução tecnológica descrita por Castells (2022) transformou a forma de ser e de estar no mundo, a ponto de a sociedade contemporânea não poder ser mais compreendida sem as tecnologias da informação e da comunicação. Essa nova arquitetura social, que opera em rede e em tempo real, possibilita ações em velocidade surpreendente, o que faz com que a tecnologia constitua um componente estrutural da própria sociedade.

Esse componente estrutural das tecnologias da informação e comunicação impactou tanto o processo produtivo do capital quanto a vida humana como um todo, em que os dados são acumulados em prol de um novo modelo: o capitalismo de vigilância. Esse modelo se caracteriza pela assimetria informacional, pois as empresas que nele atuam detêm um vasto conhecimento sobre nós, enquanto o que elas aprendem não é compartilhado conosco. De acordo com Zuboff (2020, p. 22), expoente da teoria, o capitalismo de vigilância "sabe tudo sobre nós, ao passo que suas operações são programadas para não serem conhecidas por nós. Eles acumulam vastos domínios de um conhecimento novo proveniente de nós, mas que não é para nós".

A dinâmica do capitalismo de vigilância é algo sem precedentes; a extrema assimetria de conhecimento de poder que esse modelo gera revoga direitos fundamentais na sociedade, engendrando um sentimento de vulnerabilidade social. Isso porque nossa vida é transformada unilateralmente em dados, experiências de consumo, é expropriada e manipulada como uma nova forma de controle social

(ZUBOFF, 2020, p. 71). Entretanto, tal controle sobre o comportamento humano compromete a autodeterminação, tudo isso à revelia de normas reguladoras (ZUBOFF, 2020, p. 126) das empresas que operam nesse modelo de capital.

O fenômeno da ausência de regulação das empresas que operam no sistema descrito por Zuboff decorre do legado neoliberal, que defende a autorregulação sob o argumento de que a regulação é opressora[2]. Exemplo disso é o Google, que gastou mais de 17 milhões de dólares em 2011 com atividades de *lobby* para proteger seus interesses empresariais, realizando incursões para impedir propostas legislativas que pudessem tolher operações de superávit comportamental. Naquela época, o Google aproveitou a ausência de legislação para colocar na rua carros autônomos, recrutando funcionários do ex-presidente Obama para influenciar reguladores estatais (ZUBOFF, 2020, p. 148).

A extração de dados neste atual modelo permanece ativa porque os governos também dependem da iniciativa privada para realizar suas atividades de controle social. Dessa forma, constitui interesse (também) do Estado a não regulação e a captura de mais e mais dados para formulação de um superávit comportamental, uma vez que os governos se beneficiam de dados que são de propriedade particular (COURT OF JUSTICE OF THE EUROPEAN UNION, 2014) para o exercício de controle social[3].

Exemplo disso é o deslocamento de um Secretário de Defesa dos Estados Unidos da América ao Vale do Silício em busca de estratégias para enfrentar ameaças de segurança no ciberespaço (Alba, 2016), bem como o compartilhamento de

2. "Um estudo fascinante de Jodi Short, professora de Direito na Universidade da Califórnia, ilustra de forma empírica o papel da ideologia neoliberal, como uma explicação importante para as ambições do Google e seu sucesso na defesa de território sem legislação. Short analisou 1.400 artigos de análise jurídica sobre o tema da regulação, todos publicados entre 1980 e 2005. Conforme prediz a influência de Hayek e Fridman, o tema dominante nessa literatura era a 'natureza coercitiva de governo administrativo' e a sistemática conflação de regulação da indústria com 'tirania' e 'autoritarismo'. Segundo essa visão de mundo, toda regulação é opressiva, e a burocracia deve ser repudiada como uma forma de dominação humana" (ZUBOFF, 2020, p. 130).

3. Nesse sentido, é oportuno destacar: "Se antes tínhamos o indivíduo no passado, hoje temos perfis. Assim como 1984 critica acidamente os governos totalitários de esquerda e de direita, o terror do stalinismo e a barbárie do nazifascismo, Admirável Mundo Novo também questiona o culto ao avanço da técnica, a linha de montagem, a produção em série e a uniformidade, criando um cenário em que as próprias pessoas são programadas e adestradas para cumprir um papel numa sociedade de castas biologicamente definidas, na qual a racionalidade se torna religião, a ciência em ídolo, tudo em um mundo no qual a experiência do sujeito parece não mais fazer sentido" (CAMARGO, 2022, p. 22).

ferramentas de informações do Google com a CIA (AHMED, 2025). Outro exemplo é a disponibilização de satélites para vigilância "ao vivo" com o compartilhamento de informações de empresas privadas para monitoramento de atividades relacionadas ao terrorismo (TOTAL INFORMATION AWARENESS, 2025).

O fenômeno global do capitalismo de vigilância também atinge o Brasil em todos os segmentos, tanto no âmbito público quanto no privado. Porém, a cultura da proteção de dados ainda é incipiente em nosso país, e é por isso que empresas, como a *Tools for Humanity*, julgaram adequada a "compra" do escaneamento de íris da população brasileira, oferecendo 48 criptoativos em troca (MILANEZI, 2025). Além disso, é por isso que diversos estados brasileiros implementaram, à revelia de legislação específica, a tecnologia de reconhecimento facial em prol da segurança pública (PIRES et al., 2021).

Entretanto, a proteção de dados, antes de forma implícita (SARLET, 2021), constitui um direito fundamental explicito. A inclusão da Emenda Constitucional 115/2022, que será abordada no primeiro capítulo, reflete a realidade de uma sociedade tecnológica e informacional, na qual as interações ocorrem em rede (CASTELLS, 2022) e sob a influência do capitalismo de vigilância.

De acordo com a dogmática constitucional, os direitos fundamentais têm como característica eficácia plena e vigência automática (CARVALHO; LIMA, 2015) – o que obriga o Estado a zelar pelos direitos fundamentais mesmo (e sobretudo) no exercício do poder punitivo. Para Pereira:

> "o estágio de desenvolvimento jurídico atual representa a legitimação e a fixação dos direitos fundamentais como valores axiológicos do ordenamento jurídico positivo, consagrando a estrutura constitucional para fins de aplicação imediata e de vinculação do Estado" (PEREIRA, 2014, *e-book*).

Diante desse paradigma social em que mais dados são capturados, armazenados e utilizados para o fim de obtenção de determinada informação, o objetivo é o de analisar, em termos de estado de arte, a temática da proteção de dados em âmbito penal e como os Tribunais Superiores vêm tratando a proteção de dados em âmbito penal.

A pesquisa utilizou o método dedutivo, com procedimento teórico e técnica biográfica documental e jurisprudencial, buscando identificar avanços e lacunas no tratamento jurisprudencial da matéria.

Os resultados indicam que, embora a proteção de dados tenha recebido atenção crescente em outros campos do direito, ainda há pouco desenvolvimento no âmbito penal. Essa lacuna aponta para a necessidade de aprofundamento teórico e legislativo, assegurando uma interpretação que harmonize os direitos fundamentais à privacidade e à proteção de dados em âmbito penal.

2. Proteção de dados em âmbito penal

A temática da proteção de dados não é uma discussão nova. No Brasil, uma das primeiras legislações a demonstrar preocupação com o assunto foi a Lei Geral de Proteção de Dados Pessoais (LGPD)[4], influenciada pelo Regulamento Geral de Proteção de Dados Europeu. Depois da aprovação do regulamento, o Brasil começou a debater a necessidade de um marco regulatório protecionista, uma vez que o bloco europeu passou a exigir que parceiros comerciais se adequassem a essa norma (PINHEIRO, 2022).

De acordo com Doneda (2021), a questão também foi influenciada pelas discussões promovidas nos Estados Unidos da América, por um artigo escrito por Samuel Warren e Louis Brandeis em 1980. À época, Brandeis, Juiz da Suprema Corte, demonstrou preocupação com a intromissão estatal na esfera privada em razão do avanço científico e tecnológico (caso *Olmstead v. United States*). Embora Brandeis tenha sido vencido, suas ideias fomentaram debates legislativos sobre o tratamento de dados em meio computadorizado.

Outro marco histórico importante ocorreu em 1983, quando o Tribunal Constitucional alemão enfrentou uma questão envolvendo o censo (DONEDA, 2021). A demanda referia-se a uma série de perguntas direcionadas à população para levantamento de informações demográficas, sociais e econômicas[5]. Todavia, tal metodologia gerou preocupação, tendo em vista que os dados coletados poderiam ser comparados com outros registros públicos. O Tribunal entendeu que é possível restringir o direito à autodeterminação sobre a informação, desde que se observem a proporcionalidade e os direitos de personalidade (SCHWABE; MARTINS, 2005).

4. O Marco Civil da Internet também foi um marco protetivo importante, visto que estabeleceu direitos, deveres e garantias para os usuários da internet. Todavia, foi a LGPD que passou a estabelecer com mais amplitude a proteção de direitos fundamentais relacionados com a liberdade, a privacidade e o desenvolvimento da personalidade. A LGPD também trouxe uma matriz principiológica importante, como a inclusão, a finalidade, a adequação, a necessidade, o livre acesso, a qualidade dos dados, a transparência, a segurança, a prevenção, a não discriminação, a responsabilização e a prestação de contas, nos termos do art. 6º da Lei 13.709/2018 (BRASIL, 2018).

5. Na sociedade alemã, surgiu um sentimento generalizado de insegurança por causa da impressão de que o governo pudesse se utilizar dos dados para fins diversos e controle estatal dos cidadãos. Destarte, a Corte Constitucional declarou a inconstitucionalidade da lei do censo, amparada nos arts. 1.1 e 2.1 da Lei Fundamental alemã, que garante a dignidade da pessoa humana e o direito ao livre desenvolvimento da personalidade. Com efeito, o direito à autodeterminação informativa foi concebido como um direito fundamental, na esteira do direito geral de personalidade (MELO, 2019, p. 91-92).

O Tribunal alemão destacou que, em razão da capacidade informacional, não é mais necessário analisar fichas e pastas manualmente para obtenção de uma informação. Com o processamento eletrônico de dados, obtêm-se informações detalhadas de uma pessoa, oportunizando, de forma ilimitada, o armazenamento e a consulta de dados a qualquer momento, a qualquer distância e em segundos. Segundo o Tribunal, esses dados "podem ser combinados, sobretudo na estruturação de sistemas de informações integrados, com outros bancos de dados, formando um quadro da personalidade relativamente completo ou quase" (SCHWABE; MARTINS, 2005, *e-book*), o que impede que a pessoa tenha controle suficiente sobre o uso de seus dados.

Na ocasião, o Tribunal já sinalizava a preocupação do monitoramento constante e a sensação de insegurança que isso provocava, de tal forma a atrapalhar o desenvolvimento individual do cidadão, o bem comum e a autodeterminação. A autodeterminação é essencial para comunidade democrática, fundamentada na capacidade e na participação dos cidadãos (SCHWABE; MARTINS, 2005).

O direito à autodeterminação é importante em âmbito social, porque "dá ao indivíduo o poder de ele próprio decidir acerca da divulgação e utilização de seus dados pessoais" (MENKE, 2019, p. 788). Em um contexto social de hiperconexão, essa capacidade se torna ainda mais relevante, já que muitos sentem a perda de controle sobre suas próprias vidas (SPONHOLZ, 2024). Assim, a autodeterminação é um direito importante e elementar para cultura de proteção de dados e para a própria democracia.

De acordo com Lima (2020, p. 12), proteger dados é proteger a pessoa humana, eis que o desenvolvimento individual ocorre por meio da autodeterminação informacional. Para Wolter (2018, p. 110-114), a proteção de dados está ligada à proteção da personalidade, que compreende à privacidade da pessoa e a sua autoapresentação pública.

Wolter (2018, p. 34) explica que o direito de personalidade pode ser compreendido pela metáfora que Hubmann descreveu para o direito civil, que é a teoria das esferas ou dos três círculos concêntricos. A esfera maior é a esfera social ou pública, em que é possível intervir sem grandes dificuldades, como a informação sobre qual é a profissão de alguém. O segundo círculo, intermediário, é a esfera privada ou do sigilo, em que o acesso a informações desse escopo precisa de uma justificação mais intensa, como informações sobre compras de uma pessoa, o local em que ela passa suas férias, quem são seus amigos. Por fim, o terceiro e último círculo, o menor dos três, é aquilo que contém o núcleo da esfera privada, em que não há possibilidade de justificar uma intervenção. Para o autor, esse núcleo é intocável e está diretamente ligado à dignidade humana.

É no terceiro e último círculo que se discute o que é e não é alvo de proteção jurídica. O Tribunal alemão reconheceu, por exemplo, que a utilização de um solilóquio gravado por uma pessoa enquanto ela dirige afeta o núcleo de privacidade. Greco (2018) e Wolter (2018, p. 34) indicam que a utilização da conversa de advogado e cliente também está protegida pelo "núcleo duro" do direito de privacidade.

É preciso destacar, novamente, que o direito à proteção de dados, ao ser incluído no rol de direitos fundamentais, confere ao Estado um dever de defesa ou de proteção, de tal forma que o Estado tem um dever de abstenção no devassamento da vida humana[6]. Para garantir a liberdade de locomoção, o Estado tem o dever de abster-se de prender alguém sem uma justificativa plausível. De igual forma, para garantir a proteção de dados, o Estado tem o dever de abster-se de coletar, processar ou compartilhar informações pessoais sem base legal.

Para além do dever de abstenção, o Estado também assume o compromisso de uma atuação positiva, marcada pela proteção dos direitos dos indivíduos (deveres de proteção) (GRECO, 2018, p. 35), como o compromisso de edição de uma legislação infraconstitucional para dar concretude ao direito fundamental à proteção de dados. De acordo com Mitidiero, Marinoni e Sarlet (2023, p. 471):

> "um dever de proteção a ser concretizado mediante prestações normativas e fáticas, notadamente, por meio da regulação infraconstitucional dos diversos aspectos relacionados às posições jusfundamentais referidas, assegurando-lhe a devida efetividade."

Como exposto anteriormente, a ausência de regulação específica para tratar da proteção de dados pessoais é ponto nevrálgico de crítica na comunidade jurídica. Isso porque a LGPD em âmbito cível, por opção legislativa, excluiu o marco legal para o tratamento de dados pessoais realizados para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais, nos termos do art. 4º[7].

6. Greco (2018, p. 35) explica, que "Tornam-se necessárias algumas palavras sobre aquilo que se poderia chamar de natureza dos direitos fundamentais. Segundo a concepção alemã, os direitos fundamentais são, em primeiro lugar, *Abwehrrechte*, direitos de defesa ou de proteção, dirigidos contra o Estado. Isso é, a primeira função dos direitos fundamentais é de operar no sentido de bloquear a atuação do Estado, impor a este uma omissão. O direito à vida é, em primeiro lugar, o direito de não ser morto pelo Estado, o direito à liberdade de locomoção é o direito de não ser preso pelo Estado e, da perspectiva do Estado, o correlato a esses direitos é um dever de abstenção".
7. Direito que consta no art. 2º, II, da LGPD (BRASIL, 2018).

Ocorre que a ausência de regulação específica pode colocar em risco o direito fundamental à proteção de dados. Nesse sentido, a defesa do consumidor é um direito fundamental, mas o Código de Defesa do Consumidor, ao ser editado, acabou por trazer maior segurança jurídica aos consumidores. É por isso que, para Gleizer, Montenegro e Viana (2021, p. 38), a aprovação de uma lei específica seria importante, na medida em que traria *standards* de proteção para diminuir a vulnerabilidade do titular de dados, até mesmo porque "todo poder tende a ser autoritário e precisa de limites, controle" (LOPES JR., 2023, p. 208).

É certo que o atual cenário – não regulado – conduz em notória incerteza. Com a intenção de diminuir tal incerteza é que uma Comissão de Juristas[8] estruturou um projeto de LGPD penal para regulamentar o tratamento de dados (i) da segurança pública e (ii) das atividades de persecução e repressão de infrações penais em 2020. À época, os juristas destacaram o crescimento de novas técnicas de vigilância e de investigação (Brasil, 2020a).

Logo depois da apresentação do projeto da Comissão, em junho de 2022, o Deputado Coronel Armando apresentou o Projeto de Lei (PL) 1.515/2022, com a finalidade de regulamentar o art. 4º, III, da Lei 13.709/2018 (Brasil, 2022).

Para o Lapin e o Iris, o PL do Coronel não cumpre com a efetivação da proteção de dados (Azevedo et al., 2022, p. 8). De fato, os dois modelos são bem diferentes entre si, um com perspectiva garantista e outro não (MILANEZI, 2024). Enquanto o Projeto da Comissão de Juristas se aplica a duas atividades, o PL se aplica a quatro hipóteses.

Os dois possíveis marcos regulatórios são diferentes em vários aspectos. No que diz respeito aos princípios e direitos do titular, o Anteprojeto elenca mais proteção ao estabelecer os princípios: de licitude, finalidade, adequação, necessidade, proporcionalidade, livre acesso, qualidade dos dados, transparência, segurança da informação, prevenção, não discriminação, responsabilização e prestação de contas (Brasil, 2019a).

Já o PL do Coronel incluiu apenas os princípios de licitude, finalidade, adequação, segurança da informação, prevenção, supremacia do interesse público, qualidade dos dados, não discriminação e auditabilidade – excluindo outros de extrema importância, a exemplo: de proporcionalidade, livre acesso, transparência, confidencialidade e integridade dos sistemas informáticos. A autodeterminação

8. Composta por: Nefi Cordeiro (Presidente) e Antonio Saldanha Palheiro (Vice-presidente) e membros: Laura Schertel Mendes (relatora), Pedro Ivo Velloso (secretário), Danilo Doneda, Davi Tangerino, Eduardo Queiroz, Heloisa Estelita, Humberto Fabretti, Ingo Sarlet, Jacqueline Abreu, Jorge Octávio Lavocat Galvão, Juliana Abrusio, Tercio Sampaio Ferraz Junior e Vladimir Aras.

informativa, basilar da proteção de dados, também foi retirada, enquanto no Anteprojeto ela foi alocada nos fundamentos da disciplina da proteção de dados (art. 2º).

A opção legislativa de se omitir em relação à proteção de dados penal revela a ausência de preocupação social de vigilância do Estado sem qualquer causa legítima para tanto, o que ocorre diante do levantamento da bandeira do combate à criminalidade. Segundo Wolter (2018, p. 161), nem mais se pondera sobre o princípio da presunção de inocência, perdendo-se de vista os problemas que são gerados pela vigilância sistemática.

3. Jurisprudência no campo da proteção de dados pessoais em âmbito penal

A ausência de legislação específica para tratar de dados em âmbito penal, além de não propiciar um arcabouço seguro aos cidadãos, dificulta qualquer pesquisa que vise analisar como os Tribunais Superiores estão abordando o tema. Assim, a construção do presente artigo encontrou obstáculo em relação ao início da pesquisa, eis que não foi possível indicar, no repositório dos Tribunais Superiores, uma lei ou um tema específico que envolva o objeto da pesquisa.

Com finalidade organizacional, o presente capítulo abordará o levantamento jurisprudencial realizado no repositório eletrônico do Superior Tribunal de Justiça (STJ) e do Supremo Tribunal Federal (STF), bem como quais foram os descritores utilizados e os resultados obtidos.

3.1. Jurisprudência do STJ

Em pesquisa de jurisprudência do STJ, com os descritores: "proteção", "dados penais", "proteção de dados penal", "proteção de dados criminal", apenas dois resultados foram obtidos, mesmo com a inclusão de diversos operadores disponíveis no *site*[9], sendo eles: (i) REsp 1.795.908/PB (análise feita infra); e (ii) EDcl no AgRg no AREsp 874.826/TJ, resultado que não guarda relação com a temática (Brasil, 2017a).

Na consulta ao repositório do Tribunal pelo campo "Legislação Aplicada", não há opção para pesquisa da matéria. Por outro lado, ao utilizar o campo "Jurisprudência em Teses" com os termos "dados" e o ramo do direito "Direito Penal", foram encontrados dois documentos: (i) a edição n. 167, sobre o crime de lavagem; e (ii) a edição n. 176, referente aos crimes contra a ordem tributária, econômica e às relações de consumo.

9. Pesquisa feita com operadores E, OU, ADJ, NÃO, PROX, MESMO, COM e $.

Quadro 1 – Levantamento de jurisprudência do STJ

Especificação do julgado	Síntese e informação relevante na temática de proteção de dados
(2019) Pesquisa de "Jurisprudência" REsp n. 1.795.908/PB, Relator Nefi Cordeiro, Sexta Turma, *DJe* 03.06.2019 (Brasil, 2019b)	*Acesso a dados cadastrais bancários.* Trata-se de discussão referente a dados cadastrais para com o sigilo. A Corte entendeu que dados cadastrais bancários, sendo eles, "informações de seus correntistas como número da conta corrente, nome completo, RG, CPF, número de telefone e endereço)", não estão protegidos por sigilo bancário. Segundo a Corte, o sigilo abrange tão somente movimentações financeiras (aplicações, transferências, depósitos etc.). No REsp, o STJ entendeu que o fornecimento de dados cadastrais dos titulares de contas fraudulentas não pode ser considerado como prova nula na hipótese de dados serem fornecidos sem autorização judicial, haja vista que tais dados não estão protegidos pelo direito à intimidade (art. 5º, X, CF). Assim, o acesso a dados básicos não precisa de autorização judicial, diferentemente da busca domiciliar (XI), interceptação (XII) e decreto de prisão (LXI).
Pesquisa de "Jurisprudência em Teses"[10], Edição 167, do crime de lavagem (Brasil, 2025d)	*Acesso a dados cadastrais.* Formulação da tese por intermédio de dois julgados, quais sejam: (1) REsp 1.716.224/RN e (2) REsp 1.561.191/SP. O STJ consolidou o seguinte entendimento: "Nos crimes de lavagem ou ocultação de bens, direitos e valores, a autoridade policial e o Ministério Público têm acesso, independentemente de autorização judicial, aos dados meramente cadastrais de investigados que não são protegidos pelo sigilo constitucional (art. 17-B da Lei 9.613/1998)". Na fundamentação dos julgados, um dos argumentos foi o de que a LGPD admite o tratamento de dados mesmo sem o consentimento do titular para cumprimento de obrigação legal e para atender os legítimos interesses de terceiros. Outro argumento utilizado foi o de que a LGPD Cível afastou sua aplicação para atividades de investigação criminal e persecução penal. O STJ reforçou que o Ministério Público tem competência para tratar dados cadastrais[11], por força do contido no art. 129,

10. Segundo definição do próprio STJ, "Jurisprudência em Teses apresenta, periodicamente, um conjunto de teses com os julgados mais recentes do STJ sobre determinada matéria, selecionados até a data especificada" (BRASIL, 2025c).
11. Sobre o tema, importa esclarecer que existe uma discussão sobre norma de competência e norma de autorização, não sendo possível presumir que de uma regra de competência

Especificação do julgado	Síntese e informação relevante na temática de proteção de dados
	VI e IX, CF/1988, e art. 26, I, b, e II, da Lei 8.625/1993. Além disso, foi mencionado que o Marco Civil da Internet, em seu art. 10, § 3º, prevê que os dados cadastrais podem ser solicitados pelas autoridades que detenham competência legal para tanto, o que é conferido ao Ministério Público no exercício de seu *múnus público.*
Pesquisa de "Jurisprudência em Teses", Edição 176, dos crimes contra a ordem tributária, econômica e contra as relações de consumo IV (Brasil, 2025b)	*Envio de dados da Receita Federal à Polícia ou Ministério Público.* Formulação da tese por intermédio de seis julgados, quais sejam, (1) AgRg no REsp 1.902.209/PR; 2) AgRg no *HC* 502.871/PR; (3) AgRg no REsp 1.651.222/SP; (4) AgRg no REsp 1.723.692/SP; (5) AgRg no REsp 1.836.170/SP; (6) AgRg no *HC* 546.856/SP. O STJ entendeu, em resumo, que: "O envio dos dados sigilosos pela Receita Federal à Polícia ou ao Ministério Público, após o esgotamento da via administrativa, com a constituição definitiva de crédito tributário, decorre de mera obrigação legal de se comunicar às autoridades competentes a possível prática de ilícito, o que não representa ofensa ao princípio da reserva de jurisdição". O STJ considerou que é válido o compartilhamento dos relatórios de inteligência financeira da UIF e a íntegra de procedimento investigatório feito pela Receita Federal, que define o lançamento do tributo para com os órgãos de persecução criminal, sem a obrigatoriedade de autorização judicial. Nos julgados há menção ao Tema 990, STF. No dia 14.05.2025, no Informativo 850, o entendimento da 3ª Seção, na relatoria do Min. Messod Azulay Neto, no RHC 174.173/RJ, foi publicado para entender como inviável a requisição direta de dados do Coaf sem autorização judicial.

Fonte: elaborado pela autora.

A pesquisa também foi complementada com o descritor *Convenção de Budapeste*. O repositório jurisprudencial retornou dois resultados, sendo eles: dois conflitos de competência. Um dos conflitos é de 2013, época em que o Brasil não havia ratificado a Convenção Internacional e o outro, é de 2023, ou seja, pós-ratificação da Convenção.

se tem autorização para algo, "pelo contrário, essa derivação é o raciocínio característico do Estado de polícia, e que o Estado de Direito passa a existir no momento em que se reconhece que ela não é mais possível" (WOLTER, 2018, p. 38).

Em decisão proferida posteriormente à ratificação, o STJ pontuou que a Convenção sobre Crime Cibernético foi internalizada no Brasil pelo Decreto Legislativo 37/2021, e promulgada pelo Decreto 11.491/2023. A análise feita pelo STJ refere-se à extorsão digital ou cibernética, procedimento no qual um terceiro, por meio da internet, acessa de forma ilegal sistemas de informações de uma instituição e bloqueia o acesso a dados, passando a exigir uma quantia para retorno do acesso. Porém, considerando que se tratava de crime previsto em Convenção Internacional, o STJ apenas analisou regra de competência, nos termos do art. 109, IV, da Constituição Federal (BRASIL, 2023b).

Já com relação à prova digital e à cadeia de custódia, o tema tem sido discutido de forma mais ampla pelo STJ. A exemplo, os julgados, (i) HC 653.515/RJ, relatora Ministra Laurita Vaz; (ii) RHC 143.169/RJ, relator Ministro Messod Azulay Neto, 5ª Turma[12]; e (iii) AgRg 828.054/RJ, relator Ministro Joel Ilan Paciornik.

No julgado (iii), o entendimento foi o de que a falta de procedimentos para garantir a integridade e a idoneidade dos dados extraídos de um celular resulta na quebra da cadeia de custódia e na inadmissibilidade da prova digital (Brasil, 2024a).

É de se notar que no STJ a discussão ainda é incipiente na temática da proteção de dados, causando preocupação a utilização, como reforço argumentativo para diminuição de direitos, do fato de que a LGPD cível excluiu sua aplicação em âmbito penal[13], nos termos da Edição 167, da Jurisprudência em Teses.

No que se refere à coleta da prova digital, observa-se o avanço jurisprudencial do STJ ao entender que a quebra da cadeia de custódia resulta na inadmissibilidade da prova digital (MILANEZI; RIOS; FREITAS, 2023). Recentemente (maio/2025), a Sexta Turma do STJ, analisou o uso de provas digitais obtidas a partir do aplicativo SKY ECC via cooperação jurídica internacional entre Brasil e França[14].

---

12. Nesse sentido, destaca-se o tema: "é ônus do Estado comprovar a integridade e confiabilidade das fontes de prova por ele apresentadas. É incabível, aqui, simplesmente presumir a veracidade das alegações estatais, quando descumpridos os procedimentos referentes à cadeia de custódia" (BRASIL, 2023a).
13. Nesse sentido, é a fundamentação: "37. Destaca-se, ainda, que a LGPD não se aplica ao tratamento de dados pessoais realizados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado, ou atividades de investigação e repressão de infrações penais (art. 4º, III). Desse modo, evidencia se a desnecessidade de consentimento do investigado, 'sob pena de inviabilizar a investigação'" (BRASIL, 2025d, p. 34).
14. Informativo de Jurisprudência 854, com o seguinte destaque: "A prova obtida por meio de cooperação internacional em matéria penal deve ter como parâmetro de validade a lei do Estado no qual foi produzida, nos termos do art. 13 da LINDB, podendo, contudo, não ser admitida no processo em curso no território nacional se o meio de sua obtenção violar a ordem pública, a soberania nacional e os bons costumes brasileiros". O processo tramita

3.2. Jurisprudência do STF

Já em pesquisa ao repositório do STF, com os descritores: "proteção de dados" "e" "criminal", 116 resultados foram obtidos, mas nem todos com relação ao tema. Assim, apenas foram analisados os julgados que, na concepção da autora, possuem relação e/ou são relevantes para com o tema de proteção de dados em âmbito penal.

Quadro 2 – Levantamento de jurisprudência do STF

Especificação do Julgado	Síntese e Informação Relevante na Temática de Proteção de Dados
(2024) ADI 4906, Relator: Nunes Marques, Tribunal Pleno, publicação 24.10.2024 (Brasil, 2024c).	*Compartilhamento de Dados Cadastrais de telefonia com Órgãos de Persecução Criminal.* O STF entendeu, em consonância com o STJ, que o sigilo não alcança dados cadastrais, sendo compatível o compartilhamento direto desses dados com os órgãos de persecução criminal, mesmo sem autorização da justiça. No julgado, o Relator consignou que nome, endereço e filiação não estão acobertados pelo sigilo, eis que não interferem no livre desenvolvimento da personalidade. Além disso, como reforço argumentativo, o Relator argumentou que a LGPD não tem efeito nas atividades de investigação e repressão de infrações penais.
(2023) ADC 51, Relator: Gilmar Mendes, Tribunal Pleno, publicação 28.04.2023 (Brasil, 2023c).	*Cooperação Jurídica Internacional. Obtenção de Dados de Empresas localizadas no exterior. Marco Civil da Internet. Convenção de Budapeste*. O STF analisou o art. 11, do Marco Civil da Internet e o art. 18, da Convenção de Budapeste, em que é "assegurada a aplicação da legislação brasileira em relação a atividades de coleta, armazenamento, guarda e tratamento de registros, dados e comunicações eletrônicas ocorridas em território nacional, desde que pelo menos um dos atos ou terminais se encontram em território nacional, mesmo que a pessoa

em segredo de justiça, mas alguns itens da decisão merecem destaque: (i) que a defesa teve acesso integral ao procedimento formal para trânsito de provas colhidas entre Brasil e França; (ii) que a defesa teve acesso ao *link da nuvem* administrada pela Justiça Federal; (iii) na hipótese de suspeita de que os dados enviados ao Brasil não seriam os mesmos colhidos na França, cabe à defesa demonstrar, ainda que de forma indiciária, em que se basearia tal suspeita; (iv) a cooperação internacional é sustentada na boa-fé das partes envolvidas; (v) em matéria de cooperação internacional penal, vigora o princípio da *lex diligentiae*, nos termos do art. 13, da LINDB; (vi) provas produzidas na França observam as regras lá vigentes e impor leis e regras de outro país viola a soberania do país requerido (BRASIL, 2025a).

Especificação do Julgado	Síntese e Informação Relevante na Temática de Proteção de Dados
	jurídica portadora dessas informações esteja localizada ou guarde informações no exterior". O Relator destacou a necessidade da edição de uma LGPD para Fins Penais.
(2024) ADI 5642, Relator: Edson Fachin, Tribunal Pleno, Publicação 22.08.2024 (Brasil, 2024d).	*Dados cadastrais de vítimas e suspeitos. Discussão sobre a disponibilização de meios técnicos para localização de vítimas e suspeitos. Requisição direta pelo Ministério Público e Delegados de Polícia para órgãos do poder público e empresas privadas.* Análise sobre a constitucionalidade do art. 13-B, caput, do CPP, sobre disponibilização via empresas prestadoras de serviços de telecomunicações e/ou telemática acesso a sinais, informações e outros, que permitam a localização da vítima ou de suspeitos do delito em curso. O STF entendeu que a expressão "dados cadastrais" não inclui a interceptação de voz, telemática, dados cadastrais de usuários de IP, os serviços de agenda virtual, o dado cadastrar de e-mail e extratos de conexão obtidos a partir de linha ou IP. Em conclusão da tese, "São passíveis de requisição sem controle judicial prévio, mas sempre sujeito ao controle judicial posterior, a localização de terminal ou IMEI de cidadão em tempo real por meio de ERB por um período determinado e desde que necessário para os fins de reprimir os crimes contra a liberdade pessoal descritos no art. 13-A do Código de Processo Penal; o extrato de ERB; os dados cadastrais dos terminais fixos não figurantes em lista telefônica divulgável e de terminais móveis; o extrato de chamadas telefônicas; o extrato de mensagens de texto (SMS ou MMS); e os sinais para localização de vítimas ou suspeitos, após o decurso do prazo de 12 horas constante do § 4º do art. 13-B do Código de Processo Penal".
(2006) RE 418416, Relator: Sepúlveda Pertence, Tribunal Pleno, Publicado 19.12.2006 (Brasil, *2006*).	*Busca e apreensão de equipamentos de informática (computadores e disquetes). Apreensão de computadores da empresa e alegação de violação ao sigilo das comunicações de dados.* O STF entendeu que houve a apreensão da base física onde os dados estavam armazenados (computador), o que não se confunde com a interceptação das comunicações, que tem proteção constitucional diversa. A apreensão do computador e a extração de dados foi considerada como algo legal, haja vista que havia sido determinada a apreensão de objetos "interessantes à investigação". Em argumento, constou na ementa que: "Não há violação do art. 5º, XII, da Constituição que, conforme se acentuou na sentença, não se aplica ao caso, pois não houve "quebra

Especificação do Julgado	Síntese e Informação Relevante na Temática de Proteção de Dados
	de sigilo das comunicações de dados (interceptação das comunicações), mas sim apreensão de base física na qual se encontravam os dados, mediante prévia e fundamentada decisão judicial".
(2017) RHC 132062, Relator: Marco Aurélio, Relator(a) p/ Acórdão: Edson Fachin, Publicado 24.10.2017 (Brasil, 2017b).	*Perícia e apreensão de computador.* O caso trata da perícia e apreensão de computador. Nesse caso, discutiu-se a entrega voluntária de um computador, seguida de exame pericial. Além disso, debateu-se a desnecessidade de especificação da apreensão em mandado judicial. No que tange ao sigilo das comunicações, argumentou-se que ele não alcança a troca de dados. Ademais, a Corte considerou que o sigilo das comunicações de dados não é afetado somente pelo acesso das informações armazenadas nos dispositivos eletrônicos.
(2019) Rcl 25872 AgR-AgR, Relatora: Rosa Weber, Primeira Turma, Julgado em 17.12.2019, Publicado 06.03.2020 (Brasil, 2020b).	*Sigilo de dados de terceiros*. Discussão sobre a exclusão de dados de terceiros em inquérito policial, em que a pessoa teve acesso restrito ao Relatório de Inteligência Financeira do COAF. A restrição ocorreu porque havia informações financeiras de outros investigados, tendo por objetivo a proteção de direitos fundamentais de terceiros.
(2021) RE 1055941, Relator: Dias Toffoli, Repercussão Geral (Tema 990) – Mérito *DJe*-243, Publicado 18.03.2021 (Brasil, 2019c).	*Compartilhamento de Relatórios de Inteligência Financeira*. STF entendeu pela desnecessidade de autorização judicial prévia para o compartilhamento de relatórios de inteligência financeira, devendo ser resguardado o sigilo das informações em procedimentos formalmente instaurados e sujeitos a posterior controle judicial[15]. Do tema 9920, surgiram dois entendimentos, um da (i) 1ª Turma (STF. 1ª Turma. Rcl 61.944 AgR, Rel. Min. Cristiano Zanin, julgado em 02.04.2024. STF. 1ª Turma. Rcl 70.191 AgR, Rel. Min. Alexandre de Moraes, julgado em 12.11.2024) e outro da 2ª Turma do STF (STF. 2ª Turma. HC 200.569 AgR, Rel. Min. Cármen Lúcia, Rel. p/Acórdão Min. Gilmar Mendes, julgado em 29.10.2024. STF. 2ª Turma. RE 1.393.219 AgR, Rel. Min. Edson Fachin, julgado em 01.07.2024).

15. Sobre o tema, importante consignar: Estellita (2021).

Especificação do Julgado	Síntese e Informação Relevante na Temática de Proteção de Dados
(2025) HC 252749 ED-AgR, Relator: Cristiano Zanin, Publicação 04.04.2025 (Brasil, 2025f).	*Quebra de sigilo de dados (telefônico e telemático), interceptações telefônicas, de voz, texto, imagens e sons.* Caso em que se discutia a interceptação telefônica e telemática, a última inclui acesso a todo o conteúdo disponível nas plataformas da Google, da Apple, o que inclui acesso a diversos arquivos armazenados em dispositivos informáticos. O entendimento foi o de que a medida é legal, já que a interceptação telefônica é meio de produção de prova prevista na CF.
(2024) ADI 6620, Relator: Alexandre de Moraes, Publicado 20.06.2024 (Brasil, 2023d).	*Legislação mato-grossense que institui o Cadastro de Pedófilos.* Trata-se de análise feita acerca de duas legislações do Estado do Mato Grosso, referente a sistematização de dados de condenados. O STF entendeu pela possibilidade do cadastro, desde que a pessoa seja condenada – com trânsito em julgado. A Ministra Carmen Lúcia destacou em seu voto a ausência de LGPD Penal.
(2023) ADPF 519, Relator: Alexandre de Moraes, Publicação 10.04.2023 (Brasil, 2023e).	*Identificação de veículos qualificação de proprietários. Determinação de bloqueio de contas do Telegram.* Trata-se de análise referente ao processo do Golpe contra o Estado Democrático de Direito. Dentre diversas determinações constantes na decisão importa mencionar a de identificação de todos os veículos utilizados na prática dos atos contra à democracia. Todavia, não se tem notícia no julgado de como a identificação foi realizada. A decisão não conta com nenhuma menção a proteção de dados, mas é um marco importante. Além da ADPF, é importante mencionar que existem outros julgados sobre o Golpe, sendo franqueado o acesso ao dispositivo móvel de investigados, com extração de fotografias, vídeos e outros arquivos.

Fonte: elaborado pela autora.

Em pesquisa com o termo "Convenção de Budapeste", dois resultados foram obtidos: um deles é a ADC 51, de relatoria do Ministro Gilmar Mendes, já mencionada, e o outro se trata do HC 222.141, de relatoria do Ministro Ricardo Lewandowski, sendo oportuno citar a ementa integralmente:

> "Agravos regimentais no habeas corpus. 2. Constitucional, Penal e Processual Penal. 3. Marco civil da Internet. Lei 12.965/2014. Ministério Público. Provedores e plataformas dos registros de conexão e registros de acesso a aplicações de Internet. 4. Congelamento do conteúdo de comunicações privadas e de dados pessoais da paciente, com base no art. 13, § 2º, do Marco Civil da Internet, por

determinação do Ministério Público, sem prévia autorização judicial. Ilegitimidade. 5. A disponibilização de dados pessoais, comunicações privadas ou informações relativas a registros de conexão/acesso está condicionada à determinação do juiz. A exceção fica por conta dos dados cadastrais, que podem ser alcançados por autoridades administrativas devidamente autorizadas por lei. Inteligência do art. 10, caput, e §§ 1º, 2º e 3º, da Lei 12.965/2014. 6. No caso concreto, o pedido de congelamento efetuado pelo GAECO não se limitou aos elementos permitidos pela lei: registros de conexão e de acesso a aplicações de Internet. 7. Em hipótese alguma o 'histórico de pesquisa, todo conteúdo de e-mail e iMessages, fotos, contatos e históricos de localização' podem ser considerados registros de acesso a aplicação de Internet. E mais, o próprio formato da requisição formulada pelo Ministério Público, buscando dados relativos a período que retroage mais de 5 anos, evidencia a desproporcionalidade do pedido e o descompasso entre a diligência efetuada e o permissivo legal. 8. A concepção do direito à privacidade como uma garantia individual de abstenção do Estado na esfera privada individual passou por profundas transformações no decorrer do século XX. Devido ao próprio avanço das tecnologias da informação, assistiu-se a uma verdadeira mutação jurídica do sentido e do alcance do direito à privacidade. A releitura do direito à privacidade coincide com o desenvolvimento jurisprudencial do conceito de autodeterminação informacional (*die informationelle Selbsstbestimmung*) pelo Tribunal Constitucional Alemão. Essa nova abordagem revelou-se paradigmática por ter permitido que o direito à privacidade não mais ficasse estaticamente restrito à frágil dicotomia entre as esferas pública e privada, mas, sim, se desenvolvesse como uma proteção dinâmica e permanentemente aberta às referências sociais e aos múltiplos contextos de uso. 9. A maior abrangência da proteção atribuída ao direito de autodeterminação repercute no âmbito de proteção do direito à proteção de dados pessoais, que não recai sobre a dimensão privada ou não do dado, mas sim sobre os riscos atribuídos ao seu processamento por terceiros. A força normativa do direito fundamental à proteção de dados pessoais decorre da necessidade de proteção da dignidade da pessoa humana, vis-à-vis a contínua exposição dos indivíduos ao risco de comprometimento da autodeterminação informacional. 10. No caso, embora o acesso às informações tenha decorrido de decisão judicial, a própria coleta dos dados, ou congelamento, ocorreu sem a observância dos procedimentos legais. Noutros termos, se é verdade que o sigilo das informações não foi vulnerado sem prévia autorização judicial, também é correto afirmar que o controle da paciente sobre seus dados foi subtraído sem a observância dos procedimentos legais e sem qualquer ordem judicial. 11. Uma vez inserida na equação a autodeterminação informacional, o mero congelamento de dados sem autorização judicial e fora das hipóteses legais afronta a tutela da privacidade. É inconstitucional, portanto, a subtração do controle do cidadão sobre suas informações (congelamento) sem observância das regras de organização e procedimento, ainda que a quebra do sigilo em si tenha

> ocorrido, posteriormente, mediante ordem judicial. 12. É impossível diferenciar a amostragem de dados no momento da coleta – congelamento – daquela que estaria disponível apenas no momento da autorização judicial. A inviabilidade dessa prognose torna imperioso que, para fins de proteção dos dados pessoais, não seja exigido da paciente a comprovação de tentativas de acesso ou modificação do conteúdo. 13. Ao requerer o congelamento fora das hipóteses legais, o Ministério Público pretendeu retirar dados pessoais e comunicações privadas do âmbito de disponibilidade dos investigados. E como tal, a medida afronta não apenas a legislação, como também o direito à autodeterminação informativa. 14. Agravos regimentais não providos. 15. Acórdão redigido nos termos do art. 38, inciso IV, alínea 'b', do RI/STF" (HC 222.141 AgRg, rel. Min. Ricardo Lewandowski, rel. p/acórdão Gilmar Mendes, 2ª T., j. 06.02.2024, Processo eletrônico *DJe*-s/n Divulg 02.04.2024 Public 03.04.2024) (BRASIL, 2024b, p. 1-3).

No julgado, é possível observar que a disponibilização de dados pessoais, de comunicações privadas ou informações relativas a registros de conexão/acesso está condicionada à determinação judicial. Entretanto, dados cadastrais podem ser alcançados pelas autoridades administrativas, conforme entendimento já consolidado do STF e do STJ[16].

Na análise do HC, o STJ considerou desproporcional o acesso de dados com lapso retroativo de cinco anos. O julgado também fez incursões importantes sobre a autodeterminação informacional e ao princípio da proporcionalidade, reconhecendo a nulidade de provas obtidas a partir de dados preservados em contas da internet mediante o requerimento do Ministério Público.

A pesquisa não retornou com o Recurso Extraordinário 1.301.250, tema de Repercussão Geral 1.148, que discutirá os "limites para decretação judicial da quebra de sigilo de dados telemáticos, no âmbito de procedimentos penais, em relação a pessoas indeterminadas" (Brasil, 2025)[17]. De acordo com o Instituto Brasileiro de Ciências Criminais (2023), a medida representa um risco aos direitos coletivos

16. Formulação da tese oficial: "São nulas as provas obtidas a partir de dados preservados em contas da internet (com o congelamento e a consequente perda da disponibilidade), mediante requerimento do Ministério Público, sem a prévia autorização judicial de quebra de sigilo e fora das hipóteses legais" (CAVALCANTE, [s.d.]).

17. O Ministro Alexandre de Moraes abriu divergência e demonstrou indignação com a iniciativa do Google levar o assunto ao Supremo. Segundo o Ministro, as *big techs* têm todas as nossas informações, não existindo um banco de dados maior que o Google. Para ele, impressiona o Google entrar com um mandado de segurança para impedir uma investigação envolvendo o assassinato de uma vereadora sob a alegação de que isso fere a intimidade, quando o Google usa dos mesmos dados para mandar propagandas personalizadas (HIGÍDIO, 2023).

difusos, como o livre desenvolvimento da personalidade e a liberdade de expressão. Para Scalcon e Ferreira (2023), a intervenção nos direitos fundamentais precisa de reserva de lei, não existindo no ordenamento jurídico a previsão para quebra de dados pessoais de pessoas indeterminadas. Atualmente, o feito está com vistas ao Ministro Gilmar Mendes[18].

O levantamento jurisprudencial supradestacado demonstra que o STF teve uma análise mais profunda da temática de proteção de dados, de forma a analisar, ainda que indiretamente, a teoria dos círculos concêntricos mencionada no capítulo interior, a exemplo da decisão de acesso a dados cadastrais.

É comum encontrar na fundamentação dos votos o destaque de que não existe uma LGPD penal e que seria importante a edição de uma norma que desse conta de proteger dados utilizados me proveito de investigações criminais – isso confirma a hipótese inicial da pesquisa, qual seja, a de que é necessário um aprofundamento legislativo que homenageie o direito fundamental à proteção de dados pessoais, inclusive nos meios digitais.

O HC 222.141 também reflete acerca de parâmetros importantes para proteção de dados, haja vista que aborda temas como o da proporcionalidade e da autodeterminação. A autodeterminação, de acordo com o abordado no primeiro capítulo, é elementar para proteção de dados.

18. Decisão: Apregoado o processo, pediu vista antecipada dos autos o Ministro Gilmar Mendes. Nesta assentada, o Ministro Alexandre de Moraes aditou seu voto com proposta de tese (tema 1.148 da repercussão geral) no seguinte sentido: "1) É constitucional a requisição judicial de registros de conexão ou de registros de acesso a aplicativos de internet para fins de investigação criminal ou instrução processual penal, inclusive o fornecimento de dados pessoais por provedores, em cumprimento de medida de busca reversa por palavra-chave, com fundamento no art. 10 e no art. 22 da Lei 12.965/2014 (Marco Civil da Internet), desde que preenchidos os requisitos de (a) fundados indícios de ocorrência do ilícito; (b) motivação da utilidade dos registros solicitados para fins de investigação ou instrução probatória; (c) período ao qual se referem os registros. 2) A ordem judicial poderá se referir a pessoas indeterminadas, mas determináveis a partir de outros elementos de provas, obtidos previamente na investigação e que justifiquem objetivamente a medida, desde que necessária, adequada e proporcional, justificando-se, ainda, a inexistência de outros meios menos invasivos para obter tais informações e a conveniência da medida em relação à gravidade do delito investigado. 3) A determinação judicial conterá, com precisão, os indexadores utilizados para a busca pretendida na base de dados do provedor, devendo a suspeita estar suficiente e formalmente fundamentada, de maneira proporcional. Esses indexadores podem envolver tanto as palavras-chave pesquisadas por indivíduos como determinações geográficas e temporais da busca." Aguardam os demais Ministros. Ausente, ocasionalmente, o Ministro Luís Roberto Barroso (Presidente). Presidiu o julgamento o Ministro Edson Fachin (Vice-Presidente). Plenário, 24.04.2025 (BRASIL, 2025e).

4. Considerações finais

A proteção de dados está intimamente ligada à dignidade da pessoa humana. Proteger dados significa proteger os direitos de personalidade, a autodeterminação e, sobretudo, a democracia.

Na pesquisa, observou-se que ambos os Tribunais reconhecem a importância de norma específica para proteger dados em âmbito penal. No entanto, a ausência de norma reguladora não pode justificar a não proteção do direito em questão, justamente porque se trata de direito fundamental e tem força vinculativa.

No julgamento da Repercussão Geral 1.301.250, o STF debaterá temas importantes: de um lado, o Google, empresa que opera no capitalismo de vigilância, apregoando pela impossibilidade de agências de segurança terem acesso a dados de IPs e *Devices IDs* de um grupo de pessoas que fizeram pesquisas relacionadas com a vereadora Marielle Franco; de outro, a divergência aberta por Alexandre de Moraes, que adverte que a referida empresa já tem acesso a dados pessoais de casa um de nós, utilizando-se de tal superávit comportamental – de acordo com os ensinamentos de Zuboff – para o envio de propaganda personalizada.

Dos ensinamentos expostos na doutrina explorada neste artigo, para se concretizar o direito à proteção de dados, necessita-se de uma série de fatores, que vão desde a justificação disposta em lei formal e de conteúdo determinado, proporcionalidade, separação informacional de poderes/atividades até a vedação de armazenamento de dados em estoque. Além disso, é preciso distinguir normas autorizativas e de competência, o que parece não ocorrer em alguns dos julgados destacados alhures.

Por fim, de acordo com o levantado até a presente data, a pesquisa confirmou sua hipótese inicial, qual seja, a de que é necessário um aprofundamento legislativo e jurisprudencial que homenageie o direito fundamental à proteção de dados pessoais, inclusive nos meios digitais.

Referências

AHMED, Nafeez. How the CIA made Google. *Medium*, 22 jan. 2015. Disponível em: [https://medium.com/insurge-intelligence/how-the-cia-made-google--e836451a959e]. Acesso em: 10.05.2025.

ALBA, Davey. Pentagon taps Eric Schmidt to make it more Google-ish. *Wired*, 2 mar. 2016. Disponível em: [https://wired.com/2016/03/ex-google-ceo--eric-schmidt-head-pentagon-innovation-board/]. Acesso em: 10.05.2025.

AZEVEDO, Cynthia Picolo Gonzaga de; LIMA, Eliz Marina Bariviera de; SILVA, Felipe Rocha da; RODRIGUES, Gustavo Ramos; DUTRA, Luiza Corrêa de Magalhães; SANTARÉM, Paulo Rená da Silva; RODRIGUES,

Victor Barbieri Vieira Rodrigues. *Nota técnica*: análise comparativa entre o anteprojeto de LGPD penal e o PL 1.515/2022. Brasília: Instituto de Referência em Internet e Sociedade (IRIS) e Laboratório de Políticas Públicas e Internet (LAPIN), 2022. Disponível em: [https://lapin.org.br/wp-content/uploads/2022/11/Nota-tecnica-Analise-comparativa-entre-o-anteprojeto-de-LGPD-Penal-e-o-PL-15152022-1.pdf]. Acesso em: 20.06.2025.

BRASIL. STJ, Comissão entrega à Câmara anteprojeto sobre tratamento de dados pessoais na área criminal. *STJ Notícias*, 5 nov. 2020a. Disponível em: [https://stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/05112020-Comissao-entrega-a-Camara-anteprojeto-sobre-tratamento-de-dados-pessoais-na-area-criminal.aspx]. Acesso em: 20.06.2025.

BRASIL. STJ, *Jurisprudência em teses*. 2025b. Disponível em: [https://scon.stj.jus.br/SCON/jt/doc.jsp?tipo=JT&materia=%22DIREITO+PENAL%22.MAT.+NAO+%22DIREITO+PENAL+E+PROCESSUAL+PENAL%22.MAT.&livre=dados&b=TEMA&p=true&thesaurus=JURIDICO&l=20&i=2&operador=E&ordenacao=MAT,@NUM]. Acesso em: 20.05.2025.

BRASIL. STJ, *Jurisprudência em teses*. Versão 4.0.7.39 de 27 ago. 2025c. Disponível em: [https://scon.stj.jus.br/SCON/jt/jt.jsp]. Acesso em: 20.05.2025.

CAMARGO, Rodrigo Oliveira de. *Tratamento de dados, persecução penal e garantia do direito de defesa*. 2022. Tese (Doutorado em Ciências Criminais) – Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2022. Disponível em: [https://tede2.pucrs.br/tede2/bitstream/tede/10605/5/TES_RODRIGO_OLIVEIRA_DE_CAMARGO_COMPLETO.pdf]. Acesso em: 20.06.2025.

CARVALHO, Alexander Perazo Nunes; LIMA, Renata Albuquerque. A eficácia horizontal dos direitos fundamentais, *Revista Opinião Jurídica*. Fortaleza, v. 13, n. 17, p. 11-23, dez. 2015. Disponível em: [https://redalyc.org/articulo.oa?id=633868966002]. Acesso em: 15.06.2025.

CASTELLS, Manuel. *A sociedade em rede*. Trad. Roneide Venancio Majer. 24. ed. Rio de Janeiro: Paz & Terra, 2022.

CAVALCANTE, Márcio André Lopes. São nulas as provas obtidas a partir de dados preservados em contas da internet (com o congelamento e a consequente perda da disponibilidade), mediante requerimento do Ministério Público, sem a prévia autorização judicial de quebra de sigilo e fora das hipóteses legais. *Buscador Dizer o Direito*, [s.d.]. Disponível em: [https://buscadordizerodireito.com.br/jurisprudencia/detalhes/0dd4f2526c7c874d06f19523264f6552]. Acesso em: 20.06.2025.

COURT OF JUSTICE OF THE EUROPEAN UNION. Press Release 70/14: *Judgment in Case C-131/12*: Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González. Luxembourg, 13 may

2014. Disponível em: [https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf]. Acesso em: 20.06.2025.

DONEDA, Danilo. Fundamentos teóricos e históricos da proteção de dados no Brasil. In: DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JÚNIOR, Otávio Luiz (Coords.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021.

ESTELLITA, Heloisa. O RE 1.055.941: um pretexto para explorar alguns limites à transmissão, distribuição, comunicação, transferência e difusão de dados pessoais pelo COAF. *Revista Direito Público*. Brasília, v. 18, n. 100, p. 606-636, 2021. Disponível em: [https://doi.org/10.11117/rdp.v18i100.5991].

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

GAROFANO, Raquel Roque. *Limitação de finalidade no tratamento de dados pessoais pelo público*: teste de legalidade da reutilização para fins de interesse público. Rio de Janeiro: Lumen Juris, 2022.

GLEIZER, Orlandino; MONTENEGRO, Lucas; VIANA, Eduardo. *O direito de proteção de dados no processo penal e na segurança pública*. Rio de Janeiro: Marcial Pons, 2021.

GRECO, Luiz. O inviolável e o intocável no direito processual penal: considerações introdutórias sobre o processo penal alemão (e suas relações com o direito constitucional, o direito de polícia e o direito dos serviços de inteligência). In: WOLTER, Jünger. *O inviolável e o intocável no direito processual penal*: reflexões sobre dignidade humana, proibições de prova, proteção de dados (e separação informacional de poderes) diante da persecução penal. Trad. Alaor Leite e Eduardo Viana. 1. ed. São Paulo: Marcial Pons, 2018.

HIGÍDIO, José. Procurando Marielle: STF suspende caso sobre quebra de sigilo de usuários indeterminados do Google. *Consultor Jurídico*, 28 set. 2023. Disponível em: [https://conjur.com.br/2023-set-28/stf-suspende-quebra-sigilo-usuarios-google/]. Acesso em: 19.06.2025.

INSTITUTO BRASILEIRO DE CIÊNCIAS CRIMINAIS. Habilitação como *amicus curiae*. *Consultor Jurídico*, set. 2023. Disponível em: [https://conjur.com.br/wp-content/uploads/2023/09/parecer-ibccrim1.pdf]. Acesso em: 22.06.2025.

JÚNIOR, Otávio Luiz (Coord.). *Tratado de proteção de dados pessoais*. Rio de Janeiro: Forense, 2021.

LIMA, Cinthia Rosa Pereira de. *Comentários à Lei Geral de Proteção de Dados*: Lei n. 13.709/2018, com alteração da Lei 13.853/2019. São Paulo: Almedina, 2020.

LOPES JR., Aury. *Direito processual penal*. 20. ed. São Paulo: Saraiva Jur, 2023.

MELO, Bricio Luis da. *A submissão obrigatória à identificação de perfil genético para fins criminais*: uma reflexão crítica sob a luz da dignidade da pessoa humana. São Paulo: Letras Jurídicas, 2019.

MENKE, Fabiano. A proteção de dados e o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. *Revista Jurídica Luso-Brasileira*. Lisboa, ano 5, n. 1, p. 781-809, 2019. Disponível em: [http://cidp.pt/revistas/rjlb/2019/1/2019_01_0781_0809.pdf]. Acesso em: 10.06.2025.

MILANEZI, Gabriela. Empresa paga cerca de R$ 500 por escaneamento de íris; entenda como é feito. *CNN Brasil*, 29 jan. 2025. Disponível em: [https://cnnbrasil.com.br/nacional/sudeste/sp/empresa-paga-cerca-de-r-500-por-escaneamento-de-iris-entenda-como-e-feito/]. Acesso em: 20.05.2025.

MILANEZI, Raissa de Cavassin. *Banco de perfil genético e multibiométrico desde a perspectiva da proteção de dados pessoais e do pacote anticrime*. 2024. Dissertação (Mestrado em Direito) – Pontifícia Universidade Católica do Paraná, Curitiba, 2024. Disponível em: [https://pergamum-biblioteca.pucpr.br/acervo/370561]. Acesso em: 20.06.2025.

MILANEZI, Raissa de Cavassin; FREITAS, Cinthia Obladen de Almendra; EFING, Antônio Carlos. Capitalismo de vigilância e os reflexos na sociedade de consumo. *Revista de Direto do Consumidor*, São Paulo, ano 32, v. 148, p. 129-146, jul.-ago. 2023.

MILANEZI, Raissa de Cavassin; RIOS, Rodrigo Sánchez; FREITAS, Cinthia Obladen de Almendra. *Avanço jurisprudencial na cadeia de custódia de prova digital e a Convenção de Budapeste sobre Cibercrime*. Conselho Nacional de Pesquisa e Pós-Graduação em Direito, 2023. Disponível em: [https://site.conpedi.org.br/publicacoes/w7dsqk3y/43wvq0a2/7vou9T9Iu2Jb8xUY.pdf]. Acesso em: 15.06.2025.

MITIDIERO, Daniel; MARINONI, Luiz Guilherme; SARLET, Ingo Wolfgang. *Curso de direito constitucional*. 12. ed. São Paulo: SaraivaJur, 2023.

PEREIRA, Leonardo Fadul. Representatividade democrática: o protagonismo judicial em questão. In: BASTOS, Elísio Augusto Velloso; MERLIN, Lise Tupiassu; CICHOVSKI, Patrícia Blagitz (Orgs.). *Constitucionalismo e direitos fundamentais*. São Paulo: Gen, 2014.

PINHEIRO, Patrícia Peck. *Proteção de dados pessoais*: comentários à Lei 13.709/2018. 2. ed. São Paulo: Saraiva Educação, 2020.

PIRES, Ana Beatriz Santos et al. Alvos predeterminados: um estudo de caso sobre a implementação da tecnologia de reconhecimento facial na Bahia. In: ALMEIDA, Eloísa Machado de; ESTELLITA, Heloisa (Coords.). *Dados, privacidade e persecução penal*: cinco estudos. São Paulo: FGV Direito, 2021.

Disponível em: [https://repositorio.fgv.br/server/api/core/bitstreams/29256984-be0c-4f94-8bab-ff178c503bc7/content]. Acesso em: 20.06.2025.

SARLET, Ingo Wolfgang. *Privacy and Data Protection Magazine*, 2021. Disponivel em: [https://europeia.pt/content/files/pdpm_04_06_02.pdf]. Acesso em: 10.05.2025.

SCALCON, Raquel; FERREIRA, André da Rocha. O problema da quebra coletiva de sigilo de dados pessoais contra pessoas indeterminadas. *Boletim IBCCRIM*, São Paulo, v. 31, n. 370, set. 2023. Disponível em: [https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/682/139]. Acesso em: 23.06.2025.

SCHWABE, Jürgen; MARTINS, Leonardo. *Cinquenta anos de jurisprudência do Tribunal Constitucional Federal alemão*. Direito Constitucional Material I (Direitos Fundamentais – Art. 1-19 GG). Montevideo: Konrad-Adenauer-Stiftung, 2005. Disponível em: [https://kas.de/c/document_library/get_file?uuid=c0b3d47d-beba-eb55-0b11df6c530ddf52&groupId=252038]. Acesso em: 15.05.2025.

SPONHOLZ, Marina Schmidlin. *Autodeterminação informacional e* blockchain *como contribuições do direito e da tecnologia para o fortalecimento da cooperação cooperativa*. 2024. Dissertação (Mestrado em Direito) – Pontifícia Universidade Católica do Paraná, Curitiba, 2024. Disponível em: [https://pergamum-biblioteca.pucpr.br/acervo/370110]. Acesso em: 15.05.2025.

TOTAL INFORMATION AWARENESS. In: WIKIPEDIA. Wikimedia, 2025. Disponível em: [https://en.wikipedia.org/w/index.php?title=Total_Information_Awareness&oldid=1306250707]. Acesso em: 20.05.2025.

WOLTER, Jünger. *O inviolável e o intocável no direito processual penal* – Reflexões sobre dignidade humana, proibições de prova, proteção de dados (e separação informacional de poderes) diante da persecução penal. Trad. Alaor Leite e Eduardo Viana. 1. ed. São Paulo: Marcial Pons, 2018.

ZUBOFF, Shoshana. *Capitalismo de vigilância*. Tradução de George Schlesinger. 1. ed. Rio de Janeiro: Intrínseca, 2020.

Legislação

BRASIL. Anteprojeto da Comissão de Proteção Dados Segurança e Persecução. Brasília: Câmara dos Deputados, 2019a. Disponível em: [https://camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/documentos/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf]. Acesso em: 10.01.2024.

BRASIL. Lei 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, 14.08.2018. *DOU* 15.08.2018. Disponível em:

[https://planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm]. Acesso em: 20.06.2025.

BRASIL. Projeto de Lei 1.515/2022. 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. Brasília: Câmara dos Deputados, 2022. Disponível em: [https://camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2326300#tramitacoes]. Acesso em: 20.06.2025.

Jurisprudência

BRASIL. STF, ADC 51/DF, rel. Min. Gilmar Mendes, TP, j. 23.02.2023c, *DJe* 07.03.2023. Disponível em: [https://stf.jus.br/arquivo/cms/bibliotecaConsultaProdutoBibliotecaPastaFachin/anexo/ADC51.pdf]. Acesso em: 20.05.2025.

BRASIL. STF, ADI 4.906/DF, rel. Min. Nunes Marques, TP, j. 11.09.2024c, *DJe* 11.09.2024. Disponível em: [https://portal.stf.jus.br/jurisprudencia/obterInteiroTeor.asp?idDocumento=781424127]. Acesso em: 20.05.2025.

BRASIL. STF, ADI 5.642/DF, rel. Min. Edson Fachin, TP, j. 18.04.2024d. Disponível em: [https://portal.stf.jus.br/processos/detalhe.asp?incidente=5117846]. Acesso em: 20.05.2025.

BRASIL. STF, ADI 6.620/MT, rel. Min. Alexandre de Moraes, TP, 20.06.2023d. Disponível em: [https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=777837648]. Acesso em: 20.05.2025.

BRASIL. STF, ADPF 519/DF, rel. Min. Alexandre de Moraes, TP, 12 jan. 2023e. Disponível em: [https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=766769007]. Acesso em: 20.05.2025.

BRASIL. STF, AgRg em AgRg na Recl. 25.872/SP, rel. Min. Rosa Weber, TP, j. 17.12.2019, publicado: 06.03.2020b. Disponível em: [https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=752160014]. Acesso em: 20.05.2025.

BRASIL. STF, AgRg nos EDcl no HC 252.749/PR, rel. Min. Cristiano Zanin, 1ª T., j. 31.03.2025f. Disponível em: [https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=785785396]. Acesso em: 20.05.2025.

BRASIL. STF, RE 418.416-8/SC, rel. Min. Sepúlveda Pertence, TP, j. 10.05.2006. Disponível em: [https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=395790]. Acesso em: 20.05.2025.

BRASIL. STF, RE 1.055.941/SP – RG – Mérito (Tema 990), rel. Min. Dias Toffoli, TP, 04.12.2019c. Disponível em: [https://portal.stf.jus.br/jurisprudencia/obterInteiroTeor.asp?idDocumento=755364496]. Acesso em: 20.05.2025.

BRASIL. STF, RE 1.301.250/RJ – RG, rel. Min. Rosa Weber, vista à Ministra (Min. Gilmar Mendes), TP, 24.04.2025e. Disponível em: [https://portal.stf.jus.br/processos/detalhe.asp?incidente=6059876]. Acesso em: 20.05.2025.

BRASIL. STF, RO em HC 132.062/RS, rel. Min. Marco Aurélio, red. do Ac. Min. Edson Fachin, 1ª T., j. 22.11.2016, *DJe* 24.10.2017b. Disponível em: [https://portal.stf.jus.br/jurisprudencia/obterInteiroTeor.asp?idDocumento=13902497]. Acesso em: 20.05.2025.

BRASIL. STJ, AgRg no HC 828.054/RN, rel. Min. Joel Ilan Paciornik, 5ª T., j. 23.04.2024, *DJe* 29.04.2024a. Disponível em: [https://processo.stj.jus.br/SCON/pesquisar.jsp?i=1&b=ACOR&livre=(%27AGRHC%27%20INPATH(CLAS)%20AND%20%27828054%27%20INPATH(NUM))%20OR%20((%27AgRg%20no%20HC%20828054%27)%20INPATH(SUCE))&thesaurus=JURIDICO&fr=veja]. Acesso em: 20.06.2025.

BRASIL. STJ, CC 197.030/AM, rel. Min. Laurita Vaz, 14.06.2023b. Disponível em: [https://processo.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202301896150&dt_publicacao=29/04/2024]. Acesso em: 19.05.2025.

BRASIL. STJ, EDcl no AgRg no AREsp 874.820/RJ, rel. Min. Nefi Cordeiro, 14.11.2017a. Disponível em: [https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1853787&num_registro=201900409400&data=20190905&peticao_numero=201900335018&formato=PDF]. Acesso em: 20.05.2025.

BRASIL. STJ, HC 222.141/PR, rel. Min. Ricardo Lewandowski, j. 06.02.2024. *DJe* 03.04.2024b. Disponível em: [https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=775652964]. Acesso em: 20.05.2025.

BRASIL. STJ, RHC 143.169/RJ, rel. Min. Messod Azulay Neto, 5ª T., *DJe* 02.03.2023a.

BRASIL. STJ, Processo em segredo de justiça, rel. Min. Rogerio Schietti Cruz, 6ª T., por unanimidade, j. 06.05.2025, *DJ* 19.05.2025a.

BRASIL. STJ, REsp 1.795.908/PE, rel. Min. Nefi Cordeiro, 6ª T., j. 21.05.2019, *DJe* 03.06.2019b. Disponível em: [https://processo.stj.jus.br/processo/pesquisa/?num_registro=201900409400]. Acesso em: 20.05.2025.

BRASIL. STJ, REsp 1.955.981/GO, rel. Min. Nancy Andrighi, CE, 06.02.2025d. Disponível em: [https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202101326250&dt_publicacao=06/02/2025]. Acesso em: 20.05.2025.

Autora convidada



PESQUISA DO EDITORIAL



Área do Direito: Digital; Penal

Veja também Doutrina relacionada ao tema

- Direito penal e proteção de dados pessoais: uma leitura dialógica a partir da Lei 13.709/18 e do direito do consumidor, de Mariana Battochio Stuart e Victor Augusto Estevam Valente – *RDC* 140/333-357;
- Proteção de dados e responsabilidade criminal: um exame de perspectiva comparada, de Filipe Lovato Batich e Rhasmye El Rafih – *BRTO* 37;
- Proteção dos dados pessoais como direito fundamental: a evolução da tecnologia da informação e a Lei Geral de Proteção de Dados no Brasil, de Gianfranco Faggin Mastro Andréa, Higor Roberto Leite Arquite e Juliana Moreira Camargo – *RDCI* 121/115-139; e
- Tratamento de dados pessoais em investigações criminais: o direito fundamental à autodeterminação informativa como limite constitucional, de André da Rocha Ferreira – *RBCCrim* 185/115-159.

Veja também Jurisprudência relacionada ao tema

- STF, ADIn 4906, j. 11.09.2024, *DJe* 24.10.2024;
- STF, ADIn 5642, j. 18.04.2024, *DJe* 22.08.2024;
- STF, ADIn 6620, j. 18.04.2024, *DJe* 20.06.2024;
- STJ, AgRg no HC 828054, j. 23.04.2024, *DJe* 29.04.2024; e
- STJ, AgRg no RO em HC 143169, j. 07.02.2023, *DJe* 02.03.2023.

Veja também Legislação relacionada ao tema

- Lei 13.709/2018.

Índice Alfabético-remissivo

AUTORES

A

AMARAL, Augusto Jobim do
– Reconhecimento facial: biopolítica granular e controle customizado no Brasil, p. 143

ANDREATTA, Samuel
– A coleta de dados em larga escala e as possibilidades críticas de direito comparado: sistema de dupla proteção, p. 203

B

BELIATO, Araceli Martins
– O uso da inteligência artificial na predição do feminicídio e o direito à explicabilidade e à autodeterminação informativa, p. 169

C

CALLEGARI, André Luís
– Da nuvem à corte: o julgamento constitucional da prova penal invisível, p. 25

CANI, Luiz Eduardo
– Compartilhamento de dados financeiros na persecução penal, p. 51

D

DUMONT, Paola Alcântara Lima
– Técnicas antiforenses: obstrução da justiça ou garantia da defesa?, p. 227

G

GIAMPAOLI, Anderson Pires
– Devida investigação criminal: compromissos epistêmicos e probatórios na extração de dados pessoais em fontes abertas, p. 115

L

LIMA, Thallita Gabriele Lopes
– *Faces make cases:* o caso *Clearview AI* e os desafios do uso de tecnologias algorítmicas no sistema de justiça criminal brasileiro, p. 85

M

MENDES NETO, José Guimarães
– Da nuvem à corte: o julgamento constitucional da prova penal invisível, p. 25

MORAES, Rafael Francisco Marcondes de
– Devida investigação criminal: compromissos epistêmicos e probatórios na extração de dados pessoais em fontes abertas, p. 115

SILVA, Roberta de Lima e
– Devida investigação criminal: compromissos epistêmicos e probatórios na extração de dados pessoais em fontes abertas, p. 115

S

SARKIS, Jamilla Monteiro
– Técnicas antiforenses: obstrução da justiça ou garantia da defesa?, p. 227

T

TRAVASSOS, Gabriel Saad
– Reconhecimento facial: biopolítica granular e controle customizado no Brasil, p. 143

TEMAS

A

AI – *Faces make cases*: o caso *Clearview AI* e os desafios do uso de tecnologias algorítmicas no sistema de justiça criminal brasileiro, p. 85

Anátomo-política – Reconhecimento facial: biopolítica granular e controle customizado no Brasil, p. 143

Autodeterminação informacional

– Da nuvem à corte: o julgamento constitucional da prova penal invisível, p. 25

– Dossiê "proteção de dados pessoais e ciências criminais": prólogo de uma formação jurídico-penal, p. 11

B

Biopoder – Reconhecimento facial: biopolítica granular e controle customizado no Brasil, p. 143

Biopolítica granular – Reconhecimento facial: biopolítica granular e controle customizado no Brasil, p. 143

C

Cadeia de custódia – Devida investigação criminal: compromissos epistêmicos e probatórios na extração de dados pessoais em fontes abertas, p. 115

Cibercriminalidade – Dossiê "proteção de dados pessoais e ciências criminais": prólogo de uma formação jurídico-penal, p. 11

Clearview – *Faces make cases*: o caso *Clearview AI* e os desafios do uso de tecnologias algorítmicas no sistema de justiça criminal brasileiro, p. 85

Coleta de dados em larga escala – A coleta de dados em larga escala e as possibilidades críticas de direito comparado: sistema de dupla proteção, p. 203

Compartilhamento de provas – Compartilhamento de dados financeiros na persecução penal, p. 51

Convenção de Budapeste – Análise jurisprudencial dos tribunais superiores no campo da proteção de dados pessoais em âmbito penal, p. 277

Criminologia crítica – A coleta de dados em larga escala e as possibilidades críticas de direito comparado: sistema de dupla proteção, p. 203

D

Dados pessoais – *Faces make cases*: o caso *Clearview AI* e os desafios do uso de tecnologias algorítmicas no sistema de justiça criminal brasileiro, p. 85

Devida investigação criminal – Devida investigação criminal: compromissos epistêmicos e probatórios na extração de dados pessoais em fontes abertas, p. 115

Direito fundamental à proteção de dados – Análise jurisprudencial dos tribunais superiores no campo da proteção de dados pessoais em âmbito penal, p. 277

E

Eficiência investigativa – Da nuvem à corte: o julgamento constitucional da prova penal invisível, p. 25

Epistemologia – Devida investigação criminal: compromissos epistêmicos e probatórios na extração de dados pessoais em fontes abertas, p. 115

F

Feminicídios – O uso da inteligência artificial na predição do feminicídio e o direito à explicabilidade e à autodeterminação informativa, p. 169

Fontes abertas – Devida investigação criminal: compromissos epistêmicos e probatórios na extração de dados pessoais em fontes abertas, p. 115

Formação jurídica – Dossiê "proteção de dados pessoais e ciências criminais": prólogo de uma formação jurídico-penal, p. 11

G

Garantia de defesa – Técnicas antiforenses: obstrução da justiça ou garantia da defesa?, p. 227

Garantias fundamentais – Da nuvem à corte: o julgamento constitucional da prova penal invisível, p. 25

Governamentalidade algorítmica – Reconhecimento facial: biopolítica granular e controle customizado no Brasil, p. 143

J

Jurisprudência penal – Análise jurisprudencial dos tribunais superiores no campo da proteção de dados pessoais em âmbito penal, p. 277

Justiça criminal – *Faces make cases*: o caso *Clearview AI* e os desafios do uso de tecnologias algorítmicas no sistema de justiça criminal brasileiro, p. 85

L

LGPD Penal – Análise jurisprudencial dos tribunais superiores no campo da proteção de dados pessoais em âmbito penal, p. 277

O

Obstrução de Justiça – Técnicas antiforenses: obstrução da justiça ou garantia da defesa?, p. 227

Opacidade – O uso da inteligência artificial na predição do feminicídio e o direito à explicabilidade e à autodeterminação informativa, p. 169

P

Privacidade – O uso da inteligência artificial na predição do feminicídio e o direito à explicabilidade e à autodeterminação informativa, p. 169

Processo penal

– Compartilhamento de dados financeiros na persecução penal, p. 51

– Dossiê "proteção de dados pessoais e ciências criminais": prólogo de uma formação jurídico-penal, p. 11

Proteção de dados

– Compartilhamento de dados financeiros na persecução penal, p. 51

– Reconhecimento facial: biopolítica granular e controle customizado no Brasil, p. 143

Prova digital – Devida investigação criminal: compromissos epistêmicos e probatórios na extração de dados pessoais em fontes abertas, p. 115

R

Reconhecimento facial

– *Faces make cases*: o caso *Clearview AI* e os desafios do uso de tecnologias algorítmicas no sistema de justiça criminal brasileiro, p. 85

– Reconhecimento facial: biopolítica granular e controle customizado no Brasil, p. 143

Relatório de inteligência financeira – Compartilhamento de dados financeiros na persecução penal, p. 51

Representação fiscal para fins penais – Compartilhamento de dados financeiros na persecução penal, p. 51

S

Segurança jurídica – Da nuvem à corte: o julgamento constitucional da prova penal invisível, p. 25

Sigilo médico – O uso da inteligência artificial na predição do feminicídio e o direito à explicabilidade e à autodeterminação informativa, p. 169

T

Técnicas antiforenses – Técnicas antiforenses: obstrução da justiça ou garantia da defesa?, p. 227

Tecnologia – A coleta de dados em larga escala e as possibilidades críticas de direito comparado: sistema de dupla proteção, p. 203

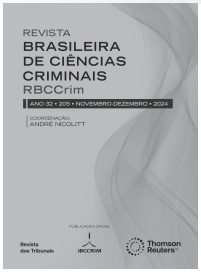
Tecnologias de vigilância – *Faces make cases*: o caso *Clearview AI* e os desafios do uso de tecnologias algorítmicas no sistema de justiça criminal brasileiro, p. 85

V

Vigilância algorítmica – Dossiê "proteção de dados pessoais e ciências criminais": prólogo de uma formação jurídico-penal, p. 11

Vigilância digital – Da nuvem à corte: o julgamento constitucional da prova penal invisível, p. 25

Normas de Publicação – *Revista Brasileira de Ciências Criminais*



Política editorial determinada pela equipe editorial em conformidade com o conselho editorial da RBCCRIM, sujeita à revisão periódica.

1. Dados gerais do periódico

- **Nome**: *Revista Brasileira de Ciências Criminais (RBCCRIM)*
- **Responsável**: Instituto Brasileiro de Ciências Criminais (IBCCRIM)
- **Formato**: impresso (Editora Thomson Reuters)
- **Ano de criação**: 1992 (sem interrupções)
- **Periodicidade**: bimestral
- **Recebimento de manuscritos**: fluxo contínuo e editais especiais
- **ISSN**: 1415-5400
- ***Qualis***: A1

2. Linha editorial:

A *Revista Brasileira de Ciências Criminais* visa à publicação de **trabalhos científicos** relacionados às **ciências criminais**, essencialmente compreendidas entre as áreas de Direito Penal, Direito Processual Penal e Criminologia, além de seus pontos de transdisciplinaridade com outras esferas do conhecimento, como a psicologia, a medicina, a antropologia, a sociologia etc.

Com o objetivo de abranger tal escopo editorial, o periódico é dividido nas seguintes **seções**:

a) *Direito Penal*: abrangendo Teoria Geral, Parte Especial, Legislação Penal Especial e Direito Penal Econômico;

b) *Processo Penal;*

c) *Crime e Sociedade;*

Ademais, a *RBCCRIM*, almejando a interlocução entre a estruturação de uma sólida doutrina nas ciências criminais e seu impacto na prática judicial, também publica **comentários críticos a decisões jurisprudenciais**, preferencialmente aquelas emanadas dos tribunais superiores e internacionais. Tais contribuições integram a seção *Direito em Ação* – Comentário

Jurisprudencial. Além disso, também são publicados **Pareceres** acerca da aplicação prática de teorias relevantes às ciências criminais.

Por fim, visando à divulgação de importantes trabalhos científicos publicados em âmbito nacional e internacional, especialmente pesquisas acadêmicas, há a seção **Resenhas Críticas,** em que se apresentam breves comentários a tais publicações, ensejando críticas e incentivo ao debate científico. Ocasionalmente, também serão admitidas e publicadas **entrevistas** avaliadas pela coordenação como relevantes à promoção do debate científico concernente ao escopo do periódico.

3. Regras para submissão

O envio dos trabalhos deverá ser feito por meio de cadastramento direto no sistema (OJS): https://publicacoes.ibccrim.org.br/index.php/RBCCRIM/index . Recomenda-se a utilização de processador de texto Microsoft Word (formatos doc.). Caso seja usado outro processador de texto, os arquivos devem ser gravados no formato RTF (de leitura comum a todos os processadores de texto).

3.1. Condições para submissão

a) É exigida **titulação mínima de mestrado (de autores e coautores)** para submissão de artigos ao processo de avaliação.

b) O artigo deve ser inédito; portanto, não publicado em nenhum outro periódico científico e/ou canais de comunicação. Vale ressaltar que ineditismo não deve ser confundido com originalidade, podendo o tema tratado pelo artigo já ter sido abordado por outros autores(as) e/ou publicações;

c) Todos os artigos serão submetidos à inspeção com programa antiplágio. Não são considerados inéditos os textos: divulgados na *internet*; já publicados no exterior (ainda que em outra língua); publicados em anais de eventos científicos. Serão considerados inéditos os artigos que consistam em versões reduzidas de dissertações de mestrado ou teses de doutorado, embora publicados integralmente em bancos de teses de programas de pós-graduação, e os publicados anteriormente em anais de eventos científicos, mas que apresentem efetivos aprimoramentos em razão de debates e estudos posteriores (destacar tais modificações à equipe editorial no e-mail da submissão). Alterações não justificadas em trabalhos já publicados só serão toleradas até o limite de 30% de coincidência de caracteres.

d) Assim, em qualquer das hipóteses acima referidas, quando trabalho idêntico ou substancialmente semelhante tiver sido publicado pelo autor em outro veículo de comunicação, ainda que em outro idioma, esse fato deve ser declarado expressamente no texto e informado ao editor no momento da submissão, **sob pena de proibição de novas submissão pelo período de um ano**.

e) Traduções de artigos também poderão ser submetidas à apreciação do periódico, desde que acompanhadas da autorização de seus respectivos autores e, quando necessário, do

periódico que detenha seus direitos de publicação. No entanto, a decisão sobre a sua publicação ou não será prerrogativa da coordenação da *Revista*.

f) Uma vez submetido um artigo para avaliação, objetivando sua possível publicação, é vedada a submissão simultânea do mesmo trabalho a outro periódico ou publicação, sob pena de impedimento de submissão de novos trabalhos a este periódico pelo período de um ano;

g) Após o recebimento e cadastramento do trabalho, entraremos em contato para acusar a recepção e solicitar eventuais informações faltantes.

4. Elementos formais obrigatórios

a) Os artigos deverão ser precedidos de uma página de apresentação, na qual se fará constar obrigatoriamente: título do trabalho, nome do autor (ou autores), qualificação (situação acadêmica, títulos com ano de obtenção, instituições às quais pertença e a principal atividade exercida), endereço completo para correspondência, telefone, e-mail, link para o currículo LATTES e número do ORCID.

b) Os trabalhos devem ter entre 20 e 40 páginas, com tolerância de duas para mais ou duas para menos; e resenhas críticas (até 15 páginas). Os parágrafos devem ser justificados. Não devem ser usados recuos, deslocamentos, nem espaçamentos antes ou depois.

c) Como fonte, **usar a Times New Roman, corpo 12. Os parágrafos devem ter entrelinha 1,5; as margens superior e inferior 2,0 cm e as laterais 3,0 cm**. A formatação do tamanho do papel deve ser A4.

d) Os parágrafos devem ser justificados. Não devem ser usados deslocamentos, nem espaçamentos antes ou depois de cada tópico; devem ter entrelinha 1,5; as margens superior e inferior 2,0 cm e as laterais 2,5 cm. A formatação do tamanho do papel deve ser A4.

e) Os trabalhos podem ser escritos em português, espanhol, inglês, francês, alemão ou italiano. Em qualquer caso, **deverão ser indicados, no idioma do artigo e em inglês, o título do trabalho, o respectivo resumo (até 200 palavras) e cinco palavras-chave.**

f) Os artigos devem possuir os seguintes elementos em português e inglês: título/*title*; resumo/*abstract*; palavras-chave/*keywords*; sumário (apenas em português ou na língua original do artigo).

g) A numeração do sumário deverá obrigatoriamente ser feita em algarismos arábicos. É vedada a numeração dos itens em algarismos romanos. No sumário deverão constar os itens com até três dígitos. Exemplo:

Sumário: 1. Introdução – 2. Responsabilidade civil ambiental: legislação: 2.1 Normas clássicas; 2.2 Inovações: 2.2.1 Dano ecológico; 2.2.2 Responsabilidade civil objetiva. Considerações finais. Referências.

h) Os artigos deverão conter itens específicos para introdução, considerações finais (conclusões) e referências.

i) A *Revista Brasileira de Ciências Criminais (RBCCrim)* não se responsabilizará por realizar qualquer complemento nos trabalhos, tais como inserção de sumário, resumo ou palavras-chave, que ficam à elaboração exclusiva do autor do artigo.

j) O título do artigo não deverá ser excessivamente extenso, mas necessariamente precisa apresentar de modo claro a temática e a delimitação de seu objeto.

k) A qualificação/afiliação do(s) autor(es) deve obedecer ao seguinte critério: iniciar com a titulação acadêmica (da última para a primeira); caso exerça o magistério, inserir os dados pertinentes, logo após a titulação; em seguida, completar as informações adicionais (associações ou outras instituições de que seja integrante e seu respectivo estado da federação e a cidade); finalizar com a função ou profissão exercida (que não seja na área acadêmica). Deverá ser indicado e-mail para contato. Exemplo:

   Doutor em Direito Processual Penal pela PUC-SP. Professor em Direito Processual Penal na Faculdade de Direito da USP. Membro do IBDP. Juiz Federal em Londrina. ORCID. E-mail.

l) Solicita-se que o autor informe em nota de rodapé qualquer financiamento ou benefícios recebidos de fontes comerciais (por ex., se o artigo é fruto de parecer contratado), e que declare não haver conflito de interesses que comprometam a cientificidade do trabalho apresentado. Se o trabalho for resultante de pesquisas financiadas por órgãos de fomento (desconsiderar bolsas de iniciação científica, mestrado e doutorado ou de editais destinados aos programas como o PROEX, PROAP, PROSUP e versões semelhantes dos órgãos estaduais de fomento), deverá haver tal informação em nota de rodapé, especificando o edital de que resulta o financiamento.

m) As Referências deverão seguir o padrão da norma NBR 6023/2018 (da Associação Brasileira de Normas Técnicas – ABNT). As referências bibliográficas completas deverão constar apenas da lista de REFERÊNCIAS, ao final do texto. Exemplo: PEREIRA, Frederico V. *Delação premiada*: legitimidade e procedimento. 3. ed. Curitiba: Juruá, 2016. p. 45. Em notas de rodapé não se inclui a referência completa, podendo-se utilizar do modelo autor/data/página. Esse mesmo modelo deverá ser utilizado no corpo do texto, quando de citações de trechos de obras, devendo a informação vir entre parênteses. Exemplos: PEREIRA, 2016, p. 45, quando em notas de rodapé; e (PEREIRA, 2016, p. 45), quando no corpo do texto.

n) Palavras em língua estrangeira devem constar com uso de *itálico*. Jamais deve ser usado negrito ou sublinhado.

o) Citações diretas (transcrição textual de parte da obra de autor consultado) no corpo do texto devem seguir a norma NBR 1052 (ABNT/2002), ou seja:

   – Citações diretas de até três linhas devem estar contidas entre aspas duplas, no corpo do parágrafo a que se referem. Exemplo: Barbour (1971, p. 35) descreve: "O estudo da morfologia dos terrenos [...] ativos[...]". OU: "Não se mova, faça de conta que está morta." (CLARAC; BONNIN, 1985, p. 72)

– Citações diretas de mais de três linhas devem ser destacadas do texto, com recuo de 4 cm da margem esquerda, com letra menor (corpo 10) que a utilizada no texto corrido, espaçamento simples entre as linhas e sem aspas.

> A teleconferência permite ao indivíduo participar de um encontro nacional ou regional sem a necessidade de deixar seu local de origem. Tipos comuns de teleconferência incluem o uso da televisão, telefone e computador. Através de audioconferência, utilizando a companhia local de telefone, um sinal de áudio pode ser emitido em um salão de qualquer dimensão. (NICHOLS, 1993, p. 181).

p) As referências legislativas ou jurisprudenciais devem conter todos os dados necessários para sua adequada identificação e localização. Em citações de sites de internet deve-se indicar o *link*, introduzido pela expressão "Disponível em:" e a data de acesso, precedida da expressão "Acesso em:". As datas devem seguir o padrão de abreviação universal ABNT. Exemplo: 20 ago. 2012; 15 set. 2018; 22 mar. 2019 etc.

q) Sugere-se que esquemas, organogramas, tabelas e gráficos sejam inseridos no texto por meio de imagens, de modo a evitar distorções na posterior diagramação.

5. Cientificidade

Os artigos deverão apresentar caráter científico, definindo e esclarecendo um ou mais problemas específicos, sumarizando os estudos prévios sobre a temática e informando aos leitores o estado em que se encontra uma determinada área de investigação. Além disso, o trabalho deve buscar identificar relações, contradições, lacunas e inconsistências na literatura e indicar sugestões para a resolução dos problemas identificados.

Preferencialmente, serão publicados artigos que apresentem contribuição inédita e efetiva às ciências criminais, a partir de referências sólidas e/ou pesquisa empírica inédita. Assim, o trabalho deverá ser uma fonte confiável para o leitor conhecer o estado atual de cada área acerca da temática abordada, é necessária a referência a todas as informações nele inseridas e, ainda, precisam ser identificados e justificados os métodos de correção estatística que eventualmente sejam utilizados.

5.1. Pressupostos de Integridade Ética em Pesquisa

a) Autoria: Todas as pessoas que contribuíram para a pesquisa devem ser indicadas. Cada autor deve ter participado suficientemente do trabalho para poder assumir publicamente a responsabilidade pelo seu conteúdo. Sua participação deve incluir: a) a concepção ou delineamento ou ainda análise e interpretação dos dados, ou ambos; b) redação do manuscrito ou sua revisão, quando inclua critica intelectual importante

de seu conteúdo; c) aprovação final da versão a ser publicada. A simples participação na coleta de dados não justifica autoria.[1]

b) Coautoria: Quando se tratar da publicação de resultados obtidos por meio de pesquisa coletiva, é preciso certificar-se da contribuição intelectual direta e efetiva e do consentimento de todos os colaboradores. A cessão de recursos financeiros e de infraestrutura não é indicação de coautoria.

c) Vedação de Plágio: Quando uma ideia ou uma formulação utilizada no trabalho não sejam evidentemente de domínio público na área de pesquisa em questão, presume-se que se trata de contribuição original. Se não for esse o caso, a ideia ou formulação devem ser expressamente creditadas, sob pena de plágio.

d) Vedação de Autoplágio: Quando trabalho idêntico ou substancialmente semelhante tiver sido publicado em outro veículo de comunicação, ainda que em outro idioma, esse fato deve ser declarado expressamente no texto e informado ao editor no momento da submissão. A falta de menção expressa a esse fato caracterizará o autoplágio.

e) Responsabilidade: O autor ou, quando for o caso, cada um dos autores é responsável pela qualidade do trabalho como um todo, a menos que os limites de sua contribuição sejam indicados de modo expresso e preciso.

f) Termo de consentimento livre e esclarecido (TCLE): Sempre que, em virtude do objeto ou outras circunstâncias de pesquisa, for possível a identificação dos entrevistados, será exigida a apresentação de TCLE dos entrevistados que puderem ser identificados.

g) Conflito de interesses: quando houver possível conflito de interesses, os autores devem informar a equipe editorial no ato da submissão do trabalho. Os editores decidirão sobre a configuração de conflito de interesses avaliando se a cientificidade da obra foi comprometida.

h) Responsabilidade com Dados

- Fontes: Sempre que se faz referência a dados, é necessário que sejam apontadas as suas fontes.
- Termo de Confidencialidade: Sempre que um trabalho fizer uso de dados obtidos através de TC, é preciso que os autores enviem o termo no ato da submissão do trabalho para que se possa apurar sua observância.
- Manipulação: Sempre que se utilizarem métodos de correção estatística, estes devem ser identificados e justificados.

1. MONTENEGRO, Mario R.; ALVES, Venâncio A. Ferreira. Critérios de autoria e coautoria em trabalhos científicos. Acta boT. bras. 11 (2): 1997. Acesso em: 25 abr. Disponível em: [http://www.scielo.br/pdf/abb/v11n2/v11n2a14.pdf].

5.2. Responsabilidade editorial

a) O parecer cego deve ser feito com rigor, objetividade, imparcialidade e presteza. O interesse em realizar a melhor avaliação deve prevalecer em face de outros interesses, como o cumprimento estrito de prazos estipulados. As divergências de juízos não devem ser tomadas como razões suficientes para a emissão de parecer desfavorável.

b) O revisor deve tratar com confidencialidade e não fazer uso próprio das informações a que tenha tido acesso no exercício de sua função de avaliador.

c) O revisor deverá abster-se de sua função de avaliador, por potencial conflito de interesse, quando mantiver colaboração científica regular, em atividade de pesquisa, publicação, orientação ou tutoria, ou quando tiver relação familiar ou afetiva com algum dos pesquisadores responsáveis pela proposta submetida à sua avaliação.

d) Todos os casos em que se verificarem violações de natureza ética serão devidamente apurados pela coordenação da *Revista Brasileira de Ciências Criminais (RBCCrim)*, mediante estudo, debate e encaminhamento das providências cabíveis.

5.3. Política de Privacidade

a) Os nomes e endereços informados nesta *Revista* serão usados exclusivamente para os serviços prestados por esta publicação, não sendo disponibilizados para outras finalidades ou a terceiros.

b) A *Revista Brasileira de Ciências Criminais (RBCCrim)* adota o sistema de controle duplo-cego por pares, de modo que há anonimato entre os avaliadores e autores, respeitando o sigilo sobre os dados do redator do parecer no momento do encaminhamento ao autor.

c) Com relação aos pareceres eventualmente emitidos pelos avaliadores da *Revista Brasileira de Ciências Criminais (RBCCrim)*, embora utilize-se o sistema de controle duplo-cego (em que autor e revisores não têm informações recíprocas no momento da avaliação), após a finalização do processo editorial, a partir do momento da tomada da decisão final pela equipe editorial, não há proibição de publicização do parecer pelo seu autor (parecerista). Por exemplo, autoriza-se (e sugere-se) a publicação do conteúdo das avaliações no sistema PUBLONS. Ou seja, os direitos autorais sobre os pareceres são dos seus respectivos autores (pareceristas). O direito de anonimato em relação à avaliação é disponível ao parecerista, que pode optar por publicar posteriormente o parecer emitido.

d) A partir dessa lógica, deve-se ressaltar que os autores dos artigos submetidos não podem dar publicidade a eventuais pareceres recebidos, salvo em caso de autorização expressa do parecerista.

e) Por fim, ao submeter o artigo para o processo editorial da *Revista Brasileira de Ciências Criminais (RBCCrim)*, o autor está ciente e autoriza eventual divulgação do parecer emitido por qualquer avaliador do periódico, por exemplo, no sistema PUBLONS.

6. Resenhas críticas, pareceres, comentários jurisprudenciais e entrevistas

a) Resenhas de livros: não serão aceitas resenhas meramente descritivas. Serão publicadas somente **resenhas críticas** de livros de interesse jurídico e científico para o escopo editorial do periódico, com a citação de outras referências, e não somente um resumo do trabalho específico. O tamanho do texto deve respeitar os limites e requisitos das informações necessárias para a boa compreensão do texto analisado (Item 2, b).

b) Os comentários jurisprudenciais poderão ser enviados à *Revista* e serão publicados, respeitando as regras acima, com o limite de páginas reduzido a 20 laudas. Deve haver uma análise crítica do julgado, a partir de referências doutrinárias representativas acerca da temática em estudo.

c) Os pareceres deverão abordar caso relevante e atual de concretização prática acerca de discussão teórica importante às ciências criminais. Deverá ser embasado em referências consistentes e atualizadas. Se houver qualquer tipo de financiamento, isso deve ser exposto em nota de rodapé, de modo a atestar eventuais conflitos de interesse.

d) As entrevistas com pesquisadores de renome poderão ser propostas ou enviadas à *Revista*, com base na avaliação combinada dos seguintes critérios:

- Representa um avanço no conhecimento que merece ser divulgado para a sociedade?
- Contribui para a popularização do conhecimento científico?
- Apresenta inovações significativas?
- Pode ter impacto na sociedade ou na definição de políticas públicas?
- Além do público-alvo (jornalistas), a entrevista poderá ser utilizada também por tomadores de decisão, pesquisadores, estudantes e público em geral?
- Tamanho: deve ser composta por 4 a 10 questões e o texto deve conter o máximo de 15.000 caracteres com espaço;
- Idioma: poderão ser encaminhadas nos idiomas português, inglês ou espanhol;
- Imagem: deverão, obrigatoriamente, ser acompanhadas pela foto do entrevistado, que deve ser enviada em arquivo anexo (.jpg ou .gif), com boa resolução (acima de 100 KB) e com autorização prévia do entrevistado. Caso seja de interesse deste, pode ser incluída também uma imagem que complemente o conteúdo da entrevista;
- Dados sobre o entrevistado: breve texto com dados sobre o entrevistado, contendo informação sobre o currículo, incluindo instituição à qual está afiliado, produção científica resumida, formação acadêmica, outros;
- *Lead*: as entrevistas deverão estar acompanhadas do *lead,* que consiste em um pequeno texto que fornece ao leitor a informação básica sobre o tema. O *lead* deve conter informação que responda às seguintes questões: "O quê" e/ou "Quem?", "Quando?", "Onde?", "Como?", e "Por quê?".

e) A avaliação das resenhas, comentários jurisprudenciais, pareceres e entrevistas serão realizados pela equipe editorial da *RBCCRIM*, a partir da relevância, cientificidade e pertinência do trabalho, além da titulação do autor, sem envio à análise cega por pares.

7. Processo de avaliação e publicação

a) Controle preliminar formal *(desk review):* Recebido o manuscrito, inicialmente haverá um controle preliminar realizado pelos editores (chefe, assistentes, executivos ou editores associados) do periódico, o que condicionará seu envio para o controle por pares. Em tal momento, a avaliação se limitará aos aspectos formais essenciais do artigo, conforme as regras expostas anteriormente, analisando os seguintes aspectos:
   1. O trabalho obedece às normas de publicação da *Revista Brasileira de Ciências Criminais (RBCCrim)*?
   2. O trabalho é compatível com a linha editorial do periódico?
   3. O trabalho apresenta linguagem adequada e cientifica, sem erros excessivos? (considerar que haverá revisão gramatical e de ortografia, se aprovado)
   4. O trabalho é inédito?
   5. A temática abordada é atual e/ou relevante?
   6. O artigo utiliza referências atualizadas e de autores nacionais e estrangeiros representativos na temática abordada?

b) Em caso de rejeição preliminar, o autor será notificado, mediante o envio do parecer emitido com os motivos da recusa. Em tal situação, o artigo poderá ser submetido novamente à avaliação para volume posterior, se mantido o ineditismo e corrigidas as deficiências indicadas.

c) No curso da avalição por pares, havendo dois pareceres discordantes sobre a publicação ou não do trabalho, este será encaminhado a um terceiro parecerista. Em casos excepcionais, poder-se-á encaminhar o trabalho para um parecerista convidado, desde que a especificidade do tema e o notório conhecimento do parecerista na área assim o justifique. Do mesmo modo, se por inércia dos avaliadores a conclusão da análise restar pendente por prolongado período e por empate de decisões contrárias, a coordenação da *Revista* poderá desempatar com a elaboração de um parecer de Minerva.

d) Na avaliação do parecerista, os trabalhos poderão ser rejeitados, aprovados ou aprovados com ressalvas (com sugestões para correções necessárias). Nesta última hipótese, o autor será informado acerca das correções sugeridas, podendo corrigi-las ou manter justificadamente seu formato original. Em qualquer situação, a decisão final acerca da publicação do trabalho é da equipe editorial do periódico, que poderá condicionar a sua publicação à realização de mais de uma rodada de correções, caso as justificativas apresentadas para a não adoção das recomendações não pareçam consistentes e satisfatórias.

e) Em todos os casos, os pareceres anônimos (sem identificação do avaliador) ficam à disposição dos autores.

8. Direitos autorais

a) Os direitos autorais dos artigos publicados são do autor, com direitos do periódico sobre a primeira publicação.

Os autores somente poderão utilizar os mesmos resultados em outras publicações indicando claramente este periódico como o meio da publicação original. Se não houver tal indicação, considerar-se-á situação de autoplágio.

Portanto, a reprodução, total ou parcial, dos artigos aqui publicados fica sujeita à expressa menção da procedência de sua publicação neste periódico, citando-se o volume e o número dessa publicação. Para efeitos legais, deve ser consignada a fonte de publicação original.

9. Revisão, diagramação, impressão e publicação

Finalizado o processo editorial de seleção dos artigos, os trabalhos aprovados e selecionados para o respectivo volume são enviados para a revisão e diagramação, realizadas ao encargo do IBCCRIM e da Editora Revista dos Tribunais (RT).

Assim, são realizadas a revisão gramatical e ortográfica, bem como a formatação (diagramação) dos arquivos, que retornam ao IBCCRIM. Em seguida, em data próxima à publicação, haverá novo contato com o autor para a análise das sugestões de correção pós-revisão e verificação da formatação, com prazo de 3 (três) dias para resposta. Em caso de inércia, as correções sugeridas pela revisão serão integralmente aceitas. Nesse momento, solicita-se que o autor se abstenha de realizar alterações profundas no texto, mas somente realize a revisão sugerida e atualizações indispensáveis.

No que tange à revisão de ortografia, o IBCCRIM adota a correção ortográfica (ortografia, acentuação, hifenização etc.) do mais recente Acordo Ortográfico (2009) em vigor (obrigatório desde 01/01/2016), até mesmo para citações de originais anteriores ao Acordo. Exceção é feita a documentos antigos em contextos nos quais a preservação da grafia original tem importância e significado historiográfico e/ou linguístico etc.

Em seguida, os artigos, com as aprovações e rejeições dos autores às sugestões de revisão, são encaminhados para a diagramação final e publicação.

A Revista Brasileira de Ciências Criminais (RBCCrim) adota postura de integral respeito ao autor, de modo a vedar qualquer alteração sem sua aprovação (salvo a falta de resposta no prazo determinado), ainda que aparentem ser "meras correções ortográficas". Qualquer atitude distinta a tal diretriz é repudiada pela equipe editorial do periódico.

10. Critérios de espera e preferência para publicação

a) A publicação dos trabalhos aprovados pelo controle por pares e selecionados pelos editores do periódico segue a ordem cronológica de submissão e aprovação, com exceção de autores convidados. Contudo, em razão das regras impostas pela comissão Qualis/

CAPES, existem critérios para avaliação e publicação preferencial, que podem ser atendidos pelos autores visando à maior agilidade na publicação de seu trabalho.

b) Em razão das regras de exogenia, artigos de autores representantes do Estado de São Paulo são limitados a 25% do total de trabalhos publicados por volume, de modo que há uma fila específica para artigos que se enquadrem em tal circunstância;

c) Diante das regras de qualidade impostas, cada volume publicado conterá entre 50 a 60% dos artigos com autor (ao menos um) que possua titulação de doutor, de modo que há limitação à publicação de trabalhos sem autoria de autor com essa titulação;

d) Artigos em coautoria entre professores permanentes de Programas de Instituições de Ensino Superior de diferentes unidades da federação, com filiação devidamente identificada;

e) Artigos originais de profissionais vinculados a Instituições de Ensino Superior estrangeiras;

f) Artigos em inglês ou em outras línguas, ainda que o autor seja brasileiro;

g) Artigos resultantes de pesquisas financiadas por órgãos de fomento (desconsiderar bolsas de iniciação científica, mestrado e doutorado ou de editais destinados aos programas como o PROEX, PROAP, PROSUP e versões semelhantes dos órgãos estaduais de fomento) devidamente identificados no texto (especificar o edital de que resulta o financiamento em nota de rodapé).

h) Além de tais hipóteses, podem ser publicados com preferência trabalhos que abordem temática de iminente atualidade e que possam se tornar obsoletos em razão do decurso da demora para publicação. Tal situação é determinada por decisão da equipe editorial da *Revista Brasileira de Ciências Criminais (RBCCrim)* e pode ser sugerida pelos pareceristas em sua avaliação.

i) Vale ressaltar, contudo, que os critérios expostos neste tópico determinam a preferência do artigo no processo de avaliação e publicação, mas não são requisitos indispensáveis. Por exemplo, embora textos com autoria de escritor com titulação de doutor tenham preferência, não há impedimento para publicação de artigos sem tal característica. Todos serão submetidos ao controle por pares, que adotará idênticos parâmetros na seleção, visando à produção científica de qualidade no periódico.

10.1. Autores convidados

Conforme decisão de sua equipe editorial, a *Revista Brasileira de Ciências Criminais (RBCCrim)* poderá convidar autores para publicar artigos sobre temáticas específicas, em razão de sua relevância, atualidade e marcante contribuição crítica às ciências criminais. Em tal situação, excepcionalmente, não haverá controle por pares *(double blind peer review)* e atenção à fila de aprovados para publicação. Conforme regra da Qualis/CAPES, o percentual de artigos de autores convidados fica limitado a 25% por volume.

10.2. Volumes e dossiês especiais

A *Revista Brasileira de Ciências Criminais (RBCCrim)* poderá publicar volumes especiais ou dossiês específicos em seus volumes ordinários, em razão da relevância e da pertinência da temática, conforme decisão da equipe editorial e de seu conselho editorial. O volume ou dossiê poderá ficar sob responsabilidade de um editor associado que possua relevante conhecimento sobre o tema. Em tal situação, haverá divulgação de edital contendo as informações necessárias, como regras e prazos para submissão. De todo modo, haverá o controle por pares *(double blind peer review)*.

Diretrizes ao Corpo de Avaliadores – *Revista Brasileira de Ciências Criminais*



Diretrizes determinadas pela equipe editorial em conformidade com o conselho editorial da RBCCRIM, sujeitas à revisão periódica.

1. Composição do corpo de avaliadores

O corpo de avaliadores da *RBCCRIM* é composto por mestres, doutorandos e doutores, com distinto conhecimento acerca das ciências criminais. Os **artigos submetidos são avaliados por pareceristas de igual ou superior titulação ao autor de maior titulação**.

Interessados em compor o corpo de pareceristas e contribuir com a *RBCCRIM* que cumpram os requisitos abaixo (item 2) deverão se cadastrar por meio do seguinte link: https://publicacoes.ibccrim.org.br/index.php/RBCCRIM/index

Como contraprestação à contribuição realizada pelo parecerista, serão fornecidas, conforme solicitação, **declarações de sua participação no corpo permanente e individuais por parecer emitido** (para fins de preenchimento e comprovação em Lattes nos campos *Revisor de Periódico* e *Produção Técnica – Parecer,* sem divulgação do título do artigo avaliado*).* **As declarações serão emitidas uma vez ao ano (mês de dezembro)**, englobando todos os pareceres emitidos no período, salvo casos de urgência motivada.

Além disso, o parecerista que respeitar integralmente as regras contidas nestas Diretrizes e no documento de Política Editorial da *RBCCRIM*, especialmente com a atenção aos prazos para resposta, **receberá um código de acesso da versão digital do volume referente à avaliação realizada** (fornecido diretamente pela Editora RT e mediante requisição)**.**

Por fim, a cada quatro (4) pareceres realizados adequadamente e com respeito ao prazo determinado, o avaliador terá direito a **um exemplar impresso da *RBCCRIM*,** conforme disponibilidade no estoque do IBCCRIM. O exemplar deverá ser retirado pessoalmente (ou por terceiro, com autorização por escrito) na sede do IBCCRIM em São Paulo, pois não haverá pagamento de custos e disponibilidade para postagem nos correios.

Na versão impressa da revista, será publicada a lista dos avaliadores que efetivamente emitiram pareceres referentes ao respectivo volume/mês.

Para fins de **determinação do volume (mês) em que houve a colaboração do parecerista**, por se tratar de periódico de fluxo contínuo (salvo em caso de dossiês temáticos), serão adotados os seguintes critérios:

a) se, na decisão editorial (após o recebimento de todos os pareceres) o artigo for aprovado, considerar-se-á o volume (mês) em que o artigo for publicado;

b) se, na decisão editorial (após o recebimento de todos os pareceres) o artigo for rejeitado, considerar-se-á o volume (mês) em que o artigo for rejeitado pela decisão final da equipe editorial.

Portanto, por exemplo, embora o parecerista tenha enviado a avaliação em um determinado mês (junho), se houver pareceres divergentes (sendo necessária a redistribuição a novo avaliador) e a rejeição ocorrer em agosto, considerar-se-á que todos os avaliadores contribuíram ao volume da *RBCCRIM* de agosto.

2. Requisitos para ingresso no corpo de avaliadores

O pesquisador interessado em compor o corpo de pareceristas e contribuir com a *RBCCRIM* deverá:

a) possuir currículo LATTES atualizado (se brasileiro);

b) possui número de registro ORCID;

c) possuir a titulação de mestre ou estar cursando doutorado em Direito ou áreas afins;

d) possuir conhecimento específico acerca das ciências criminais, demonstrado a partir de titulação, experiência na pesquisa e docência ou sólida produção bibliográfica relacionada à área das ciências criminais;

e) atestar disponibilidade para a realização de **dois pareceres por bimestre** com respeito aos prazos e regras da RBCCRIM.

Em razão das regras determinadas pela Qualis/CAPES, haverá preferência a pesquisadores com doutorado finalizado, professores de Programas de Pós-Graduação e não vinculados ao estado de São Paulo (regra de exogenia).

3. Diretrizes para realização da avaliação

Em razão dos prazos exigidos para a publicação da *Revista*, e a fim de evitar atrasos na resposta aos autores e no próprio encaminhamento dos textos à Editora, o parecer deve ser enviado no **prazo máximo de 15 (quinze) dias**. Caso haja qualquer dificuldade no atendimento do mencionado prazo, deve-se notificar o periódico para que se busque a solução adequada. O envio do parecer deve ser **em formato DOC (WORD), e não em PDF**, pois posteriormente os dados do avaliador precisam ser suprimidos para o envio anônimo ao autor.

Se houver qualquer identificação do autor do artigo ou sua temática apresentar complexidade que deva ser analisada por avaliador específico, tal fato deve ser informado imediatamente, a fim de que se encaminhe o trabalho a outro parecerista. Contudo, deve-se considerar que existem **limites para a quantidade de recusas à avaliação pelo parecerista**, o que pode resultar no afastamento do avaliador do corpo permanente.

Assim, após a leitura do trabalho encaminhado, deve-se **preencher o formulário constante no modelo de parecer**, manifestando a avaliação do artigo. Na confecção da justificativa do parecer, poder-se-á utilizar o espaço necessário. Além disso, também pode ser realizada a avaliação do texto por meio da **ferramenta de revisão do WORD**, com sugestões de alterações e comentários, desde que atente-se à exclusão de qualquer dado que possa identificar o parecerista. Isso não afasta a necessidade de preenchimento e justificação do parecer.

Para a realização da avaliação, impõe-se o conhecimento prévio das regras contidas no documento referente à Política Editorial da RBCCRIM, que pode ser acessado no link: https://www.ibccrim.org.br/rbccrim_normas_publicacao.

Considerando tais diretrizes e os critérios elencados no modelo de parecer, deve-se iniciar a avaliação pelos "critérios de exclusão" (parte 1), que determinam aspectos formais indispensáveis ao artigo científico, sob pena de rejeição preliminar, o que, de qualquer modo, precisa ser motivado no campo de justificação (parte 3). Se considerado apto em tal análise, deve-se realizar a avaliação qualitativa conforme os "critérios de avaliação" (parte 2), determinando uma nota ao artigo, e, ao final, motivando tal decisão. Por fim, deve-se apontar o parecer final e os demais aspectos acessórios.

A ausência de justificativa ou sua inconsistência acarreta a invalidade do parecer! A mera marcação dos critérios e definição de nota é insuficiente, sendo necessária a motivação específica, onde deve-se descrever brevemente o conteúdo fundamental do trabalho analisado e sua adequação aos critérios determinados.

4. Regras sobre disponibilidade e prazos de resposta

Cada integrante do corpo permanente de avaliadores da *RBCCRIM* deverá estar disponível para emitir **até dois pareceres por bimestre no prazo de 15 dias a partir do recebimento da solicitação**.

Em caso de não realização do parecer em razão da temática específica do artigo enviado necessitar **avaliador *ad hoc***, tal situação deverá ser motivada especificamente no formulário de avaliação.

A cada período de atividade de 12 meses, o avaliador poderá solicitar a **suspensão temporária** de encaminhamento de novos artigos para avaliação pelo prazo de até 3 meses, sem afastamento do corpo de avaliadores permanentes.

Em caso de inatividade por 2 meses (não resposta às solicitações) ou duas negativas injustificadas consecutivas, descumprimento das regras e desrespeito reiterado dos prazos, o avaliador será **imediatamente afastado** do corpo permanente de pareceristas da *RBCCRIM*, sem prejuízo de posterior reingresso quando atestada a necessária disponibilidade.

5. Pressupostos de integridade ética aos avaliadores

(Versão inspirada nas diretrizes adotadas e sugeridas pela *Revista Teoria Jurídica Contemporânea*, periódico do PPG em Direito da UFRJ. Disponível em: [https://revistas.ufrj.br/index.php/rjur/about/editorialPolicies]. Acesso em: 16.03.2016).

O parecer cego deve ser feito com rigor, objetividade, imparcialidade e presteza. A avaliação deve ser realizada com o objetivo de aprimorar a produção científica do Direito.

O parecerista não deve utilizar critérios distintos daqueles determinados no modelo de parecer da *RBCCRIM*. Um trabalho não deve ser rejeitado por discordâncias pessoais do avaliador (salvo se o trabalho sustentar posições avessas e incompatíveis às diretrizes regimentais e políticas do IBCCRIM) ou formalidades distintas das requeridas pelo periódico, mas **devem ser considerados somente critérios científicos para o aprimoramento das ciências criminais**.

O revisor deverá abster-se de sua função de avaliador, por potencial **conflito de interesse**, quando manter colaboração cientifica regular, em atividade de pesquisa, publicação, orientação ou tutoria, ou quando tiver relação familiar com algum dos pesquisadores responsáveis pela proposta submetida à sua avaliação. "Há conflito potencial de interesses nas situações em que a coexistência entre o interesse que deve ter o pesquisador de fazer avançar a ciência e interesses de outra natureza, ainda que legítimos, possa ser razoavelmente percebida, por ele próprio ou por outrem, como conflituosa e prejudicial à objetividade e imparcialidade de suas decisões científicas, mesmo independentemente de seu conhecimento e vontade."

6. Princípios para uma boa avaliação[1]

Confidencialidade: é essencial que a confidencialidade do processo de correção do artigo seja respeitada, durante a avaliação e mesmo após a divulgação dos resultados. Por isso, requer-se do(a) avaliador(a) que mantenha o sigilo a respeito dos trabalhos avaliados, evitando comentar ou divulgar, verbalmente ou por escrito, qualquer questão relacionada aos artigos avaliados. O anonimato, garantido pelo processo de avaliação cega (*double blind peer review*), deve ser protegido mesmo após a entrega do parecer. O respeito a esse princípio do processo de avaliação é considerado essencial.

Imparcialidade: a produção intelectual na área das ciências sociais aplicadas, como é o Direito, é historicamente marcada pela tensão entre a cientificidade e os valores ou preferências, sejam eles políticos, religiosos ou éticos. É um grande desafio, portanto, avaliar um trabalho carregado por tais tensões. Por isso, recomenda-se uma "autovigilância" constante no processo de avaliação, para que preferências como convicções políticas ou outras convicções subjetivas não contaminem a correção do artigo. Isso não implica conceder, no processo de avaliação, que qualquer tipo de trabalho ou argumentação é aceitável, mas apenas a busca por uma aferição imparcial e objetiva da qualidade, rigor e fundamentação dos argumentos apresentados.

Fundamentação: a melhor forma de garantir imparcialidade na avaliação do artigo é fundamentar, de forma clara e objetiva, as percepções sobre o trabalho e decisões tomadas a partir daí. Para tanto, é fundamental que os(as) avaliadores(as) se familiarizem com a política editorial da *RBCCrim* e suas diretrizes. É importante que a avaliação ocorra de forma fundamentada

1. Recomendações adaptadas do Guia de avaliação de TCC do programa de pós-graduação *lato sensu* da FGV Direito SP | *GVlaw*, disponível online.

nestes parâmetros. A avaliação deve, necessariamente, ser exercida a partir das mesmas normas e diretrizes divulgadas ao tempo da submissão do artigo ao processo avaliação.

Respeito aos prazos: o processo de avaliação deve obedecer a prazos para que sejam reunidas as condições mais céleres possíveis de resposta aos(às) autores(as). Atrasos podem gerar graves consequências para os(as) autores(as) e para a *RBCCrim* como um todo, tais como prejuízos ao cronograma de produtividade acadêmica exigida pelos programas de pós-graduação ou morosidade para a confecção antecipada dos próximos números da *Revista*. Não há impedimento à comunicação de indisponibilidade ou afastamento temporário, sem prejuízo de posterior reingresso quando atestada a necessária disponibilidade.

***Feedback* Construtivo**

A avaliação de um trabalho acadêmico implica em um importante exercício de empatia, colaboração e autoconhecimento. O *feedback* pode alcançar diferentes resultados, a depender da forma que foi emitido: pode ser encorajador e oferecer uma boa contribuição para o artigo, ou ser destrutivo e desestimular o destinatário, sem oferecer qualquer contribuição científica/acadêmica útil para o trabalho. Portanto, sugerimos que, ao dar *feedback* sobre o trabalho sob sua avaliação, leve em consideração as seguintes sugestões:

(I) **Comece ressaltando os pontos positivos**: iniciar uma avaliação ressaltando os pontos fortes do artigo pode auxiliar o destinatário a receber melhor as críticas colocadas, com a segurança de que outros aspectos foram levados em conta. O *feedback* deve sempre ser equilibrado e levar em conta a integralidade do artigo. Muitas vezes, o ato de apenas enumerar o que está errado desestimula o receptor, que se sente desprestigiado e não favorece uma avaliação justa, tendo em vista que é focada apenas nos erros.

(II) **Seja específico e ofereça alternativas:** é muito importante evitar comentários genéricos, que dificultam a compreensão do que pode ser desenvolvido pelo(a) autor(a). Comentários como "muito bom", "muito ruim", "terrível" etc, costumam não apontar nenhuma direção e não fornecem uma colaboração efetiva. Sugestões objetivas facilitam a compreensão e dão ao(à) autor(a) a oportunidade de corrigir seus erros e aprimorar suas habilidades para as próximas pesquisas. A especificidade também auxilia o receptor da informação a entender os critérios para a sua avaliação e a aceitar isso como uma colaboração, não como uma punição.

(III) **Seja mais descritivo e gentil:** assumir uma postura avaliativa muito assertiva pode prejudicar a forma com que essa informação será recebida pelo(a) autor(a). Não podemos esquecer que, para além da avaliação final, esse momento integra uma relação de troca e crescimento com um(a) autor(a) que não espera de uma instituição acadêmica uma contribuição pouco construtiva e hostil. O anonimato garantido pela "avaliação cega" não pode nos fazer esquecer de que, "do outro lado" do Formulário de Avaliação, haverá um autor(a) que receberá os comentários.

(IV) **Evite adjetivos:** Normalmente, uma avaliação bem fundamentada e construtiva se caracteriza por trazer poucos adjetivos. Simplesmente dizer que um determinado

argumento é "ruim" ou "frágil" é diferente de demonstrar, concretamente, a contradição lógica implicada por esse mesmo argumento. A adjetivação, com frequência, fala menos do artigo e mais das preferências do(a) avaliador(a), pouco contribuindo, portanto, para a compreensão, pelo(a) autor(a), sobre as forças e deficiências de seu artigo.

(V) **Ofereça uma contribuição:** cada pessoa possui uma forma de desenvolver seu raciocínio e uma maneira de escrever. Avaliar não significa impor sua forma de desenvolver a pesquisa, mas sim colocar ao(à) pesquisador(a) uma opção de como o estudo poderia ser melhor desenvolvido. Ainda que esse *feedback* implique apontar um erro, colocar isso como uma sugestão facilita a absorção da informação, pois muitas vezes a crítica direta desperta a resistência do receptor.

REVISTA BRASILEIRA DE CIÊNCIAS CRIMINAIS

IBCCRIM

CONDIÇÕES PARA SUBMISSÃO (*CHECKLIST*)

(ou "como evitar uma rejeição preliminar")

* requisitos básicos que não excluem a necessidade de integral atenção às demais regras da Política Editorial da *RBCCRIM* (https://www.ibccrim.org.br/rbccrim_normas_publicacao)

- ✓ **O artigo é inédito e livre de plágio?** Ele não está sendo avaliado para publicação por outra revista? Quando um trabalho idêntico ou semelhante tiver sido publicado em meio distinto (ainda que em outro idioma), esse fato deve ser informado ao editor no momento da submissão.
- ✓ O cadastro do artigo no sistema de submissões (OJS) foi preenchido em sua integralidade? https://publicacoes.ibccrim.org.br/index.php/RBCCRIM/index . OBS: o arquivo precisa estar no formato doc (word).
- ✓ O trabalho aborda temática relacionada às ciências criminais e é compatível com a linha editorial da *RBCCRIM?*
- ✓ O texto é precedido de título, **resumo (até 200 palavras) e cinco palavras-chave, todos no idioma do artigo e em inglês, além de sumário (no idioma do artigo)**?
- ✓ O artigo é divido em tópicos e apresenta **itens específicos para introdução, considerações finais (ou conclusões) e referências**?
- ✓ O trabalho tem entre 20 e 40 páginas, sem espaçamentos entre os parágrafos, 1.5 de entrelinha, fonte *Times New Roman* (tamanho 12 no corpo), margens superior e inferior com 2,0 cm e laterais com 3,0 cm?
- ✓ A qualificação do(a)(s) autor(a)(es), número de ORCID e seu e-mail estão indicados?
- ✓ **Os autores e coautores possuem titulação mínima de mestrado?**
- ✓ Se houver financiamento, os dados do edital estão indicados em nota de rodapé?
- ✓ Se houver apresentação de resultados de pesquisa empírica inédita envolvendo seres humanos, há a indicação em nota de rodapé da aprovação por comitê de ética?
- ✓ O artigo utiliza **referências** atualizadas e de autores nacionais e estrangeiros representativos na temática abordada?
- ✓ O trabalho respeita integralmente as demais regras da Política Editorial da *RBCCRIM?*

A garantia da motivação e o artigo 935 do Código Civil: a inconstitucionalidade da vinculação do juízo cível às sentenças do Tribunal do Júri

Reasoned decisions and the article 935 of the Brazilian Civil Code: unconstitutionality of the binding effects from the jury's decisions to the civil justice

Daniel de Oliveira Pontes
Mestrando em Direito Processual na Universidade do Estado do Rio de Janeiro (UERJ). Advogado.
danielop@globo.com

Data de recebimento: 01.11.2017
Data de aprovação: 12.11.2017 e 16.11.2017

modelo

Áreas do Direito: Processual; Civil; Penal

Resumo: No presente artigo, destaca-se a problemática dos julgamentos do Tribunal do Júri, em que os jurados decidem por íntima convicção e em sigilo. Diante dessas peculiaridades, pretende-se analisar se as sentenças prolatadas nesse rito especial do processo penal podem repercutir no cível, em especial pela garantia da motivação das decisões jurisdicionais.

Palavras-chave: Motivação – Garantias – Júri – Vinculação – Inconstitucionalidade.

Abstract: The present work seeks to analyze this problem regarding Jury's decisions, because they are confidential and unjustified. Such characters could prevent the application of the article 935 to obey the right of the parts to reasoned decisions.

Keywords: Decisions – Rights – Jury – Binding – Unconstitutionality.

Sumário: 1. Introdução e delimitação do tema. 2. O conteúdo da garantia da motivação em um Direito Processual constitucionalizado. 2.1. O neoconstitucionalismo e seu impacto no Direito Processual. 2.2. O princípio da motivação como garantia estrutural da prestação jurisdicional. 3. O artigo 935 do Código Civil e a influência do juízo penal no cível. 4. Os julgamentos no Tribunal do Júri: a peculiaridade do sigilo do voto e da soberania dos veredictos. 5. A inconstitucionalidade da incidência do artigo 935 do CC nos casos de Tribunal do Júri frente à garantia da motivação. 6. Conclusões. 7. Referências.

1. Introdução e delimitação do tema

Ao longo do tempo, o exercício do poder jurisdicional já comportou relações diversas com a exigência da fundamentação de seus atos: a íntima convicção, a prova tarifada e o livre convencimento motivado. No Código de Processo Civil (CPC) atual, afloram críticas de que não haveria liberdade na formação do convencimento, de modo que nos encaminharíamos para um novo momento histórico, tendo em vista que o direito processual deve servir como mecanismo de controle às decisões judiciais.[1]

Seja como for, é induvidoso que, no atual estado de coisas, a motivação se tornou uma garantia estruturante do processo, que legitima o próprio exercício da jurisdição pelo agente público.

7. Referências

BARROSO, Luís Roberto. Neoconstitucionalismo e constitucionalização do direito (o triunfo tardio do direito constitucional no Brasil). *Revista de Direito Administrativo*, v. 240, p. 1-42, abr.-jun. 2005.

CALAMANDREI, Piero. *Procedure and democracy*. Trad. John Clarke Adams e Helen Adams. New York: New York University Press, 1956.

CINTRA, Antonio Carlos de Araújo; GRINOVER, Ada Pellegrini; DINAMARCO, Cândido Rangel. *Teoria geral do processo*. 31. ed. São Paulo: Malheiros Editores, 2015.

GALDINO, Flavio. A evolução das ideias de acesso à justiça. In: SARMENTO, Daniel; GALDINO, Flavio (Org.). *Direitos fundamentais*: estudos em homenagem ao professor Ricardo Lobo Torres. Rio de Janeiro: Renovar, 2006.

MARINONI, Luiz Guilherme; ARENHART, Sergio; MITIDIERO, Daniel. *Novo curso de processo civil*. São Paulo: Ed. RT, 2015. v. 2.

PICARDI, Nicola. *Jurisdição e processo*. Trad. Carlos Alberto Alvaro de Oliveira. Rio de Janeiro: Forense, 2008.

STRECK, Lenio Luiz. O novo Código de Processo Civil (CPC) e as inovações hermenêuticas. *Revista de Informação Legislativa*, Brasília, ano 52, n. 206, p. 33-51, abr.-jun. 2015.

TIMOTEO, Gabrielle. Normativos internacionais e escravidão. *Revista Hendu,* n. 4, p. 70-83, 2013. Disponível em: [www.periodicos.ufpa.br/index.php/hendu/article/view/1716/2137]. Acesso em: 27.10.2017.

1. STRECK, Lenio Luiz. O novo Código de Processo Civil (CPC) e as inovações hermenêuticas. *Revista de Informação Legislativa*, Brasília, ano 52, n. 206, p. 33-51, abr.-jun. 2015.

modelo

Diagramação eletrônica:
Linotec Fotocomposição e Fotolito Ltda., CNPJ 60.442.175/0001-80

Impressão e encadernação:
DEK Comércio e Serviços Ltda., CNPJ 01.036.332/0001-99