INSTITUTO BRASILEIRO DE ENSINO, DESENVOLVIMENTO E PESQUISA
PROGRAMA DE PÓS-GRADUAÇÃO STRICTO SENSU EM DIREITO
DOUTORADO ACADÊMICO EM DIREITO CONSTITUCIONAL

PAULO AUGUSTO MOREIRA LIMA

# ARMAZENAMENTO DE DADOS DIGITAIS PESSOAIS NA INVESTIGAÇÃO CRIMINAL E NO PROCESSO PENAL: LIMITAÇÃO AO INDISPENSÁVEL, DEVIDO PROCESSO PENAL INFORMACIONAL E PUBLICIDADE

**BRASÍLIA**

**2024**

PAULO AUGUSTO MOREIRA LIMA

# ARMAZENAMENTO DE DADOS DIGITAIS PESSOAIS NA INVESTIGAÇÃO CRIMINAL E NO PROCESSO PENAL: LIMITAÇÃO AO INDISPENSÁVEL, DEVIDO PROCESSO PENAL INFORMACIONAL E PUBLICIDADE

Tese de Doutorado apresentada ao programa de Pós-Graduação Stricto Sensu, da Instituto de Direito Público (IDP), como requisito parcial à obtenção do título de Doutor em Direito.

**Orientador:** Prof. Dr. Ilton Norberto Robl Filho

**BRASÍLIA**

**2024**

Código de catalogação na publicação – CIP

L732a Lima, Paulo Augusto Moreira

Armazenamento de dados digitais pessoais na investigação criminal e no processo penal: limitação ao indisponível, devido ao processo penal informacional e publicidade / Paulo Augusto Moreira Lima. — Brasília: Instituto Brasileiro Ensino, Desenvolvimento e Pesquisa, 2024.

328 f.

Orientador: Prof. Dr. Ilton Norberto Robl Filho.

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

1. Direito processual penal. 2. Proteção de dados - Brasil. 3. Dados digitais. I.Título

CDDir 341.43

Elaborada por Pollyana da Silva Marra – CRB 1/3704

PAULO AUGUSTO MOREIRA LIMA

# ARMAZENAMENTO DE DADOS DIGITAIS PESSOAIS NA INVESTIGAÇÃO CRIMINAL E NO PROCESSO PENAL: LIMITAÇÃO AO INDISPENSÁVEL, DEVIDO PROCESSO PENAL INFORMACIONAL E PUBLICIDADE

Tese de Doutorado apresentada ao programa de Pós-Graduação Stricto Sensu, da Instituto de Direito Público (IDP), como requisito parcial à obtenção do título de Doutor em Direito.

**Orientador:** Prof. Dr. Ilton Norberto Robl Filho

Brasília, 10 de dezembro de 2024.

**BANCA EXAMINADORA**

---

Prof. Dr. Ilton Norberto Robl Filho
Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa – IDP
Orientador

---

Prof. Dr. Ademar Borges de Sousa Filho
Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa - IDP
Membro Interno

---

Prof. Francisco Monteiro Rocha
Universidade Federal do Paraná – UFPR
Membro Externo

---

Profa. Dra. Danyelle da Silva Galvão
Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa - IDP
Membro Interno

## AGRADECIMENTOS

À Lea, meu amor e minha vida, pelo encanto de cada dia.

A Davi e Gabriel, pela alegria.

Aos meus pais, por tudo, carrego os ensinamentos comigo.

À minha avó, pelo carinho e pela presença, mesmo na ausência.

A todos os professores que tive, do jardim ao doutorado, sou um pouco de cada um.

A Deus, por todos os desafios.

À vida, por oferecer o mistério entre o destino e as escolhas. Quanto mais fugimos, mais estamos onde deveríamos estar.

Por fim, agradeço ao meu orientador, Professor Ilton Robl, por encorajar a mudança no tema da tese e viabilizar meu período de pesquisa na Universidade de Granada, o que foi um verdadeiro divisor de águas.

Granada não é apenas o local da belíssima Alhambra e símbolo da riqueza do multiculturalismo árabe, judeu e cristão. Como afirmou Henry Miller, "um destino nunca é um lugar, mas uma nova maneira de ver as coisas". Nessa busca por novos olhos, estar naquela parte da Andaluzia me inspirou a compreender verdadeiramente o valor da proteção de dados para a liberdade do indivíduo. Eis o infalível paradoxo da necessidade de se afastar para entender o que está perto. Aquela espécie de magia em ir para longe e depois voltar transformado.

"Welcome to your life
There's no turning back
Even while we sleep
We will find you
Acting on your best behavior
Turn your back on mother nature
Everybody wants to rule the world"
(TEARS FOR FEARS. *Everybody Wants to Rule the World*. In: **Songs from the Big Chair**. Mercury Records, 1985)

## RESUMO

As técnicas especiais de investigação aumentaram o armazenamento de dados pessoais nos arquivos policiais, assim como o processo penal eletrônico potencializou a exposição dessas informações pessoais armazenadas. Propõe-se compreender se a praxe jurídica brasileira na persecução penal está alinhada com o direito fundamental à proteção de dados, e se o framework regulatório é suficiente para concretizar esse direito. Por meio do Estudo da legislação pertinente e com uso de metodologia qualitativa, procedeu-se à análise da legislação e jurisprudência brasileira e europeia, especialmente espanhola. Os meios de investigação tecnológicos resultam na captação e armazenamento de dados em quantidade superior à necessária para a investigação, sem prazo e forma de descarte, o que resulta no acúmulo de dados pessoais. O processo penal eletrônico, sem limitação de acesso e formas de anonimização, resultou em abusos e distorceu institutos clássicos, como o princípio da publicidade, do contraditório e do devido processo legal. A pesquisa demonstra que o atual formato de armazenamento de dados na persecução penal afronta o direito à proteção de dados.



**Palavras-chave**: Armazenamento de dados pessoais; proteção de dados; investigação e processo penal.

## ABSTRACT

The special investigation techniques have increased the volume of personal data stored in police files, while electronic criminal proceedings have heightened the exposure of these stored personal data. The study aims to analyze whether the Brazilian legal practice in criminal prosecution aligns with the fundamental right to data protection and whether the existing regulatory framework is sufficient to ensure this right. Through a study of relevant legislation and a qualitative methodology, Brazilian and European (especially Spanish) legislation and case law were analyzed. It was observed that technological investigation methods result in the collection and storage of data beyond what is necessary for the investigation, without defined criteria for disposal, leading to an accumulation of personal data. Additionally, electronic criminal proceedings, with unrestricted access and lack of anonymization methods, have caused abuses and distorted classical principles, such as publicity, adversarial proceedings, and due process of law. The research shows that the current data storage format in criminal proceedings confronts the right to data protection.



**Key words**: Personal data storage; data protection; criminal investigation and procedure.

**SUMÁRIO**

# 1 INTRODUÇÃO: VÊ-SE TUDO, SEM NUNCA SER VISTO[1]

Não há mais dados insignificantes. A conclusão do Tribunal Constitucional da Alemanha no julgamento[2] do caso do Censo Democrático, que em 1983 parecia inspiradora, hoje soa preocupante. Isso se deve ao crescimento exponencial da captação de dados pessoais pelo Estado e por grandes corporações, além da possibilidade de que, no futuro cada vez mais iminente e real, essas informações sejam utilizadas contra nós.

A posição de ativo mais valioso do mundo[3], antes ocupada pelo ouro e pelo petróleo, foi tomada pelos dados pessoais devido ao avanço tecnológico, que trouxe benefícios como a expansão do saber, a superação de barreiras geográficas e o acesso facilitado ao conhecimento. Contudo, a 4ª Revolução Industrial[4], marcada pela inteligência artificial, *big data*, *machine learning* e um mundo interconectado por meio da internet, redes sociais, aplicativos e smartphones, apresenta efeitos colaterais significativos, especialmente a coleta massiva e armazenamento de dados pessoais.

A inteligência artificial, tratada no início como uma mera ferramenta digital, evoluiu e atingiu outro patamar ao ser combinada com algoritmos que gerenciam dados em grande escala (big data[5]), com objeto de gerar conclusões e ações. Segundo Doneda[6], processar dados é aplicar técnicas para obter resultados mais valiosos e refinados, com informações mais completas. Esse desenvolvimento fez com que dados antes considerados irrelevantes se tornassem significativos. Quando processados pela inteligência artificial, esses dados são

---

[1] A frase evidencia a assimetria do modelo panóptico, em que o observado não enxerga quem o vigia, criando uma dinâmica de poder desequilibrada. Nesse sistema, a invisibilidade do observador reforça o controle sobre os observados, que, ao não saberem quando estão sendo monitorados, internalizam a sensação de vigilância constante. Essa relação encontra um paralelo na presente tese, entre os titulares dos dados pessoais e aqueles que captam e armazenam tais informações. (FOUCAULT, Michel. *Vigiar e Punir:* Nascimento da prisão. Tradução de Raquel Ramalhete. 36. ed. Petrópolis: Vozes, 2008).

[2] A Lei do Censo de 1982 na Alemanha previa a coleta detalhada de informações pessoais, como religião, renda, composição familiar, situação profissional, o que levantou preocupações sobre a privacidade e o potencial uso indevido desses dados pelo Estado. O Tribunal Constitucional da Alemanha, em resposta, reconheceu o direito à autodeterminação informacional, derivado do princípio da dignidade humana, estabelecendo diretrizes rígidas para a coleta e uso de dados pessoais pelo Estado, garantindo que tais práticas respeitassem a privacidade e a liberdade dos indivíduos. Volkszählungsurteil. (ALEMANHA**.** Tribunal Constitucional Federal. *Decisão n.º 1 BvR 209/83, de 15 de dezembro de 1983*. Disponível em: https://www.bverfg.de/e/rs19831215_1bvr020983.htm. Acesso em: 30 out. 2024.)

[3] THE ECONOMIST. The world's most valuable resource is no longer oil, but data. *The Economist*, 6 May 2017. Disponível em: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. Acesso em: 4 out. 2024.

[4] SCHWAB, Klaus. *A Quarta Revolução Industrial*. São Paulo: Edipro, 2016.

[5] KENNEDY, Russ. The New Era Of Big Data. *Forbes*, 24 maio 2023. Disponível em: https://www.forbes.com/councils/forbestechcouncil/2023/05/24/the-new-era-of-big-data/. Acesso em: 4 out. 2024.

[6] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. 2. ed. São Paulo: Thomson Reuters Brasil, 2021. *E-book.* p. RB-2.5.

capazes de traçar perfis detalhados das pessoas, contribuindo para aumentar o sentimento de inexistência de espaços livres de observação, o que prejudica o livre desenvolvimento pessoal[7]. Laura Schertel[8] sustenta que não existem mais dados irrelevantes, tendo em vista que o risco de processamento de dados reside mais na finalidade e nas possibilidades de processamento do que no tipo de dados tratados.

A coleta e armazenamento em massa de dados pessoais refletem uma equação bastante desproporcional. De um lado, grandes corporações e o Estado, que administram esses dados, possuem amplo conhecimento a respeito de seus titulares. De outro, os próprios titulares dos dados desconhecem o que é coletado e armazenado sobre eles, em clara situação de desigualdade e assimetria informacional. Frank Pasquale[9] conceitua esse fenômeno como *one-way mirror* (espelho de sentido único), no qual a transparência é unilateral. Nessa realidade, os perigos à proteção de dados pessoais atingem níveis sem precedentes.

A frase escrita por George Orwell no livro 1984, "nada lhes pertencia, exceto os poucos centímetros cúbicos dentro de seus crânios"[10] evidencia o sentimento de perda de liberdade do homem constantemente vigiado. O Estado que tudo sabe transforma o ser humano em uma 'pessoa de vidro', pois a posse de dados sensíveis sobre os cidadãos cria uma espécie de panóptico — desta vez, invisível e dissimulado. Michel Foucault descreve o Panóptico como "uma máquina de dissociar o par ver-ser visto: no anel periférico, se é totalmente visto, sem nunca ver; na torre central, **vê-se tudo, sem nunca ser visto**"[11].

Para evitar a formação de uma sociedade de pessoas de vidro, completamente expostas, o avanço da tecnologia tornou imprescindível a tutela efetiva do direito à proteção de dados pessoais. Surge, assim, um grande desafio para os ordenamentos jurídicos, marcado pelo antagonismo entre a evolução lenta e cautelosa do Direito e a velocidade da revolução digital e tecnológica.

Felipe Giacomolli[12] utiliza uma analogia interessante para ilustrar como mudanças aparentemente superficiais na tecnologia podem causar transformações significativas:

---

[7] Sobre a extinção da separação entre o público e o privado consultar: ARENDT, Hannah. *A condição humana*. 11. ed. Rio de Janeiro: Forense Universitária, 2010.

[8] MENDES, Laura Schertel. Autodeterminação informativa: a história de um conceito. *Pensar Revista de Ciências Jurídicas Universidade de Fortaleza*, Fortaleza, v. 25, n. 4, 2020. p. 1- 18.

[9] PASQUALE, Frank. *The black box society*: The secrets algorithms that control money and information. Cambridge: [*s. l.*], 2015.

[10] ORWELL, George. *1984*. São Paulo: Companhia das Letras, 2009. p. 28.

[11] FOUCAULT, Michel. *Vigiar e Punir:* Nascimento da prisão. Tradução de Raquel Ramalhete. 36. ed. Petrópolis: Vozes, 2008.

[12] GIACOMOLLI, Felipe. *Gerenciamento tecnológico do sistema de justiça penal*: as novas tecnologias no âmbito do policiamento, da investigação e da decisão. Rio de Janeiro: Marcial Pons, 2023. p. 122.

> As inovações disruptivas e as evoluções tecnológicas exponenciais da nossa era constituem a 'pele da cultura', intitulada obra de Derrick de Kerckhove (1997), Gloeckner, parafraseando o poeta Paul Valery sobre o paradoxo da pele (o órgão mais superficial do ser humano, mas também o mais profundo), expõe como as mudanças aparentemente superficiais afetam, na verdade, aquilo que há de mais profundo na sociedade contemporânea.

Em todo o mundo, não faltam exemplos de uso de dados pessoais para os mais diversos fins, o que gerou reações dos governos na forma de leis e regulamentos. Em 2018, a China criou um projeto no qual cidadãos com baixo score social seriam impedidos de comprar passagens de trem ou de avião[13]. Todas as decisões desse sistema somente são possíveis graças à coleta massiva de dados pessoais e tratamento automatizado. Após o escândalo do *Cambridge Analytica*[14], em que o *Facebook* vendeu perfis de usuários e informações para que a empresa de análise de dados influenciasse eleitores no Brexit e nas eleições presidenciais dos EUA, é preciso refletir se a inviolabilidade da intimidade e da vida privada (art. 5, X, da CF) ainda se mantém na sociedade digital, ou se tornou apenas uma questão de crença.

Com um futuro cada vez mais incerto, seja em relação ao surgimento de novas pandemias, conflitos bélicos, governos antidemocráticos, ou com o advento de tecnologias ainda desconhecidas, é fundamental adotar um olhar voltado para o futuro que reflita uma postura cautelosa e preventiva. Não é possível prever como os dados pessoais, que continuam sendo armazenados sem critério, serão utilizados, especialmente no contexto do processo penal. Nesse cenário, os riscos devem ser avaliados não apenas com base na tecnologia existente, mas também com uma perspectiva de longo prazo. Assim, a pesquisa propõe um ponto de equilíbrio para evitar o excesso no armazenamento de dados pessoais, garantindo que esses elementos sejam guardados apenas pelo tempo estritamente necessário. Além disso, os dados captados que não sirvam como prova devem ser apagados o mais rapidamente possível.

A preocupação com o excesso de dados pessoais armazenados durante investigações não se limita ao uso consciente e proposital por governos, grandes corporações e pequenos negócios que acumulam dados fragmentados em "cadastros" para acesso a diversos serviços. Os sucessivos escândalos de vazamento de informações sensíveis, como os Panama Papers[15],

---

[13] TRINDADE, Rodrigo. Grande irmão: China proibiu 23 milhões de viagens de avião ou trem em 2018. *UOL Tilt*, 3 mar. 2019. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2019/03/03/grande-irmao-china-proibiu-23-milhoes-de-viagens-de-aviao-ou-trem-em-2018.htm. Acesso em: 4 out. 2024.

[14] RUSSIA spy poisoning: What we know so far. *BBC News*, 20 mar. 2018. Disponível em: https://www.bbc.com/news/uk-43480978. Acesso em: 4 out. 2024.

[15] PANAMA Papers: The secrets of dirty money. *BBC News*, 3 abr. 2016. Disponível em: https://www.bbc.com/news/world-35954224. Acesso em: 4 out. 2024.

as revelações de Edward Snowden[16] e a operação "Vazajato"[17], servem como alerta para os riscos envolvidos nessa prática. Em 2024, um vazamento de mais de 13 TB de dados, conhecido como MOAB[18] (Mother of All Breaches), revelou informações do LinkedIn, X (antigo Twitter), Adobe, e registros de ONGs americanas e brasileiras. A melhor forma de prevenir vazamentos de dados pessoais é limitar seu armazenamento ao estritamente necessário.

Um dos aspectos mais preocupantes da tecnologia é o *ratchet effect* ou "efeito catraca". Certas ações, uma vez implementadas, tendem a se tornar permanentes, criando um efeito irreversível. Por isso, é preferível que a política de armazenamento de dados siga o princípio da precaução, assegurando que tudo o que não for essencial seja apagado. Embora cada medida, individualmente, possa ser justificada pelo teste de proporcionalidade, o efeito cumulativo do armazenamento de dados de múltiplas pessoas ainda é pouco compreendido[19].

Por coincidência ou não, pouco antes do escândalo do *Cambridge Analytica* vir à tona, foi publicado o Regulamento Geral de Proteção de Dados Europeu – General Data Protection Regulation (GDPR) n. 2016/679, Regulamento (UE) n. 2016/679. O GDPR aprofunda direitos previstos na Convenção do Conselho da Europa de 1981[20], sobre o tratamento automatizado de dados pessoais, e na Carta de Direitos Fundamentais da União Europeia de 2000. Paralelamente, a Diretiva n. 2016/680, conhecida como Diretiva Policial, foi lançada para regular a proteção de dados no campo da segurança pública e da persecução criminal[21].

O Brasil não está alheio ao fenômeno global marcado pelo uso crescente de dados pessoais e pela criação de leis regulatórias específicas. Com efeito, a criação de bancos de dados pelos órgãos públicos[22] caminha a passos largos, somando-se àqueles oriundos da iniciativa

---

[16] HARDING, Luke. What are the Panama Papers? A guide to history's biggest data leak. *The Guardian*, 5 abr. 2016. Disponível em: https://www.theguardian.com/news/2016/apr/03/what-you-need-to-know-about-the-panama-papers. Acesso em: 4 out. 2024.

[17] EXCLUSIVO: as mensagens secretas da Lava Jato. *The Intercept Brasil,* 9 jun. 2019. Disponível em: https://theintercept.com/series/mensagens-lava-jato/. Acesso em: 4 out. 2024.

[18] DHALIWAL, Jasdev. 26 billion records released: The mother of all breaches. *McAfee Blogs*, 27 fev. 2020. Disponível em: https://www.mcafee.com/blogs/internet-security/26-billion-records-released-the-mother-of-all-breaches/. Acesso em: 4 out. 2024.

[19] HAMMOUDI, Sabrina. Law and "Smart Videoprotection": the French Case. *European Review of Digital Administration & Law - Erdal*, [*s. l.*], v. 2, n. 2, p. 205-210, 2021. Disponível em: https://doi.org/10.5281/zenodo.5094234. Acesso em: 4 out. 2024.

[20] CONVENÇÃO para a Proteção dos Indivíduos com Relação ao Tratamento Automatizado de Dados Pessoais (Convenção 108). Estrasburgo: Conselho da Europa, 1981. Disponível em: https://rm.coe.int/cm-convention-108-portuguese-version-2756-1476-7367-1/1680aa72a2. Acesso em: 4 out. 2024.

[21] Na mesma época, Nos Estados Unidos, foram editadas leis como o *Children's Online Privacy Protection Act* (COPPA), que disciplina os dados colhidos de crianças com menos de 13 anos, e o *Health Insurance Portability and Accountability Act* (HIPAA), que regula do sigilo de dados médicos.

[22] Receita Federal, CNIB, Infojud, sistemas vinculados ao CNJ (SEEU, SNBA, SNCI, VC, CNACL, CNEI) Bacenjud, Infoseg, Renajud, SISTAC, DVC, Prodesp, Detran, Juntas Comerciais, Polícia Civil (boletins de ocorrência), Polícia Federal (passaporte, armas, produtos químicos, estrangeiros), concessionárias (água, energia, gás), cartórios, Secretarias das Fazendas, Procon, bancos públicos.

privada, como companhias de seguros, operadoras de telefonia, instituições financeiras e planos de saúde. Como forma de regular a matéria, foi promulgada a Lei Geral de Proteção de Dados (Lei n. 13.709/2018), em complemento ao Marco Civil da Internet (Lei n. 12.865/2014). Contudo, é sintomático observar que o direito à proteção de dados alcançou status constitucional somente em 2022, com a Emenda Constitucional nº 115 e a inclusão do inciso LXXIX no art. 5º da Constituição Federal. Como consequência, é esperado que o debate sobre o tema ganhe impulso, de modo que a persecução penal busque sua conformidade com o direito à proteção de dados.

Esse alinhamento, no entanto, enfrenta desafios. A Lei Geral de Proteção de Dados Pessoais (LGPD) representou um avanço significativo no tema da proteção de dados, mas expressamente afastou de seu âmbito de aplicação atividades relacionadas à investigação criminal, repressão de infrações penais e segurança pública[23]. Embora essa exclusão, provavelmente, tenha sido necessária para viabilizar a aprovação do projeto de lei, ao deixar de fora os sempre polêmicos temas da segurança pública e da persecução penal, acabou por transmitir a equivocada impressão de que a proteção de dados é de menor importância na esfera penal, o que repercute na prática jurídica atual. Assim, não é por acaso que o direito à proteção de dados não é considerado um pilar fundamental do processo penal brasileiro.

Como consequência desse vazio normativo, no Brasil não há regulamentação específica na seara criminal sobre quais tipos de dados pessoais podem ser armazenados, por quanto tempo devem permanecer armazenados, se podem ser utilizados para finalidades distintas daquelas que motivaram sua coleta e qual o procedimento adequado para seu descarte[24]. No atual cenário,

---

[23] Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
(...)
III - realizado para fins exclusivos de:
a) segurança pública;
b) defesa nacional;
c) segurança do Estado; ou
d) atividades de investigação e repressão de infrações penais; ou (...)
§ 1º 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. *Lei n. 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 4 out. 2024.)

[24] A grande questão a ser enfrentada em relação ao armazenamento de dados na investigação criminal diz respeito a que tipo de dado pessoal pode ser armazenado, por quanto tempo deve permanecer armazenado, quais os requisitos para ser utilizado em finalidade diversa daquela que motivou sua captação, e qual o procedimento para seu descarte. Na ausência de enfrentamento a essas questões, bem como diante da falta de arcabouço legal, os órgãos policiais e o Ministério Público estão a armazenar e acumular dados pessoais de investigados e terceiros em seus arquivos sem qualquer direcionamento legal. Parte insignificante destes dados pessoais é juntada nos inquéritos policiais e passam a ser qualificados como prova. Contudo, a parcela majoritária destes dados pessoais é armazenada indefinidamente nos arquivos policiais.

sem uma regulamentação própria, informações e dados pessoais podem ser armazenados por longos períodos ou até mesmo indefinidamente, podendo ser reproduzidos de forma descontextualizada ou utilizados para finalidades distintas das originalmente previstas, tudo isso sem qualquer controle por parte de seus titulares.

Para aprofundar essa discussão, é fundamental compreender que as modernas técnicas especiais de investigação - como a interceptação telemática, o acesso a dados digitais armazenados em aparelhos celulares e computadores, a vigilância eletrônica e a obtenção de geolocalização a partir de torres de telefonia móvel - proporcionam amplo acesso a dados pessoais, não apenas de investigados, mas também de terceiros inevitavelmente atingidos com tais medidas. O tratamento de grandes volumes de dados pessoais é uma exigência típica das sociedades de massa e resultado direto do uso de meios tecnológicos de investigação. Como consequência, essas técnicas geram, como um efeito colateral, uma quantidade imensa de arquivos que contém dados sensíveis de investigados e terceiros. O arquivamento indefinido de tais informações em bases policiais e judiciais cria um estado de insegurança e restringe, de forma desnecessária, o direito à privacidade e à proteção de dados.

No processo penal, a lógica referente ao armazenamento de dados pessoais difere daquela observada na fase de investigação. Aqui, a preocupação é evitar o devassamento de dados pessoais de réus, testemunhas e outros sujeitos processuais, promovido pelo processo eletrônico. Não se pode sustentar a existência de proteção de dados pessoais no processo penal se todas as informações processuais, decisões e documentos forem disponibilizados para amplo acesso na internet, sem qualquer forma de anonimização ou restrição de acesso. As vantagens da publicidade e da transparência correm o risco de ser comprometidas pela criação de bancos de dados privados, pelo uso discriminatório de informações processuais, pelo *bullying* processual, além de ameaças e tentativas de intimidação que podem prejudicar o funcionamento do sistema criminal e o próprio acesso à justiça.

Além da falta de arcabouço legal, há uma questão cultural que influencia essa falta de regramento quanto aos dados pessoais na persecução penal. A integração do direito à proteção de dados na persecução penal nos remete a um debate que vem sendo travado do outro lado do Atlântico desde os anos 1970[25]. Muito antes da GDPR e da Diretiva Policial 680, na Europa, o tema vem sendo amadurecido ao longo de cinco décadas e continua em construção. Em

[25] A exemplo da Bundesdatenschutzgesetz, editado em 1977 na Alemanha. ALEMANHA. Bundesgesetzblatt. *Komplette Ausgabe, n. 7, 1977*. Disponível em: https://www.bgbl.de/xaver/bgbl/start.xav?start=//*%5B@attr_id=%27bgbl177i0201.pdf%27%5D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl177007.pdf%27%5D__1711023794148. Acesso em: 30 out. 2024.

contraste, no Brasil, as discussões mais relevantes ainda ocorrem no nicho específico do Direito à Proteção de Dados, com o tema tratado de forma secundária no âmbito do Direito Constitucional e do Processo Penal. Além disso, o cidadão brasileiro encara com naturalidade a troca de seus dados pessoais por descontos ou pelo uso gratuito de serviços em websites e redes sociais. No âmbito da persecução penal, observa-se, no máximo, uma tímida tentativa de proteger os dados pessoais, indiretamente, por meio da invocação do direito à privacidade. Talvez se acredite que, após a apreensão de dados pessoais em uma investigação criminal, a titularidade desses dados passe ao domínio do Estado, um conceito equivocado.

Na intersecção entre o direito à proteção de dados e o processo penal, observa-se um ponto de opacidade que tem passado despercebido tanto pela academia quanto pela prática jurídica: o armazenamento de dados pessoais. As questões relacionadas à proteção de dados não se limitam à fase de captação[26]. Entre a coleta e o uso final ou o compartilhamento desses dados, existe uma área cinzenta representada pelo armazenamento, aspecto frequentemente negligenciado e que se mantém como um dos principais gargalos no tratamento de dados.

Em razão dessa lacuna, surgem dúvidas sobre a capacidade do nosso sistema jurídico em dar suporte ao trabalho dos órgãos de persecução penal, garantindo, ao mesmo tempo, a proteção de dados. A ausência de normas que abranjam integralmente a realidade da persecução penal pode resultar em um processo paradoxal, no qual o próprio instrumento oficial do Estado para apurar e julgar crimes acaba por violar direitos e comprometer a credibilidade do sistema. Se mantido esse modelo, o processo penal pode se desviar de sua concepção original, que é ser um instrumento de proteção do cidadão contra o poder estatal.

Para a nossa realidade atual, ainda em análise e sem conclusões definitivas, parece ingênuo sustentar a autorregulação de dados pessoais na área criminal. Além disso, não se justifica a acumulação massiva de informações sensíveis para enfrentar o terrorismo ou o crime organizado, como se fosse uma espécie de tábua de Carnéades[27]. O Estado, com a assimetria de poder que possui, pode ser tentado a abusar dessa ferramenta contra os infratores da lei e

[26] Conforme art. 5º, inciso X, da LGPD, são formas de tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, **armazenamento**, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

[27] A Tábua de Carnéades é uma alegoria filosófica utilizada para discutir situações em que a extrema necessidade de autopreservação entra em conflito com preceitos morais ou legais. Dois náufragos no mar encontram uma tábua que pode salvar apenas uma pessoa. Para sobreviver, um dos náufragos empurra o outro para fora da tábua, resultando na morte desse indivíduo. Essa alegoria deriva de uma história hipotética apresentada pelo filósofo grego Carnéades, no século II a.C., para explorar o conceito de estado de necessidade e justificar ações que, em condições normais, seriam consideradas moralmente erradas.

inimigos políticos. Por isso, além do avanço tecnológico, é essencial uma regulação específica sobre o tratamento de dados na persecução penal, visando evitar possíveis abusos de poder.

Essas inquietações conduzem ao problema da pesquisa, que pode ser formulado a partir de uma simples pergunta: O atual formato de armazenamento de dados pessoais nas investigações criminais e no processo penal afronta o direito fundamental à proteção de dados?

Portanto, o objetivo geral é verificar se o armazenamento de dados pessoais nas investigações e no processo penal está conforme o direito constitucional à proteção de dados. Esse objetivo conduzirá à análise da suficiência do atual framework regulatório, composto pela LGPD, Marco Civil da Internet, CPP e a legislação criminal extravagante[28], para regular o tratamento de dados pessoais na persecução penal. Além desse objetivo geral, é essencial que a pesquisa aborde certos objetivos específicos, cujas respostas formarão um mosaico para a construção da tese e para a solução do problema proposto. Assim, a pesquisa buscará investigar se as medidas de investigação tecnológicas atuais estão em acordo com a proteção de dados, se o processo penal em meio eletrônico aumentou os riscos de devassamento de dados pessoais e se os institutos processuais clássicos estão aptos para lidar com os desafios trazidos pela tecnologia em relação ao armazenamento de dados pessoais.

Neste trabalho, parte-se da hipótese, baseada na revisão da literatura apresentada, de que a prática atual de armazenamento de dados pessoais nas investigações criminais e no processo penal, além de ser desnecessária para a eficiência, viola o direito à proteção de dados. Essa violação é potencializada pelo vácuo decorrente da ausência de legislação específica que regule adequadamente essa matéria no contexto da persecução penal. A implementação efetiva da proteção de dados no processo penal enfrenta obstáculos não apenas tecnológicos, mas também jurídicos, em razão da falta de uma lei que contemple especificamente essa área. Este estudo adota como trilha argumentativa as transformações impostas pela tecnologia digital ao Direito, exigindo novas soluções jurídicas e a ressignificação de institutos tradicionais, como o princípio da publicidade processual, da privacidade e do devido processo legal, que foram originalmente concebidos para um contexto anterior à era digital.

Ressalte-se que o Brasil não detém ampla liberdade para decidir *se* e *quando* o direito à proteção de dados deve ser um objetivo permanente do processo penal. A adaptação do nosso

[28] Lei de Interceptação Telefônica (Lei n. 9.296/1996), que regula as escutas telefônicas e telemáticas; da Lei da Identificação Criminal (Lei n. 12.037/2009), que cuida do registro de dados pessoais, inclusive perfis genéticos, para uso em investigações criminais; os arts. 17-B e 17-E da Lei de Lavagem de Dinheiro (Lei n. 9.613/1998) sobre acesso a dados cadastrais; os arts. 15 a 17 da Lei do Crime Organizado (Lei n. 12.850/2013); e os arts. 13-A e 13-B do Código de Processo Penal (CPP), que disciplinam o acesso a dados cadastrais e metadados para uso em investigações criminais sobre tráfico de pessoas.

sistema de justiça criminal ao GDPR e à Diretiva (UE) n. 2016/680 é fundamental para viabilizar a cooperação internacional e o compartilhamento de informações com a União Europeia, medida essencial para enfrentamento da criminalidade organizada e transnacional. Sem esse alinhamento, o Brasil pode se deparar com barreiras legais[29] para acessar dados de europeus ou estrangeiros residentes na União Europeia. Nesse contexto, a integração entre o Ministério Público, o Departamento de Polícia Federal e a Eurojus, um dos órgãos supranacionais da União Europeia, depende da adoção de um marco normativo brasileiro de proteção de dados específico para o processo penal. Embora nosso sistema legal não precise ser cópia fiel do modelo europeu, as proteções oferecidas devem ser equivalentes.

Esse contexto justifica a necessidade de uma nova abordagem prática e normativa voltada à proteção dos titulares de dados pessoais. É com base nessa demanda que o armazenamento de dados pessoais no processo penal deve ser considerado parte fundamental do direito à proteção de dados. Embora a prática de armazenar informações pessoais em investigações criminais e no processo penal esteja em plena expansão, esse fenômeno tem recebido pouca atenção da academia. Diante desse vácuo, o presente trabalho se propõe a analisar se o armazenamento de dados pessoais em investigações criminais e no processo penal está em conformidade com os princípios do direito à proteção de dados e se os institutos processuais clássicos estão atualizados para lidar com essas transformações.

No Brasil, desde a aprovação da Lei Geral de Proteção de Dados (LGPD), a discussão principal em relação à proteção de dados pessoais tem se concentrado na atuação das grandes empresas de tecnologia e no compartilhamento de dados pelo setor público. Contudo, poucos são os estudos que se debruçaram sobre o tratamento de dados no processo penal, e menos ainda aqueles que abordam uma das formas de tratamento: o armazenamento de dados.

De acordo com o banco de teses e dissertações da Biblioteca Brasileira de Teses e Dissertações, embora haja trabalhos que abordem o tema da proteção de dados no processo penal, a forma de tratamento concernente ao armazenamento de dados não é abordada de modo específico. No contexto internacional, em pesquisa realizada no Open Access Theses and Dissertations por meio das palavras-chave *personal data protection, data storage, criminal investigation, criminal procedure, criminal law, criminal justice system*, foram encontradas teses que abordam dados pessoais nas investigações, porém com o foco voltado não para o

[29] Foi firmado acordo de cooperação entre a Polícia Federal e o Serviço Europeu de Polícia Europol – promulgado pelo Decreto n. 10.364/2020 –, para atividades de inteligência estratégica, mas sem a possibilidade de transferência de dados pessoais, conforme seu art. 1º.

armazenamento de dados, mas sim mirando a legalidade de algumas formas de investigação, a exemplo do trabalho *The legality of DNA databases in the* criminal investigation[30].

O artigo de González Cano, *Cesión y tratamiento de datos personales en el proceso penal*[31] discute a importância de que a atividade de obtenção de provas seja regida pelos princípios da especialidade, idoneidade, excepcionalidade, necessidade e proporcionalidade, em razão das restrições ao direito fundamental à proteção de dados.

O artigo de Montoro Sánchez, *Los principios rectores del tratamiento de datos de carácter personal y sus implicaciones en el proceso penal*[32], embora aproxime o tratamento de dados ao processo penal, não aborda especificamente as formas de tratamento de dados nem as especificidades das técnicas de investigação tratadas nesta tese.

A tese de Gómez Rodríguez, *Aspectos procesales de los delitos informáticos y tecnológicos*[33] traz considerações relevantes sobre a relação entre o direito e a tecnologia, porém com ênfase em questões processuais.

O artigo de Laro González[34], examina a relação entre proteção de dados e processo penal com foco na Diretiva Policial 680.

Assim, embora as obras mencionadas estejam alinhadas ao objetivo desta tese, especialmente no que tange ao diálogo entre o direito à autonomia informacional e o processo penal, não têm a especificidade proposta neste trabalho. Esses estudos carecem de análises sobre as formas específicas de tratamento de dados pertinentes ao armazenamento e não abrangem as medidas de investigação tecnológica em cada uma de suas particularidades.

Diante desse cenário, há necessidade de pesquisa focada no armazenamento de dados pessoais nas investigações criminais e no processo penal, preenchendo a lacuna deixada na academia em relação a um problema de grande importância prática. Desse modo, a originalidade deste trabalho reside na investigação detalhada desse problema, na apresentação

---

[30] Galea, Dianne. *The legality of DNA databases in the criminal investigation.*Degree: 2016, University of Malta URL: https://www.um.edu.mt/library/oar/handle/123456789/17285

[31] GONZÁLEZ CANO, M. Isabel. Cesión y tratamiento de datos personales en el proceso penal. Avances y retos inmediatos de la Directiva (UE) 2016/680. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, v. 5, n. 3, p. 1331-1384, set./dez. 2019. Disponível em: https://doi.org/10.22197/rbdpp.v5i3.279. Acesso em: 1 nov. 2024

[32] MONTORO SÁNCHEZ, Juan Alejandro. Los principios rectores del tratamiento de datos de carácter personal y sus implicaciones en el proceso penal. *Revista Acta Judicial*, n. 10, p. 37-73, jul.-dez. 2022

[33] GÓMEZ RODRÍGUEZ, Álvaro. *Aspectos procesales de los delitos informáticos y tecnológicos*. 2021. 403 f. Tese (Doutorado em Ciências Sociais e Jurídicas) – Universidad Rey Juan Carlos, Escuela Internacional de Doctorado, Madrid, 2021

[34] LARO GONZÁLEZ, María Elena. Nuevos horizontes para el derecho de protección de datos personales, al amparo del nuevo reglamento general de protección de datos y de la directiva relativa al tratamiento de datos personales en el ámbito penal. *Anuario de la Facultad de Derecho*, Universidad de Extremadura, n. 38, p. 503-516, 2022. Disponível em: https://www.unex.es/contenido/artigo/Laro_nuevos_horizontes_para_el_derecho.pdf. Acesso em: 4 out. 2024.

dos desafios para sua implementação diante das limitações legais e técnicas impostas pela legislação e pela prática, e na proposição de formas de instrumentalização desse direito.

A abordagem do problema da pesquisa será marcada por uma constante tensão entre a busca pela eficiência na persecução penal e a proibição do devassamento, entre a rapidez das inovações tecnológicas e a cautela do Direito, além da falta de unidade entre a jurisprudência (prática útil) e a ciência (teoria). A partir desse tortuoso caminho, onde se busca um equilíbrio entre a aplicação da lei e a preservação dos direitos fundamentais, pode ser que, no futuro, consigamos alcançar uma melhor harmonia entre Direito e tecnologia.

Certamente, em alguns anos, a academia não mais se ocupará das inquietações mencionadas neste trabalho, o que nos remete à tese[35] de livre docência do Prof. Augusto Tavares Rosa Marcacini na Universidade de São Paulo a respeito dos impactos da máquina datilográfica nos processos judiciais no início do século passado. Com a substituição do papel e tinta, havia muitas dúvidas quanto à autenticidade das peças e o receio de que decisões fossem conhecidas antes da publicação oficial[36]. Atualmente, a maior parte dos operadores do Direito sequer manuseou uma máquina datilográfica, mas, naquela época, seu uso causava inquietações quanto à integridade e higidez do processo.

Portanto, este trabalho se propõe a abordar e analisar as dificuldades e insuficiências na garantia do direito à proteção de dados nas investigações criminais e no processo penal, especialmente no que se refere ao armazenamento de dados, resultando em propostas práticas e legislativas para sanar esses problemas. Para isso, a pesquisa será estruturada em quatro capítulos, cada um compondo uma parte do mosaico que formará a tese e responderá ao problema de pesquisa.

O capítulo um desta tese apresenta o problema, a hipótese e as lacunas do debate. Por fim, é oferecida uma explicação detalhada sobre a metodologia adotada no desenvolvimento da pesquisa, para orientar os leitores quanto aos limites e escopo do trabalho.

---

[35] MARCACINI, Augusto Tavares Rosa. *Processo e Tecnologia*: garantias processuais, efetividade e a informatização processual. 2011. 456 f. Tese (Livre Docência em Direito) – Universidade do Estado de São Paulo (USP), São Paulo, 2011. p. 28.

[36] "Duas allegações principaes fazem-se contra as sentenças datylographadas: a primeira de que facilita seu conhecimento antes de publicada, e a segunda, de que, não sendo indelével a tinta das machinas e podendo ser facilmente corrigido o escripto, póde este desaparecer, ou ser alterada a decisão. Nenhuma dessas alegações, porém, é procedente: quanto á primeira, basta que o juiz declare, no final da mesma, que foi ella por elle escripta em machina de seu uso; e quanto á segunda, os interessados devem pedir logo que a sentença fôr proferida, uma certidão della "verbo ad verbum", até que os juízes tomem a resolução, que pareça aconselhável, ou de mandar registrar suas sentenças, ou de determinar, ao remata-las, que o escrivão, sem perda de tempo, faça copia-la por pessoa de bôa caligraphia, de modo que as partes intimadas da sentença, poderão verificar a exactidão da copia". (SÃO PAULO. Tribunal de Justiça. Agravo n.º 16.886. Rel. Des. Antonino Vieira, 27 set. 1930. Revista dos Tribunais, São Paulo, n. 76, p. 100-101.)

O capítulo dois apresenta o debate sobre a proteção de dados na área criminal de forma mais ampla. Inicialmente, ele analisa o cenário atual do tratamento de dados no Brasil, tanto na teoria quanto na prática brasileira, destacando o atual framework regulatório composto pela LGPD, o Marco Civil da Internet, o Código de Processo Penal e a legislação criminal extravagante. As medidas práticas adotadas pelos órgãos de persecução penal são analisadas sob a luz da legislação vigente, considerando os direitos fundamentais à licitude, ao acesso, à informação e ao apagamento dos dados pessoais.

Em seguida, o capítulo dois explora a abordagem da União Europeia a respeito da proteção de dados no processo penal, com foco na Diretiva n. 2016/680, bem como decisões do Tribunal Europeu de Direitos Humanos (TEDH) a respeito do tema. Essa comparação internacional visa oferecer uma perspectiva mais ampla sobre como a proteção de dados é tratada em outros sistemas jurídicos.

Por fim, é discutido o conceito de "devido processo penal informacional" e como a tecnologia, juntamente ao armazenamento massivo de dados, impõe revisões nos institutos processuais tradicionais, como o contraditório e a publicidade. O objetivo do capítulo é apresentar violações à proteção de dados no processo penal brasileiro, utilizando também a perspectiva europeia como parâmetro.

O terceiro capítulo da tese aborda o armazenamento de dados nas investigações criminais, como foco em como as transformações tecnológicas influenciam diretamente as práticas investigativas. Serão analisadas técnicas de investigação pertinentes ao acesso a dispositivos de armazenamento em massa, interceptações telemáticas e telefônicas, vigilância eletrônica, infiltração online, além dos desafios relacionados à preservação da privacidade e proteção de dados. Na análise de cada uma dessas técnicas, se procurará demonstrar o arcabouço legal brasileiro, sua capacidade para tutelar o direito à proteção de dados, eventuais omissões e imperfeições da legislação. O capítulo buscará evidenciar as lacunas legislativas existentes no Brasil em comparação com os modelos europeus, especialmente o espanhol, e ressaltará a necessidade de regulamentação específica para equilibrar a eficácia investigativa com a proteção de dados, particularmente em relação ao armazenamento massivo de informações.

Também serão discutidos temas relacionados à eliminação de dados irrelevantes, destacando a importância de adotar medidas que garantam o uso exclusivo das informações estritamente necessárias ao processo penal. O objetivo específico do capítulo três é detalhar as principais técnicas especiais de investigação, explicando como essas práticas permitem a captação e o armazenamento de grandes quantidades de dados pessoais nos arquivos policiais,

a fim de confrontá-las com o direito à proteção de dados e os dispositivos legais pertinentes ao armazenamento de dados. Em essência, o capítulo se propõe a responder se o armazenamento de dados nas investigações criminais está em conformidade com o direito à proteção de dados.

A partir do confronto entre a prática e os textos legais, é possível compreender as limitações à proteção de dados e à privacidade. O debate sobre a proteção de dados na investigação criminal apresenta dois desafios principais. O primeiro é a ausência de uma legislação específica que regule as técnicas especiais de investigação, garantindo que estejam consoantes com o direito à proteção de dados. O segundo é equilibrar as necessidades dos órgãos de persecução penal com os direitos à autodeterminação informacional e à privacidade.

Por fim, o capítulo quatro analisa como a digitalização do processo penal exige a adaptação de institutos processuais clássicos, especialmente o princípio da publicidade, diante do armazenamento massivo de dados pessoais e os riscos associados à exposição dessas informações. O objetivo específico é discutir se o armazenamento de dados pessoais no processo penal está em conflito com a proteção de dados. Primeiramente, abordaremos o risco adicional que o processo eletrônico traz à proteção de dados pessoais na esfera criminal e como isso demanda uma nova interpretação do princípio da publicidade. Em seguida, discutiremos as obrigações relacionadas ao tratamento adequado dos dados armazenados, frequentemente negligenciadas no processo penal.

A conclusão trará um resumo das teses menores abordadas em cada capítulo, funcionando como um mosaico que responde ao problema da pesquisa. Com base nas conclusões de cada um desses capítulos, pretende-se, pois, finalmente responder ao problema da pesquisa de forma definitiva e propor medidas legislativas e práticas para concretizar o direito à proteção de dados na persecução penal, com ênfase no armazenamento de dados. Por fim, traz diretrizes para regulamentação da matéria pelo Conselho Nacional de Justiça.

Em relação ao recorte metodológico, é importante destacar que a pergunta que orienta esse trabalho diz respeito à realidade jurídica brasileira. Pela semelhança dos modelos de regulação de proteção de dados adotados pelo GDPR e pela LGPD, é esperado que as discussões europeias reverberem em solo brasileiro. No entanto, a transposição de debates e interpretações exige um imenso cuidado, de modo que a importação de conceitos não ocorre de forma simples.

Isso posto, cabe realizar algumas ponderações sobre as escolhas metodológicas. A tese trata da conformação do direito à proteção de dados com a prática de armazenamento de dados nas investigações e no processo penal. Assim, as escolhas sobre os temas abordados se limitaram ao objetivo de esclarecer o problema do armazenamento de dados pessoais na persecução penal no contexto brasileiro.

Cabe ressaltar que os países europeus contam com a LGPD penal ao nível comunitário, a proteção de dados é considerada na legislação penal interna sobre meios de investigação. Em geral, a atividade policial de investigação é desenvolvida com base em normas prévias e específicas. O Brasil, por sua vez, está a um passo atrás em todos esses aspectos. Este trabalho, portanto, embora realize uma pergunta originada em debate realizado no continente europeu, não pode importar as respostas. Nossa resposta deve ser construída a partir do direito brasileiro, embora se reconheça a influência europeia para a construção da nossa LGPD e incorporação do direito à proteção de dados na Constituição Federal.

Apesar das semelhanças, a LGPD e o GDPR são dois regulamentos que se inserem em sistemas jurídicos distintos. Para o caso brasileiro, além dos temas comuns ao debate europeu, é preciso observar as regulações pertinentes ao processo judicial eletrônico, os conceitos de *open court* e transparência mais alinhados com os Estados Unidos e a Inglaterra, os precedentes judiciais que abordaram o tema da proteção de dados, e a praxe policial e judicial que se mostra distinta da prática europeia.

Portanto, apesar da utilização de diferentes ordenamentos e documentos de outras jurisdições, esta tese não é um trabalho de direito comparado. As comparações eventualmente feitas visam trazer a perspectiva europeia sobre a proteção de dados na persecução penal, a fim de estimular uma reflexão mais aprofundada sobre as decisões tomadas em solo brasileiro. Utilizamos também a literatura estrangeira, especialmente da Espanha, por ser o local onde foi realizada a fase de investigação da tese doutoral, para abordar temas comuns à disciplina da proteção de dados, sem, contudo, estabelecer comparações específicas entre sistemas jurídicos. Assim, este trabalho não compara sistemas jurídicos, mas analisa um aspecto específico, utilizando experiências de outros países para embasar interpretações do sistema brasileiro. Nesse sentido, a análise da doutrina, legislação e precedentes é entendida como uma possibilidade de interpretação e não como uma resposta definitiva para os nossos problemas.

No campo jurídico, o debate inclui a interpretação do direito à proteção de dados na persecução penal, as possíveis interpretações das cortes europeias e os princípios gerais da proteção de dados, além dos limites e falhas do GDPR em abordar problemas relacionados ao armazenamento de dados nas investigações criminais e no processo penal. É importante destacar que o problema do armazenamento de dados pessoais envolve discussões em diversos campos, dos quais não é possível extrair uma síntese definitiva. Trata-se de questões políticas e sociais em disputa, cujas soluções jurídicas continuam em construção.

Portanto, este trabalho é desenvolvido a partir de uma escolha metodológica que abrange diferentes campos da disciplina jurídica, considerando distintos ordenamentos e abordagens

multidisciplinares, com foco na compreensão de uma questão específica sobre a existência de um direito. As principais fontes utilizadas na tese podem ser divididas da seguinte forma:

i) Em primeiro lugar, como condição essencial do trabalho, partiu-se uma análise dos dispositivos constitucionais e regulações pertinentes ao tratamento de dados, como a GDPR e a LGPD. Em seguida, avançou-se sobre o framework legislativo brasileiro pertinente à proteção de dados na persecução penal, técnicas especiais de investigação, normas pertinentes ao processo judicial eletrônico, particularmente a Lei 13.709/2018, a Lei 9296/1996, a Lei 12.965/2014, a Lei 12.850/2013 e o Código de Processo Penal. Nesse sentido, mapearam-se as diferenças e similaridades dos dois ordenamentos quanto ao armazenamento de dados nas investigações criminais e no processo penal.

ii) Além das fontes legais, esta tese fundamentou sua análise nos principais trabalhos que discutiram o tratamento de dados no processo penal, tanto no contexto brasileiro, quanto europeu, especialmente espanhol, como meio de elencar principais argumentos e lacunas nesses trabalhos.

iii) A resposta aos questionamentos sobre o tema dependeu do estudo sobre os princípios da proteção de dados, especialmente relacionados à persecução penal no contexto europeu e brasileiro. A pesquisa bibliográfica pretende ganhar verticalidade em temas tangentes ao armazenamento de dados na persecução penal, como técnicas especiais de investigação, processo judicial eletrônico, antecedentes criminais, princípio da publicidade, e devido processo informacional, de modo a auxiliar na resposta ao problema da pesquisa.

iv) Além dessas abordagens, o trabalho utiliza análise de precedentes da justiça brasileira e europeia sobre proteção de dados, especialmente no contexto da persecução penal. No direito europeu pesquisou-se a base do Tribunal de Justiça da União europeia (TJUE), bem como o Tribunal Europeu de Direitos Humanos (TEDH) de Estrasburgo.

Com base nesses trabalhos e na síntese interpretativa realizada pelo trabalho, foi possível construir uma proposta de instrumentalização do armazenamento de dados na persecução penal à luz do direito à proteção de dados, compondo o último capítulo desta tese.

# 5 CONCLUSÃO: O FIM É DE ONDE COMEÇAMOS[37]

## I

O processo penal não pode mais avançar sem incorporar o direito à proteção de dados como um de seus pilares centrais. Ignorar essa necessidade coloca em risco a própria essência do processo penal, que historicamente tem sido um garantidor de direitos fundamentais, transformando-o em um mecanismo que, paradoxalmente, viola esses mesmos direitos. Por isso, o armazenamento de dados pessoais para persecução penal não pode continuar nos rumos atuais por mera inércia ou tradicionalismo, sem a devida reflexão crítica[38]. Em uma sociedade democrática, a vida dos indivíduos não pode se tornar um livro aberto à absoluta devassa disfarçada do pretexto de eficiência estatal.

Carnelutti descreveu o processo penal como a "Cinderela do Direito Processual", perdida entre o Direito Penal material e o Direito Processual Civil. Hoje, podemos ver o direito fundamental à proteção de dados na persecução penal como uma nova Cinderela, negligenciado na prática e na legislação devido a sua aparente irrelevância. Contudo, assim como no conto de fadas, esse direito inevitavelmente acabará reivindicando seu papel de protagonista[39].

Este trabalho teve como uma de suas pretensões lançar as bases para uma discussão que tem sido amplamente negligenciada, tanto pela academia quanto pelos operadores do sistema de justiça criminal, a respeito do armazenamento de dados pessoais no processo penal. Além disso, a pesquisa buscou, a todo tempo, transitar entre a teoria e a prática, com o desejo, talvez ingênuo, de aproximar os livros da realidade. Ninguém conseguiu expressar tão bem essa ideia quanto Cora Coralina, poetisa da minha terra: “O saber a gente aprende com os mestres e os livros. A sabedoria, se aprende com a vida e com os humildes”.

---

[37] What we call the beginning is often the end / And to make and end is to make a beginning. / The end is where we start from. ELIOT, T. S. *Little Gidding*. Disponível em: https://www.columbia.edu/itc/history/winter/w3206/edit/tseliotlittlegidding.html. Acesso em: 16 out. 2024.

[38] "A serpente que não pode mudar sua pele tem que morrer. Assim também as mentes que são impedidas de mudar suas opiniões deixam de ser mentes" (NIETZSCHE, Friedrich. *Assim falou Zaratustra*. Tradução de Mário da Silva. São Paulo: Companhia das Letras, 2011). "A foolish consistency is the hobgoblin of little minds" (EMERSON, Ralph Waldo. *Self-Reliance*. [*S. l.*]: Project Gutemberg, 1841. Disponível em: https://www.gutenberg.org/ebooks/16643. Acesso em: 17 out. 2024).

[39] PÉREZ GIL, Julio. Medidas de investigación tecnológica en el proceso penal español: privacidad vs. eficacia en la persecución. *In*: BRIGHI, Raffaella; PALMIRANI, Monica; SÁNCHEZ JORDÁN, María Elena (ed.). *Informatica giuridica e informatica forense al servizio della società della conoscenza:* scritti in onore di Cesare Maioli. [*S. l.:s. n.*], 2018. p. 187-198.

## II

No capítulo 2 demonstrou-se que o armazenamento massivo de dados na persecução penal é um problema real no Brasil, embora pouco conhecido, o que dificulta a criação de contramedidas legislativas e práticas. Como evidência, a Lei 13.709/2018 exclui expressamente de seu escopo o tratamento de dados para atividades de investigação e repressão de crimes, o que enfraquece direitos fundamentais relacionados à licitude, acesso, informação e apagamento na proteção de dados no processo penal. Também foi analisado o quadro normativo na União Europeia e a evolução do direito à autonomia informacional, evidenciando a falta de maturidade dessa questão no Brasil.

A partir dessa análise, apresentou-se o marco regulatório brasileiro, no qual as Leis 9.296/1996, 12.850/2013 e 12.965/2014 regulam as medidas de investigações tecnológicas, mas não incluem disposições específicas sobre a proteção de dados. A Lei 12.965/2014 (Marco Civil da Internet) e a Lei 13.709/2018 foram consideradas insuficientes para regulamentar a proteção de dados na esfera criminal. Demonstrou-se que o uso de analogias e interpretações extensivas tem sido uma prática comum, o que compromete o princípio da licitude. Além disso, foi discutida a insuficiência da Convenção de Budapeste sobre Cibercrime, promulgada pelo Decreto nº 11.491/2023, para suprir o vazio normativo na proteção de dados na persecução penal.

No estudo do modelo europeu, destacaram-se as principais disposições da Diretiva Policial 2016/680, visando apontar as lacunas da legislação brasileira em comparação à diretiva europeia. Ressaltou-se o princípio da licitude, que exige fundamento legal para o tratamento de dados; o direito à informação, que preza pela transparência nas ações de tratamento; e a necessidade de limitar o tratamento de dados ao estritamente necessário para atingir os objetivos. Esses pilares sustentam outros princípios, como segurança, minimização, limitação de conservação, categorização, proteção de dados sensíveis, registro de operações, anonimização e cifragem. Também foi discutido como a Diretiva Policial 2016/680 aborda o armazenamento de dados, impondo regras claras sobre informação, retificação e apagamento. A transposição da diretiva pela Espanha foi apresentada como um exemplo de regulação eficaz das medidas de investigação tecnológica, garantindo a proteção de dados.

Em seguida, discutiu-se que a manutenção do atual modelo brasileiro pode prejudicar investigações transnacionais, especialmente quando envolvem o acesso a dados pessoais armazenados na União Europeia ou relacionados a cidadãos europeus. Por fim, questionou-se se a criação de uma LGPD Penal seria suficiente para solucionar os problemas apontados, destacando a falta de diálogo entre a proteção de dados e o direito processual penal, bem como

o vazio normativo que compromete o princípio da licitude devido ao uso excessivo de analogias e interpretações extensivas.

Após a análise do quadro regulatório brasileiro, cujo objetivo foi evidenciar a ausência de normas específicas para a proteção de dados no processo penal, especialmente no que se refere ao armazenamento de dados pessoais, abordou-se o direito à informação e ao acesso. Essa análise se justifica porque, sem conhecimento do tratamento de dados, o direito ao apagamento não pode ser exercido. E sem o apagamento, o problema do armazenamento excessivo de dados nas investigações permanece sem solução. O direito à proteção de dados só é efetivo se o titular for informado sobre quem possui seus dados e para qual finalidade.

Embora o Brasil preveja, em parte, o direito à informação no art. 5º, incisos XIV, XXXIII e LXXII da Constituição Federal, que asseguram o acesso à informação e ao habeas data; no art. 37, *caput* e § 3º, que trata do princípio da publicidade e da participação do usuário na administração pública; no art. 93, IX, e no art. 216, § 2º, que reforçam a transparência judicial e administrativa; no art. 6º da LGPD, que trata da boa-fé no tratamento de dados; e na Lei de Acesso à Informação (Lei nº 12.527/2011), a legislação nacional confere um direito reativo, e não proativo. Isso significa que o interessado deve solicitar ativamente o acesso às informações, o que revela a ineficácia da legislação de acesso à informação no contexto das investigações criminais. Geralmente, aqueles que não foram denunciados, mas foram afetados por medidas investigativas, desconhecem a captação e o armazenamento de seus dados pessoais. Portanto, a legislação brasileira não se alinha à Diretiva Policial, que impõe transparência no tratamento de dados e o dever de notificar os afetados.

No que diz respeito ao direito de apagamento, evidenciou-se a relação direta entre esse direito e o armazenamento massivo de dados na investigação criminal e no processo penal. O direito ao apagamento é uma solução para o problema do excesso de captação de dados, especialmente quando essas informações se tornam desnecessárias ou inúteis. O caso *Google Spain* foi utilizado como ponto de partida para discutir o direito ao esquecimento, com base nos artigos 7º e 8º da Carta dos Direitos Fundamentais da União Europeia (CDFUE) e no artigo 8º da Convenção Europeia para a Proteção dos Direitos Humanos e das Liberdades Fundamentais (CEDH), que fundamentam as decisões do TJUE e do TEDH.

Além do direito ao apagamento previsto na Diretiva Policial, analisou-se a legislação nacional, especialmente o art. 9º da Lei 9.296/1996, os artigos 93 e 94 do Código Penal e a Lei 12.654/2012, para verificar se são suficientes para garantir o direito ao esquecimento. Por fim, foram examinados casos julgados pelo TEDH, como *S. e Marper v. Reino Unido* (2008), *Peruzzo e Martens v. Alemanha* (2013), *Gaughran v. Reino Unido* (2020), *Ayçaguer v. França*

(2017), *M.M. v. Reino Unido* (2012), *Khelili v. Suíça* (2011), *M.K. v. França* (2013) e *Catt v. Reino Unido* (2019). A análise desses casos mostrou como o TEDH equilibra a retenção de dados com o direito à privacidade, destacando a necessidade de revisões periódicas, exclusão de dados e salvaguardas adequadas para proteger os direitos fundamentais.

Por fim, abordou-se o devido processo penal informacional, destacando que a tecnologia e o armazenamento massivo de dados exigem mudanças nos institutos jurídicos clássicos. O devido processo legal, em sua concepção atual, não garante mais plenamente um processo justo na esfera criminal, devido ao volume de dados e ao uso de ferramentas de inteligência artificial, que alteraram a natureza do processo. A legislação brasileira carece de salvaguardas específicas para lidar com o armazenamento massivo de dados no processo penal.

Como solução para o redesenho do devido processo legal, sugeriu-se a incorporação dos princípios da proteção de dados (art. 6º da LGPD), como finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e prestação de contas. A adoção desses princípios, juntamente com o foco nos direitos à informação, acesso e apagamento, além da integração entre o processo penal e os princípios da proteção de dados, oferece um caminho viável para reequilibrar o cenário constitucional impactado pela tecnologia.

Também foi destacada a importância das Avaliações de Impacto sobre a Privacidade (PIAs) como medidas práticas para gerenciar riscos à privacidade ao adotar tecnologias potencialmente invasivas em investigações criminais, com foco na necessidade, adequação, eficácia e proporcionalidade.

## III

No capítulo 3, foram analisadas as principais técnicas especiais de investigação capazes de coletar e armazenar de grandes volumes de dados pessoais em processos criminais. A criação de uma sociedade digital e conectada provocou uma mudança profunda na forma de investigar crimes. O uso da internet, aplicativos e dispositivos eletrônicos estabeleceu uma "vida digital", uma dimensão em que as pessoas se relacionam e, por vezes, praticam delitos. Diante dessa nova realidade, parte significativa da investigação criminal contemporânea concentra-se na coleta, armazenamento e análise de dados pessoais com o objetivo de verificar a existência de um crime e identificar sua autoria. Nessa vertente, as investigações tendem a se concentrar na captação e análise de dados em larga escala, utilizando métodos como o acesso a dispositivos

de armazenamento em massa, interceptação telemática, acesso a registros de conexão e aplicativos, vigilância eletrônica e infiltração online.

Um dos principais gargalos do sistema jurídico brasileiro em relação às medidas de investigação tecnológica está no vácuo normativo. Não há legislação que regule adequadamente os desafios atuais desses meios de obtenção de prova e que alinhe o processo penal com a proteção de dados. Com efeito, a Lei nº 9.296/1996 é frequentemente invocada para justificar medidas que não se enquadram como interceptação telefônica, telemática ou escuta ambiental, como o acesso a dispositivos de armazenamento em massa e a registros de conexão. A Lei nº 12.965/2014, o Marco Civil da Internet, embora preveja a obtenção de registros de conexão e aplicação, não regula a forma como essas diligências são realizadas, não tem catálogo de crime e não prevê prazos para as medidas.

Não se mostra correto o uso de analogia e interpretação extensiva da Lei nº 9.296/1996 para a decretação de medidas investigativas invasivas, tampouco a aplicação de normas que não são direcionadas para a área criminal, como o Marco Civil da Internet. Apoiar essas medidas apenas no texto constitucional, sem uma lei ordinária específica para a área criminal e com a devida densidade normativa, implica na necessidade do Poder Judiciário regulamentar detalhadamente as técnicas de investigação, o que esvazia a exigência constitucional de deliberação democrática pelo Congresso Nacional e compromete o princípio da legalidade e a tipicidade processual.

Com o reconhecimento do direito à proteção de dados na Constituição Federal, as leis que regulam os meios de investigação devem especificar como ocorrerá o tratamento de dados pessoais, estabelecendo regras e prazos para armazenamento, diretrizes para compartilhamento, medidas para minimizar vazamentos e normas para a exclusão dos dados, entre outros aspectos. A inclusão da proteção de dados como direito fundamental reforça a necessidade de que os meios de obtenção de prova contemplem disposições específicas sobre o tratamento de dados.

Diante das dificuldades impostas pela criptografia e por questões jurisdicionais à interceptação da comunicação telemática, abriu-se um novo caminho com a possibilidade de apreensão de celulares e outros dispositivos de armazenamento em massa. Esse acesso permite explorar um universo de dados muito mais amplo do que aquele oferecido pela interceptação telefônica.

Uma das particularidades do acesso a dispositivos de armazenamento em massa é que os dados pessoais acessados e apreendidos, ainda que irrelevantes para a investigação e não classificados como prova, permanecem armazenados indefinidamente. Nesses arquivos digitais, encontram-se tanto informações irrelevantes do proprietário do dispositivo quanto

dados de terceiros inevitavelmente atingidos com a medida. Essa prática resulta na criação de extensos arquivos de dados pessoais, que, por não serem apagados e muitas vezes sequer informados aos seus titulares, ficam sujeitos a novas formas de tratamento, vazamentos e uso indevido.

A resistência inicial da jurisprudência brasileira à ideia de que o acesso a dispositivos de armazenamento em massa, como celulares, representa uma ameaça à privacidade foi superada por uma compreensão mais aprofundada sobre a natureza e o volume das informações sensíveis que esses dispositivos armazenam. Reconheceu-se que os dados contidos em celulares podem oferecer uma visão altamente intrusiva da vida pessoal de um indivíduo, tornando imprescindível a obtenção de autorização judicial para seu acesso.

A Lei 9.296/1996 tem sido aplicada por analogia para acesso a dispositivos de armazenamento em massa, como se esse procedimento fosse equivalente a uma interceptação telemática. Contudo, observa-se que o art. 1 da Lei 9.296/1996 refere-se especificamente à interceptação do fluxo de comunicações em sistemas de informática e telemática, o que é distinto de acesso a dados de armazenamento em massa. O acesso a dispositivos de armazenamento em massa pode ser autorizado com fundamento no art. 7, inciso III, da Lei nº 12.965/2014. Contudo, a falta de regulamentação a respeito de como se dará o procedimento, o catálogo de crimes e requisitos da decisão judicial demonstra que o Marco Civil da Internet não é vocacionado para o processo penal, mas sim para estabelecer parâmetros gerais para a proteção da privacidade e dos dados pessoais.

A interceptação telefônica frequentemente resulta na coleta de uma quantidade significativa de informações e dados pessoais que, em sua maioria, são irrelevantes para a investigação. Isso ocorre porque além dos diálogos criminosos, tem capacidade para captar tudo que foi falado pelos investigados, sendo uma medida invasiva por excelência. A exemplo de outras técnicas de investigação, a Lei 9.296/1996, apesar de prever o descarte de diálogos que constituam meios de prova no art. 9, não regula o apagamento dos dados de terceiros ou dos investigados, mas que não constituam prova, o que contribui para o acúmulo do armazenamento de dados nos arquivos policiais.

A vigilância eletrônica é uma espécie moderna de campana policial ou levantamento de campo, destinada a produzir informação sobre o investigado, seus contatos e os locais frequentados, que podem revelar bens e documentos ocultos, circunstâncias do crime e localização de vítimas de crimes.

No Brasil, embora não haja previsão legal expressa, a vigilância policial vem sendo admitida, inclusive com reconhecimento de que prescinde de autorização judicial se localizada

em locais públicos, por não violar a intimidade (art. 5, X, CF). Somente quando realizada em recintos fechados, protegidos pela cláusula de inviolabilidade domiciliar, a observação e acompanhamento policiais devem ser precedidos de mandado da autoridade judiciária competente.

A maioria dos dados captados não tem interesse para as investigações, e fração destes dados continuam interligados com dados de terceiros. Essas características da vigilância eletrônica reforçam a necessidade de limitar a coleta apenas ao que é estritamente necessário para o caso, assim como regulamentar apagamento dos dados que não constituam em provas.

A infiltração online consiste na prática de acessar remotamente computadores e smartphones sem o conhecimento dos usuários, com o propósito de examinar o conteúdo armazenado e extrair dados informáticos que sirvam como provas. Em regra, a infiltração online se operacionaliza por meio de infecções de códigos e softwares nos dispositivos eletrônicos e sistemas informáticos do investigado, por meio de link malicioso, engenharia social ou falso aviso de atualização de sistema operacional, estratégias conhecidas como *policeware*. A infiltração online é inadmissível no Brasil por falta de previsão legal.

Acesso a dados de localização consiste em técnica especial de investigação utilizada para identificar a localização de um dispositivo, como um smartphone, seja a partir da triangulação de sinais de celular, GPS, ou acesso a dados de aplicativos que rastreiem a localização. Também pode ocorrer acesso a registros de conexão e acesso a aplicativos. No Brasil, sustenta-se essa prática com amparo no artigo 22 do Marco Civil da Internet.

Em relação à constitucionalidade do art. 22 da Lei 12.965/14, é imprescindível realizar uma interpretação conforme para incorporar os princípios do tratamento de dados previstos na LGPD. Nessa perspectiva, deve ocorrer anonimização dos dados, informação aos atingidos pela medida, atenção à finalidade da captação dos dados pessoais, e, especialmente, apagamento dos dados assim que a análise inicial descartar suspeitos e pessoas sabidamente inocentes.

Os dados de localização que não mais interessarem às investigações devem ser excluídos dos registros policiais. Com muito mais razão, os dados provenientes de mandados de busca de localização reversa também devem ser excluídos após as investigações afunilarem a lista dos suspeitos, pois contemplam dados pessoais de terceiros inocentes que estavam em determinada área em dado momento. Por fim, os dados de localização utilizados em processos criminais também devem ser excluídos em algum momento após o trânsito em julgado.

Devem ser incorporados nos autos apenas os dados catalogados como prova, desde que não comprometam significativamente a privacidade de terceiros não envolvidos no processo. Se a violação à privacidade for severa, deve haver a segregação da base de dados do processo.

Os dados pessoais que não forem classificados como prova devem ser disponibilizados apenas a seus titulares.

## IV

No capítulo 4, demonstrou-se como o processo em formato eletrônico distorceu institutos clássicos como os princípios da publicidade, do contraditório e do devido processo legal.

O Processo[40] (*Der Prozess*), escrito por Franz Kafka e publicado em 1925, serve como um contraexemplo para a comunidade jurídica, ao retratar um sistema judicial opressivo, burocrático e impenetrável. O cenário distópico dessa obra decorre dos perigos de um sistema desumanizado e desprovido de transparência, marcado pela falta de liberdade, desesperança e impotência.

Por outro lado, no processo eletrônico, ocorre justamente o contrário do processo de Kafka. Aqui, o sofrimento é causado não pelo sistema fechado e incompreensível, mas por um cenário altamente público, em que a privacidade dá lugar para um cenário em que todos sabem tudo sobre todos.

O direito deve ser compreendido a partir de sua função de realizar valores, cujo centro se encontra o valor da pessoa humana. O processo, dentro dessa perspectiva, emerge como instrumento de concretização do direito. Ada Pellegrini Grinover[41] enfatiza a importância de se interpretar as normas processuais à luz dos princípios e regras constitucionais. Além dessa constitucionalização do processo penal, outra tendência manifestada nas últimas décadas é a internacionalização desse ramo do direito, principalmente mediante a atribuição de status constitucional às normas de direitos humanos dos tratados internacionais. A face substancial do devido processo legal se evidencia por meio da aplicação de normas que sejam proporcionais e justas[42].

No capítulo 4 são tratadas questões cruciais, como: o princípio da publicidade foi excessivamente ampliado nos processos penais eletrônicos? Quais dados captados nas técnicas de investigação precisam ser obrigatoriamente anexados ao processo? Os réus devem ter acesso ao material captado e armazenado nos arquivos policiais, inclusive o que não foi anexado aos

---

[40] KAFKA, Franz. *O processo*. Tradução de Modesto Carone. São Paulo: Companhia das Letras, 2005.
[41] FERNANDES, Antonio Scarance. *Processo Penal Constitucional*. 2. ed. São Paulo: Revista dos Tribunais, 2000. p. 15.
[42] FERNANDES, Antonio Scarance. *Processo Penal Constitucional*. 2. ed. São Paulo: Revista dos Tribunais, 2000. p. 45.

autos porque não foi elencado como prova, ainda que esse material envolva apenas terceiros e corréus? Quais dados pessoais devem ser apagados, e quando fazê-lo? Quais garantias são necessárias para proteger os dados armazenados? O acesso a dados armazenados representa ameaça à privacidade e à autonomia informacional? Os princípios da ampla defesa e do contraditório são efetivamente concretizados quando os réus, sem condições técnicas e econômicas, não conseguem interpretar a imensa quantidade de dados digitais envolvidos no processo, sem o suporte de ferramentas específicas de inteligência artificial?

O processo eletrônico foi desenvolvido pelo Conselho Nacional de Justiça para assegurar maior celeridade, modernidade e segurança processual, mas se descuidou da proteção de dados. A digitalização do processo ampliou excessivamente o princípio da publicidade processual, em razão da exposição desproporcionalde dados pessoais.

O sistema jurídico brasileiro enfrenta algumas incongruências estruturais. Tal se deve ao fato de que a LGPD brasileira tenha se inspirado na GDPR europeia, modelo que garante proteção de dados nos processos judiciais, mediante anonimização e limitação de consulta a dados do processo. Porém, no que tange à publicidade, o sistema brasileiro adota a ampla publicidade (*open courts*) nos sites dos tribunais, o que permite que todo advogado, ainda que sem procuração, tenha acesso aos autos, que terceiros alheios ao processo consultem as principais decisões (consulta pública). Em suma, no sistema judicial do Brasil, publicidade e proteção de dados não dialogam de maneira harmoniosa.

A publicidade processual se funda em três principais funções: possibilitar a participação e o controle externo do público sobre a atividade jurisdicional; proteger as partes contra juízos secretos e arbitrários; e promover o direito constitucional à informação. Todavia, diante da hiper publicidade trazida pelo processo eletrônico, questiona-se se o acesso facilitado dos autos processuais não compromete excessivamente outros direitos fundamentais, como a dignidade, a privacidade e a proteção de dados pessoais. Isso porque a publicidade intensificou-se de forma desproporcional com a transição para o processo eletrônico, afrontando os artigos 6º e 7º, da LGPD, que tratam da necessidade, finalidade e consentimento no tratamento de dados.

A consulta pública permite que, de forma anônima e sem controle do número de acessos por usuário, o processo seja consultado a qualquer momento e de maneira simples, inclusive por sistemas automatizados, o que facilita a captura, o processamento e o armazenamento de dados pessoais sensíveis. Os advogados, ainda que não representem as partes, têm o direito de acessar as decisões principais, e o inteiro teor do processo e documentos anexados, se não estiver sob segredo de justiça, independentemente de justificativa legítima.

Por mais contraintuitivo que pareça, o processo eletrônico pode, na verdade, reduzir o acesso à justiça em vez de ampliá-lo. Em relação às testemunhas, a exposição excessiva aumenta o risco de represálias, pressão social, autocensura, vergonha e medo, principalmente em questões que envolvem organizações criminosas, comunidades controladas por facções e julgamentos de grande repercussão midiática. Esses fatores podem levar testemunhas a omitir a verdade, e não se apresentarem espontaneamente em determinados casos. Os réus também se sentem menos encorajados em confessar crimes e delatar comparsas em processos eletrônicos com amplo acesso público. O silêncio deixa de ser adotado como estratégia de defesa ou simples exercício do direito, e passa a funcionar como meio de evitar a execração pública. Em síntese, o amplo acesso às informações constantes em processos judiciais alimenta uma indústria de intimidação que facilita o *bullying* entre partes e testemunhas. Embora esses problemas já existissem antes do processo judicial eletrônico, eles se intensificam com a possibilidade de que os depoimentos sejam facilmente acessados online por terceiros. Isso evidencia que a exposição excessiva pode gerar um efeito reverso no acesso à justiça, desestimulando o depoimento de testemunhas e réus. A abertura irrestrita de tudo a todos cria uma ilusão de acesso à justiça; na verdade, essa prática aumenta a desinformação e o medo.

A aplicação excessiva da publicidade no ambiente digital extrapola a finalidade de informar, transformando-se em um instrumento de exposição permanente e injustificada de dados pessoais. A publicidade processual não pode ser um fim em si, pois deve estar alinhada aos princípios da necessidade e da proporcionalidade, garantindo que apenas dados essenciais sejam mantidos e divulgados. Essa excessiva publicidade proporcionada pelo processo judicial eletrônico impõe a efetivação do direito ao esquecimento, fundamentado no art. 18, inciso VI, da Lei Geral de Proteção de Dados (LGPD), que assegura ao titular o direito de solicitar a eliminação de seus dados pessoais quando não forem mais necessários ou quando seu tratamento for excessivo.

O armazenamento permanente de dados pessoais no processo penal eletrônico pode fazer com que o processo se torne mais severo do que a própria pena imposta. Além das técnicas especiais de investigação, que por si só costumam captar e armazenar um volume muito maior de dados pessoais em comparação aos métodos tradicionais, nos processos complexos envolvendo organizações criminosas é comum que dezenas de pessoas sejam processadas nos mesmos autos, o que eleva exponencialmente a quantidade de dados pessoais armazenados em um único processo.

Essa realidade obriga a questionar se é possível impor algum tipo de limitação ou impedimento ao acesso dos réus a dados pessoais de terceiros, e conduz a outros

questionamentos: quais dados pessoais devem ser efetivamente armazenados no processo penal? O advogado sem procuração deve ter o direito de acessar a integralidade de qualquer processo, conforme preconiza o art. 7º do Estatuto da Advocacia (EOAB), ou se é razoável impor algum tipo de anonimização?

A exclusão das atividades de investigação e repressão de infrações penais do âmbito de aplicação da LGPD (art. 4º, III, "d") contribui para a não concretização do direito à proteção de dados na seara criminal, de modo que caminhamos para um estado de coisas inconstitucional na área de proteção de dados, assim como o Brasil se encontra em estado inconvencional.

A prática de amplo acesso público ao processo eletrônico está criando um tipo de registro criminal mais estigmatizante que as antigas folhas de antecedentes policiais abolidas pela CF/88. Isso ocorre porque permite a formação de inúmeros bancos de dados contendo registros de processos criminais em que determinada pessoa foi ré, testemunha ou tenha sido apenas mencionada, sem qualquer limitação temporal e sem controle do Estado. É inquietante pensar que o parágrafo único do art. 20 do CPP veda a anotação de inquéritos em curso nos atestados de antecedentes, mas, paralelamente, o acesso facilitado dos processos criminais a partir da internet torna possível obter informações processuais muito mais detalhadas.

Nos Estados Unidos, a publicidade dos registros, seguida por uma crescente indústria paralela de criação de bancos de dados, trouxe consequências negativas, como restrições a financiamentos, empregos, direitos políticos e benefícios sociais. Esses são os chamados efeitos colaterais de envolvimentos criminais. A iniciativa privada se apropriou de informações presentes em bancos de dados públicos e construiu suas próprias bases, por meio da agregação de diversas fontes.

Diversamente, na Espanha a regra geral é a não publicidade dos antecedentes criminais, conforme o art. 136 do Código Penal, premissa que também se aplica aos antecedentes policiais. Na Espanha, embora as sentenças sejam públicas, na prática, é distinto o direito do público de estar presente em juízo do direito de acesso às decisões judiciais e aos dados pessoais nelas contidos. No direito espanhol, as informações processuais penais e os antecedentes criminais são vistos como parte de uma engrenagem em que o direito à proteção de dados também atua.

O Brasil adota um modelo de acesso público a decisões judiciais, sem oferecer níveis adequados de proteção aos dados pessoais. Nesse aspecto, aproxima-se do sistema de *open courts* dos Estados Unidos e da Inglaterra, o que revela um certo contrassenso, pois a LGPD brasileira é claramente inspirada no modelo europeu, o qual impõe restrições à publicidade nos processos criminais. Se a jurisprudência admite apagar referências de processos criminais com absolvição da folha de antecedentes, deve também reconhecer o direito de retirar publicações

nos sites dos tribunais que mencionem essas informações. Na prática, o acesso público a processos criminais permite a obtenção de dados até mais abrangentes do que os contidos nas certidões de antecedentes, o que provavelmente incentivará a criação de bases de dados privadas.

No que diz respeito às salvaguardas jurídicas, a decretação de sigilo dos autos e a restrição de acesso a terceiros para leitura das peças processuais não são adequados para tutelar a proteção de dados. Isso porque a publicação dos acórdãos nos sites dos tribunais não são anonimizados e expõe frequentemente o nome completo dos réus.

Se a jurisprudência admite apagar referências de processos criminais com absolvição da folha de antecedentes, deve também reconhecer o direito de retirar publicações nos sites dos tribunais que mencionem essas informações. Ademais, por força do disposto no art. 93, IX, da Constituição Federal, o sigilo é exceção.

O segredo de justiça é insuficiente para garantir a proteção de dados também porque ainda que as portas do processo sejam fechadas ao público, o mundo interno permanece vasto, abrigando uma quantidade significativa de informações sobre diversos indivíduos e empresas, acessíveis a diversos sujeitos processuais. Mesmo nesse ambiente processual "protegido" do contato externo, os réus e terceiros inevitavelmente atingidos seguem expostos a sérios riscos devido ao armazenamento de seus dados pessoais.

Limitar a consulta pública e garantir o acesso integral dos autos apenas aos advogados que representem os réus não são medidas suficientes para resolver o problema, pois os dados pessoais continuariam expostos nos processos eletrônicos. No entanto, é válido questionar se a manutenção da consulta pública no formato atual, em que qualquer pessoa pode acessar o inteiro teor de decisões e sentenças, é realmente necessária para efetivar o princípio da publicidade.

Uma das propostas consiste na segregação da base de dados fora dos autos do processo. Nesse modelo, os sujeitos processuais teriam acesso ao banco de dados após um novo juízo de proporcionalidade, distinto daquele que fundamentou o afastamento inicial do sigilo de dados. Os dados pessoais de terceiros, sem relação direta com o fato criminoso, devem ser armazenados em uma base de dados segregada. O acesso a esses dados segregados somente ocorreria mediante nova decisão judicial. Nessa solução, são anexados ao processo apenas os dados obtidos que sejam necessários para demonstrar a cadeia de custódia, os dados pessoais dos acusados relevantes para o caso e as informações anonimizadas. Todavia, a segregação da base de dados de terceiros não abrange os dados dos investigados que constam nos arquivos

policiais, mas que não foram anexados ao processo porque as autoridades investigantes entenderam que são irrelevantes para o caso.

O princípio do contraditório não deve se limitar à mera possibilidade de defesa, mas garantir que ela seja efetivamente exercida, o que implica fornecer ao réu reais condições de analisar o vasto acervo de dados digitais incluídos nos autos. Assim, é questionável se a defesa terá reais condições de analisar todo o material no prazo de 10 dias para a resposta à acusação (CPP, art. 396), sem aplicativos específicos a seu dispor. Sem essas adaptações, o devido processo penal se distanciará, cada vez mais, de sua acepção substancial.

Além dos contra-ataques normativos, medidas administrativas adotadas pelos tribunais podem se mostrar eficazes. Os tribunais podem cumprir o dever de anonimizar os dados do processo, segundo o art. 5º, XI, da LGPD. Resta discutir se essa anonimização deve abranger apenas a consulta pública ou se também deve se estender aos advogados que não sejam procuradores das partes envolvidas no processo.

Impõe-se restringir certos critérios de busca, a exemplo da proibição de busca pelo nome das partes, permitindo-a apenas pelo número do processo. Também é necessário reformular o modelo de controle de acesso, que atualmente carece de gradações entre diferentes níveis.

Não se pode permanecer preso à visão clássica de princípios constitucionais como a publicidade, o contraditório e o devido processo legal, pelo menos da forma como foram concebidos para um mundo que já não existe. Se a aplicação desses princípios comprometer a proteção de dados e a privacidade, eles precisam ser ressignificados e atualizados para a realidade contemporânea.

## V

Ao final da pesquisa, conclui-se que a prática jurídica brasileira no contexto das investigações criminais e do processo penal estão desalinhadas com o direito à autonomia informacional, principalmente no que diz respeito ao armazenamento de dados pessoais. Diante desta constatação, e a fim de que este trabalho não se restrinja ao campo teórico, propõe-se a criação de um Sistema Nacional Unificado de Gestão de Dados Pessoais em Processos Criminais, com adoção de medidas práticas no âmbito do Conselho Nacional de Justiça em três frentes distintas: apagamento de dados pessoais, anonimização de dados pessoais e adoção de modelo de gestão de dados pessoais no âmbito das investigações criminais. Tais medidas não excluem a premente necessidade de edição de nova legislação processual penal regulatória das

medidas de investigação tecnológica, que também contemple em seu texto normas pertinentes à proteção de dados.

A regulação a ser proposta pelo Conselho Nacional de Justiça não disciplinaria questões ligadas aos cidadãos comuns, mas sim aquelas inerentes à natureza típica do Poder Judiciário, em atenção ao art. 103-B, §4º e inciso I, da CRFB/88; no art. 8º do Regimento Interno do CNJ e no art. 14 do Regulamento Geral do CNJ; bem como no art. 196 do CPC. O CNJ tem competência para regular essa matéria porque os dados pessoais captados em investigações criminais, armazenados e geridos por sistemas policiais decorrem de decisões judiciais e influenciam diretamente o sistema de justiça, especialmente na produção de provas. Essa regulação assegura que as informações utilizadas respeitem a legalidade, os direitos fundamentais e os princípios da LGPD, promovendo segurança jurídica.

Trata-se de regulação com objetivo de concretizar o direito constitucional à proteção de dados, previsto no art. 5, LXXIX, da CRFB, sendo capaz de racionalizar o contraditório e a ampla defesa por meio do "enxugamento" do material digital existente nos autos.

Assim, propõe-se as seguintes diretrizes:

*(1) A Apagamento de dados pessoais*

a) Em relação aos processos já findos, os juízes com competência criminal devem determinar o apagamento de dados pessoais constantes de processos penais arquivados ou transitados há mais de cinco anos, inclusive os dados que não foram juntados nos autos e ainda se encontram nos arquivos digitais e bases de dados do Ministério Público e dos órgãos de polícia judicial.

b) O procedimento de exclusão de dados armazenados em poder dos órgãos de polícia judiciária deve ser documentado, certificado, e acompanhado por um servidor do Poder Judiciário, do Ministério Público, dos advogados com atuação no processo respectiva, mediante supervisão do juiz da causa.

c) Os dados pessoais captados e armazenados nas investigações criminais devem ser catalogados como prova e não-prova. Somente serão juntados aos autos os dados pessoais catalogados como prova. Os dados pessoais considerados como não-prova restarão segregados e armazenados na polícia judiciária, e somente seus respectivos titulares poderão acessá-los a fim de que, eventualmente, solicitem sua juntada nos autos como prova.

d) Em regra, os dados pessoais pertencentes a um determinado titular não classificados como prova não poderão ser acessados por outros réus, investigados ou terceiros, que não seus próprios titulares, salvo motivo concreto e relevante, mediante decisão judicial.

e) Apenas os elementos com valor probatório ou aqueles necessários para demonstrar a cadeia de custódia serão juntados ao processo. Demais informações não consideradas relevantes serão mantidas no arquivo policial, em base de dados segregada, até que ocorra o apagamento.

f) Os dados pessoais pertinentes à vida íntima das pessoas não serão entregues aos seus titulares, salvo se forem classificados como elemento de prova. O motivo da não inclusão da totalidade da gravação constará no recibo da não-entrega do material.

g) Os dados pessoais de terceiros, sem relação direta com o fato criminoso e não classificados como prova, devem ser mantidos no arquivo policial, em base de dados segregada. O acesso a esses dados segregados por investigados e réus somente poderá ocorrer mediante decisão judicial, após ponderação entre o interesse da defesa e a privacidade dos envolvidos, não sendo aceitável invocação genérica da cláusula de ampla defesa.

h) Os responsáveis pela investigação, ao analisarem o material apreendido, deverão juntar as provas pertinentes à autoria e materialidade, inclusive aquelas de interesse para a defesa, que possam, em tese, enfraquecer, contradizer, colocar em dúvida ou se opor às provas utilizadas para demonstrar a autoria e materialidade de um fato investigado.

i) A defesa poderá, no prazo da resposta à acusação, requerer o apagamento dos dados pessoais não utilizados como prova, salvo se houver ressalva, seja da autoridade policial, seja do Ministério Público, que tais dados estão sob análise e eventualmente serão utilizados em outras investigações ou ações penais. Se os dados não forem apagados nesta fase, no máximo serão apagados após o final do prazo prescricional da ação penal.

j) A defesa poderá, no prazo da resposta à acusação, requerer a inclusão nos autos de cópias dos arquivos que não tiverem sido incluídos nos autos pela autoridade policial ou pelo Ministério Público.

k) Decorrido o prazo de 5 anos a contar do trânsito em julgado, o Ministério Público e as pessoas que figuraram como réus na ação penal poderão requerer o apagamento dos dados pessoais utilizados como prova

l) Terceiros que não tenham sido indiciados, processados e não tenham tido conhecimento formal do procedimento penal serão notificados a respeito das comunicações que participaram e tenham sido captadas, salvo se tal providência demandar esforço desproporcional ou afetar investigações em andamento. O notificado poderá solicitar cópia das gravações que tenha participado, se tal medida não afrontar a intimidade de outras pessoas ou puder causar prejuízo ao processo, bem como requerer o apagamento dos dados tão logo sejam notificados.

*(2) Anonimização de dados pessoais*

m) Os dados pessoais dos réus e das testemunhas não devem constar das decisões judiciais publicadas nos sites dos tribunais ou acessíveis em consulta pública por quem não seja parte ou procurador. Deve-se aplicar anonimização progressiva e dinâmica para decisões judiciais, com base no nível de interesse público e histórico. Após determinado prazo, as decisões já publicadas podem ser reavaliadas a respeito do grau de visibilidade dos dados sensíveis.

n) A versão integral dos dados pessoais estará disponível tão somente nas versões das partes, seus procuradores, e membros do Ministério Público.

o) Deve-se estimular o uso de anonimização, criptografia de dados pessoais e sensíveis das partes, supressão ou inicialização dos dados pessoais.

p) Vedação de busca pelo nome das partes nos sites dos tribunais e repositórios de jurisprudência, e regulamentação de mecanismos de desindexação de decisões judiciais em plataformas públicas.

q) Encorajar a anonimização no momento da produção da sentença, incumbindo ao magistrado realizar inicialmente esse processo, em razão de ter melhores condições de avaliar quais os dados e informações que devem ser anonimizadas;

*(3) Implementação de modelo de gestão de dados pessoais no âmbito da polícia judicial*

r) Implementar políticas estritas de controle de acesso para limitar o risco de acesso não autorizado a dados pessoais arquivados nas bases de dados mantidas pela polícia judicial ou pelo Ministério Público, com suspensão imediata do acesso para investigadores e autoridades que não estejam mais trabalhando no caso.

s) Registro de ações de usuários: mediante registro das consultas feitas pelos investigadores, registro de todas as ações de usuários e sistemas, incluindo justificativa, data e hora, identificação de quem acessou dados digitais.

t) Exclusão de comunicações confidenciais cobertas por sigilo profissional, mediante decisão judicial.

u) Implementar princípio de limitação de propósito: manter uma trilha de auditoria explícita das ações dos usuários na plataforma, verificando se as ações estão dentro do escopo de um mandado ou ordem judicial. Diferentes perfis de acesso aos dados devem ser conferidos com base nas tarefas atribuídas e nas autorizações concedidas.

v) Manuseio cuidadoso dos dados: manter o material digital original fora do processamento da plataforma, utilizando uma cópia exata para análise. Para monitorar a integridade e minimizar erros, pode-se usar uma função de *hash* e um código de autenticação de mensagem.

w) Dados com alta sensibilidade como diálogos, fotos e vídeos íntimos somente poderão ser manipulados por agentes qualificados, com autorização específica e mecanismos de monitoramento constante.

x) Distinção entre categorias de sujeitos de dados: tratar os dados pessoais de condenados, suspeitos, vítimas, testemunhas e terceiros de maneira diferente, aplicando diferentes níveis de anonimização (irreversível ou desidentificado/reversível) conforme a categoria.

## VI

O sistema de justiça criminal, ainda que siga com o naufrágio sempre à espreita, deve seguir sendo um otimista realista, como disse Ariano Suassuna, pois o pessimismo é uma postura estéril, sem capacidade de transformação, e o otimismo ingênuo fecha os olhos para as dificuldades que fazem parte da vida. A discussão sobre o que fazer em relação ao armazenamento de dados pessoais envolverá diversos interesses, tanto do setor privado, quando do setor público. A impossibilidade de se buscar uma solução ideal não pode ser obstáculo para a solução possível.

Se a utopia é inalcançável, até mesmo semanticamente, ao menos devemos nos afastar da distopia. Na distopia, o sistema criminal se torna opressor e injusto em razão do colapso do controle sobre os dados pessoais, cuja abundância desnecessária se volta como uma arma de poucos sobre quase todos. Na distopia, a tecnologia se torna senhora do sistema judicial, e não o contrário. Assim, a tecnologia que deveria melhorar o acesso à justiça passa a ser usada para controlar, manipular e oprimir. Ao menos sabemos para onde não devemos ir.

Ao chegar no final da tese, inevitável a frase de T.S Eliot: "Nós nunca deixaremos de explorar, e o fim de toda nossa exploração será chegar ao ponto de partida e conhecer o lugar pela primeira vez"[43]. Esses versos sugerem que, ao longo da jornada, o verdadeiro entendimento está em retornar ao ponto de partida com uma perspectiva transformada.

O fim é de onde começamos.

[43] We shall not cease from exploration / And the end of all our exploring / Will be to arrive where we started / And know the place for the first time. ELIOT, T. S. *Little Gidding*. Disponível em: https://www.columbia.edu/itc/history/winter/w3206/edit/tseliotlittlegidding.html. Acesso em: 16 out. 2024.

# REFERÊNCIAS

ALEMANHA. Tribunal Constitucional Federal. *Decisão BVerfG 133, 277, 329 s*. Disponível em: https://www.bverfg.de. Acesso em: 30 out. 2024.

ALEMANHA**.** Tribunal Constitucional Federal. *Decisão n.º 1 BvR 209/83, de 15 de dezembro de 1983*. Disponível em: https://www.bverfg.de/e/rs19831215_1bvr020983.htm. Acesso em: 30 out. 2024

ALEMANHA. Tribunal Constitucional Federal. Decisão n.º 1 BvR 348/98, de 25 de novembro de 1999. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1999/11/rk19991125_1bvr034898.html. Acesso em: 20 ago. 2024.

ALEXANDER, Michelle. *The New Jim Crow:* Mass Incarceration in the Age of Colorblindness. Edição de décimo aniversário. Nova York: The New Press, 2020.

ALEXANDRE, Isabel. Audiências à distância em processo civil e princípio da publicidade das audiências. *Revista da Faculdade de Direito da Universidade de Lisboa*, Lisboa, v. 61 n. 1, p. 261-289, 2020. Disponível em: https://www.fd.ulisboa.pt/investigacao/producao-cientifica/revistas-cientificas/revista-da-fdul/numeros-issues/#1600783673032-2ead84bf-0998. Acesso em: 27 jan. 2024.

ALEXY, Robert. Direitos fundamentais e princípio da proporcionalidade. *O Direito*, [*s. l.*], ano 146, v. IV, p. 817-834, 2014.

ALEXY, Robert. *Teoria dos direitos fundamentais*. 2. ed. São Paulo: Malheiros, 2011.

ALIGHIERI, Dante. A Divina Comédia. Tradução de Italo Eugenio Mauro. 3. ed. São Paulo: Nova Fronteira, 2007.

ALMEIDA FILHO, José Carlos de Araujo. *Processo Eletrônico e Teoria Geral do Processo Eletrônico.* Rio de Janeiro:Forense, 2012.

ALMEIDA FILHO, José Carlos de Araújo. *Processo eletrônico e teoria geral do processo eletrônico*: a informatização judicial no Brasil. 3. ed. Rio de Janeiro: Forense, 2010.

ALVES, Daniel Bento. Uso de Malware em Investigação Criminal. Actualidad Jurídica Uría Menéndez, [*s. l.*], n. 47, 2017, p. 19-30. ISSN 1578-956X.

ANSEN, W.; AYERS, R. *Guidelines on cell phone forensics*. National Institute of Standards and Technology, Gaithersburg, MD, 2007. Disponível em: https://www.nist.gov/publications/guidelines-cell-phone-forensics. Acesso em: 6 ago. 2024.

ARABI, Abhner Youssif Mota. Utilização de dados pessoais no combate ao crime organizado: limites e possibilidades de técnicas especiais de investigação em meio digital. *Revista Judiciária do Brasil*, [*s. l.*], v. 2, n. 1, p. 69-107, jan./jul. 2022. Disponível em: https://doi.org/10.54795/rejub.n.1.180. Acesso em: 15 ago. 2024.

ARAS, Vladimir. A título de introdução: segurança pública e investigações criminais na era da proteção de dados. *In*: ARAS, Vladimir Barros; MENDONÇA, Andrey Borges de;

CAPANEMA, Walter Aranha; SILVA, Carlos Bruno Ferreira da; COSTA, Marcos Antônio da Silva (org.). *Proteção de dados pessoais e investigação criminal.* Brasília: Editora XYZ, 2020.

ARAS, Vladimir. *IA e rondas virtuais.* Blog do Vlad, 23 out. 2024. Disponível em: https://vladimiraras.blog/2024/10/23/ia-e-rondas-virtuais/. Acesso em: 29 out. 2024.

ARAS, Vladimir. Técnicas especiais de investigação. *In*: DE CARLI, Carla Verissimo (org.). *Lavagem de dinheiro:* prevenção e controle penal. 2. ed. Porto Alegre: Verbo Jurídico, 2013. p. 503-582.

ARAS, Vladimir. Testemunhas sem rosto e devido processo legal: o caso Snijders vs. Países Baixos (2024). *Blog do Vlad,* [*s. l.*], 6 fev. 2024. Disponível em: https://vladimiraras.blog/2024/02/06/testemunhas-sem-rosto-e-devido-processo-legal-o-caso-snijders-vs-paises-baixos-2024/#:~:text=2024%20Vladimir%20Aras-,Testemunhas%20sem%20rosto%20e%20devido%20processo%20legal%3A%20o%20caso%20Snijders,(anonimizadas)%20no%20processo%20penal. Acesso em: 18 out. 2024.

ARENDT, Hannah. *Entre o passado e o futuro*. São Paulo: Perspectiva, 2009.

ARENDT, Hannah. *A condição humana*. 11. ed. Rio de Janeiro: Forense Universitária, 2010.

ARRABAL PLATERO, Paloma. La incorporación al proceso de las evidencias obtenidas de equipos informáticos y de dispositivos de almacenamiento masivo de información. *Revista Aranzadi de derecho y nuevas tecnologías,* [*s. l.*], n. 56, 2021. Acesso em: 24 jan. 2024.

ARRABAL PLATERO, Paloma. Las diligencias de investigación tecnológicas en el proceso penal español. *Revista de Ciencias Sociales*, *[S. l.]*, v. 1, n. 76, 2020. Disponível em: https://revistas.uv.cl/index.php/rcs/article/view/2812. Acesso em: 6 nov. 2024.

ARRUDA, C. S. L. de. DIREITO À INFORMAÇÃO: requisito do devido processo legal em um Estado democrático de Direito. *Páginas a&b: arquivos e bibliotecas, [S. l.]*, p. 32–51, 2017. Disponível em: https://ojs.letras.up.pt/index.php/paginasaeb/article/view/1742. Acesso em: 3 nov. 2024.

ASSIS, Machado de. Verba Testamentária. *In*: ASSIS, Machado de. *Papéis Avulsos*. Rio de Janeiro: Gazeta de Notícias, 1882. Disponível em: https://machadodeassis.net/texto/verba-testamentaria/28831. Acesso em: 20 ago. 2024.

ASSO LÓPEZ, Lucía Carmina. Vigilar al vigilante: transparencia y rendición de cuentas sobre las tecnologías de vigilancia pública en México. *Revista Estudios en Derecho a la Información*, [*s. l.*], n. 15, p. 31-53, jan./jun. 2023. Disponível em: https://revistas.juridicas.unam.mx/index.php/derecho-informacion/issue/archive. Acesso em: 26 jan. 2024.

BADARÓ, Gustavo Henrique. *Processo penal*. 8. ed. Thomson Reuters Brasil: São Paulo, 2020.

BALAGUER CALLEJON, Francisco (coord.); CÁMARA VILLAR, Gregorio; LÓPEZ AGUILAR, Juan Fernando; BALAGUER CALLEJÓN, María Luisa; MONTILLA MARTOS, José Antonio. *Manual de Derecho Constitucional*. v. II. 17. ed. Madrid: Tecnos, 2022.

BALAGUER CALLEJÓN, Francisco. La constitución del algoritmo. El difícil encaje de la constitución analógica en el mundo digital. *In*: GOMES, Ana Cláudia Nascimento; ALBERGARIA, Bruno; CANOTILHO, Mariana Rodrigues (coord.). *Direito Constitucional*: diálogos em homenagem ao 80º aniversário de J. J. Gomes Canotilho. Belo Horizonte: Fórum, 2021.

BAPTISTA, Patrícia; KELLER, Clara Iglesias. Por que, quando e como regular as novas tecnologias: os desafios trazidos pelas inovações disruptivas. *Revista de Direito Administrativo*, Rio de Janeiro, n. 273, p. 123, mar. 2017. Disponível em: https://doi.org/10.12660/rda.v273.2016.66659. Acesso em: 27 out. 2024.

BARBOSA, Daniel Marchionatti; MOURA, Maria Tereza. Proteção de dados e processo penal. *In*: ARAS, Vladimir Barros; MENDONÇA, Andrey Borges de; CAPANEMA, Walter Aranha; SILVA, Carlos Bruno Ferreira da; COSTA, Marcos Antônio da Silva (org.). *Proteção de dados pessoais e investigação criminal.* Brasília: ANPR, 2020.

BARCELLOS, Ana Paula de. Devido processo legislativo, avaliação de custos e as opções hermenêuticas do STF. *Revista Quaestio Iuris*, Rio de Janeiro, v. 15, n. 3, p. 1380-1404, 2022.

BARRIO ANDRÉS, Moisés. La regulación del derecho a la protección de datos en los Estados Unidos: hacia un RGPD norteamericano. *Cuadernos de Derecho Transnacional*, [*s. l.*], v. 14, n. 2, p. 186-193, out. 2022. Disponível em: www.uc3m.es/cdt. Acesso em: 26 jan. 2024.

BECK, Ulrich. *Sociedade de Risco*: Rumo a uma Outra Modernidade. São Paulo: Editora 34, 2011.

BIONI, Bruno Ricardo. *Ensaio sobre o devido processo informacional*. [*S. l.: s. n.*], 2020. Disponível em: https://brunobioni.com.br/wp-content/uploads/2020/08/Ensaio-Devido-Processo-Informacional1.pdf. Acesso em: 26 jan. 2024.

BOBEK, Michal. Data protection, anonymity and courts. *Maastricht Journal of European and Comparative Law*, v. 26, n. 2, p. 183-189, 2019. Disponível em: https://doi.org/10.1177/1023263X19851628. Acesso em: 27 jan. 2024.

BOUSQUET, Antoine. Information, Privacy, and Just War Theory. *Ethics & International Affairs*, v. 34, ed. especial 3: The United Nations at Seventy-Five: Looking Back to Look Forward, outono 2020, p. 379-400. DOI: https://doi.org/10.1017/S0892679420000477. Acesso em: 18 ago. 2024.

BRASIL. Conselho Nacional de Justiça. Procedimento de Controle Administrativo n.º 0000547-84.2011.2.00.0000. Análise do Provimento n.º 89/2010 do Tribunal Regional Federal da 2.ª Região.

BRASIL. *Decreto-Lei n. 3.689, de 3 de outubro de 1941*. Código de Processo Penal. Rio de Janeiro: Presidência da República, 1941. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 26 jan. 2024.

BRASIL. *Decreto-Lei 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: Presidência da República, 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11491.htm. Acesso em: 5 nov. 2024.

BRASIL. *Lei n. 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 4 out. 2024.

BRASIL. *Lei n.º 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 n.º 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei n.º 9.034, de 3 de maio de 1995; e dá outras providências. Brasília, DF: Presidência da República, 2013. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm. Acesso em: 30 out. 2024.

BRASIL. *Lei n.º 9.296, de 24 de julho de 1996*. Regulamenta o inciso XII, parte final, do art. 5.º da Constituição Federal, dispondo sobre a interceptação de comunicações telefônicas e outras providências. Brasília, DF: Presidência da República, 1996. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 30 out. 2024.

BRASIL. *Lei nº 11.280, de16 de fevereiro de 2006*. Brasília, DF: Presidência da República, 2006. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11280.htm. Acesso em: 7 nov. 2024.

BRASIL. *Lei nº 11.419, de 19 de dezembro de 2006*. Dispõe sobre a informatização do processo judicial; altera a Lei nº 5.869, de 11 de janeiro de 1973 – Código de Processo Civil; e dá outras providências. Brasília, DF: Presidência da República, 2024. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11419.htm. Acesso em: 8 nov. 2024.

BRASIL. *Lei nº 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 6 nov. 2024.

BRASIL. *Lei nº 13.105, de 16 de março de 2015*. Código de Processo Civil. Brasília, DF: Presidência da República, 2015. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 10 nov. 2015.

BRASIL. *Lei nº 3.689, de 3 de outubro de 1941.* Código de Processo Penal. Rio de Janeiro: Presidência da República, 1941. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm. Acesso em: 10 nov. 2024.

BRASIL. *Lei nº 8.069, de 13 de julho de 1990*. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 30 out. 2024.

BRASIL. *Lei nº 9.807, de 13 de julho de 1999*. Estabelece normas para a organização e a manutenção de programas especiais de proteção a vítimas e a testemunhas ameaçadas, institui o Programa Federal de Assistência a Vítimas e a Testemunhas Ameaçadas e dispõe sobre a proteção de acusados ou condenados que tenham voluntariamente prestado efetiva colaboração à investigação policial e ao processo criminal. Brasília, DF: Presidência da República, 1999. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9807.htm. Acesso em: 9 nov. 2024.

BRASIL. Superior Tribunal de Justiça (3. Seção). *Recurso em Mandado de Segurança n.º 60.698 (2019/0119654-6*). Relator: Ministro Rogério Schietti Cruz, julgado em 26 ago. 2020. Disponível em: https://www.stj.jus.br. Acesso em: 7 nov. 2024.

BRASIL. Superior Tribunal de Justiça (5. Turma). *Recurso em Habeas Corpus n.º 145.329/PR*. Relator: Ministro Reynaldo Soares da Fonseca, 24 ago. 2021. Diário da Justiça Eletrônico, 30 ago. 2021.

BRASIL. Superior Tribunal de Justiça (6. Turma). *Recurso Especial AgRg n. 1.587.239.* Relatora: Min. Maria Thereza de Assis Moura, 14 ago. 2018. Disponível em: https://www.stj.jus.br. Acesso em: 10 nov. 2024.

BRASIL. Superior Tribunal de Justiça. *Agravo Regimental no Agravo em Recurso Especial n. 1676136/RS.* Relatora: Min. Laurita Vaz, 30 jun. 2020. Disponível em: https://www.stj.jus.br/sites/portalp/Inicio. Acesso em: 10 nov. 2024.

BRASIL. Superior Tribunal de Justiça. Recurso em Habeas Corpus n.º 51.531/RO. Relator: Ministro Nefi Cordeiro, 19 abr. 2016. *Diário da Justiça Eletrônico*, 9 maio 2016. Disponível em: https://www.stj.jus.br. Acesso em: 30 out. 2024.

BRASIL. Superior Tribunal de Justiça. Recurso em Habeas Corpus n.º 51.531/RO. Relator: Ministro Nefi Cordeiro, 19 abr. 2016. *Diário da Justiça Eletrônico*, 9 maio 2016. Disponível em: https://www.stj.jus.br. Acesso em: 30 out. 2024.

BRASIL. Superior Tribunal de Justiça. *RMS n. 60.698 (2019/0119654-6).* Relator: Min. Rogério Schietti Cruz, 26 ago. 2020. Disponível em: https://www.stj.jus.br. Acesso em: 10 nov. 2024.

BRASIL. Superior Tribunal de Justiça. *RMS n. 61.302 (2019/0199132-0) e RMS n. 62.143 (2019/0318252-3).* Relator: Min. Rogério Schietti, 26 ago. 2020. Disponível em: https://www.stj.jus.br. Acesso em: 10 nov. 2024.

BRASIL. Supremo Tribunal Federal (1. Turma). Habeas Corpus n.º 70.814. Relator: Ministro Celso de Mello, 1 mar. 1994. *Diário da Justiça*, p. 16649, ementa vol. 1750-02, 24 jun. 1994, p. 317. Disponível em: https://www.stf.jus.br. Acesso em: 30 out. 2024.

BRASIL. Supremo Tribunal Federal (2. Turma). *Habeas Corpus n.º 104.410/RS*. Relator: Ministro Gilmar Mendes, 6 mar. 2012. Disponível em: https://www.stf.jus.br. Acesso em: 30 out. 2024.

BRASIL. Supremo Tribunal Federal (2. Turma). *Inquérito n. 4419, Agravo Regimental*. Relator: Min. Edson Fachin, 13 jun. 2017. Acórdão eletrônico, DJe 139, divulgado em 23 jun. 2017, publicado em 26 jun. 2017. Disponível em: https://portal.stf.jus.br/. Acesso em: 10 nov. 2024.

BRASIL. Supremo Tribunal Federal (2. Turma). Recurso em Habeas Corpus n.º 132.115/PR. Disponível em: https://www.stf.jus.br. Acesso em: 30 out. 2024.

BRASIL. Supremo Tribunal Federal (2. Turma). Recurso em Habeas Corpus n.º 206.846/SP. Relator: Ministro Gilmar Mendes, 22 fev. 2022. *Diário da Justiça Eletrônico*, 25 maio 2022. Disponível em: https://www.stf.jus.br. Acesso em: 30 out. 2024.

BRASIL. Supremo Tribunal Federal (Tribunal Pleno). *Inquérito n.º 2424*. Relator: Ministro Cezar Peluso, 26 nov. 2008. Disponível em: https://www.stf.jus.br. Acesso em: 30 out. 2024.

BRASIL. Supremo Tribunal Federal. *Ação Direta de Inconstitucionalidade 1.511 MC. R*elator Ministro Carlos Velloso, 16 out. 1996, Plenário, DJ de 6 jun. 2003.

BRASIL. Supremo Tribunal Federal. *Ação Direta de Inconstitucionalidade n.º 6.387 MC-Ref/DF*. Julgamento em 6 e 7 de maio de 2020. Disponível em: https://www.stf.jus.br. Acesso em: 30 out. 2024.

BRASIL. Supremo Tribunal Federal. *Ação Direta de Inconstitucionalidade n.º 4.145/DF*. Redator para o acórdão: Ministro Alexandre de Moraes, 26 abr. 2018. *Diário da Justiça Eletrônico*, 31 jul. 2020. Disponível em: https://www.stf.jus.br. Acesso em: 30 out. 2024.

BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade n.º 4.109. Relatora: Ministra Cármen Lúcia, Redator para o acórdão: Ministro Edson Fachin, 14 fev. 2022. *Diário da Justiça Eletrônico*, DJe-075, 22 abr. 2022. Disponível em: https://www.stf.jus.br. Acesso em: 30 out. 2024.

BRASIL. Supremo Tribunal Federal. *ADPF 695.* Relator: Min. Luiz Fux, 15 set. 2022. Disponível em: https://www.stf.jus.br. Acesso em: 10 nov. 2024

BRASIL. Supremo Tribunal Federal. *Arguição de Descumprimento de Preceito Fundamental n.º 347*. Relator: Ministro Marco Aurélio, Relator p/ Acórdão: Ministro Luís Roberto Barroso, Tribunal Pleno, 4 out. 2023. Processo Eletrônico. Diário da Justiça Eletrônico, 19 dez. 2023.

BRASIL. Supremo Tribunal Federal. Arguição de Descumprimento de Preceito Fundamental n.º 444. Relator: Ministro Gilmar Mendes, 14 jun. 2018. *Diário da Justiça Eletrônico*, DJe-107, 22 maio 2019. Disponível em: https://www.stf.jus.br. Acesso em: 30 out. 2024.

BRASIL. Supremo Tribunal Federal. Habeas *Corpus n. 94.016-SP*. Relator Ministro Celso de Mello.

BRASIL. Supremo Tribunal Federal. *Habeas Corpus n.º 127.483/PR*. Relator: Ministro Dias Toffoli, Tribunal Pleno, 27 ago. 2015. *Diário da Justiça Eletrônico*, 4 fev. 2016. Disponível em: https://www.stf.jus.br. Acesso em: 30 out. 2024.

BRASIL**.** Supremo Tribunal Federal. *Informativo STF* n.º 393. Disponível em: https://www.stf.jus.br/arquivo/informativo/documento/informativo393.htm. Acesso em: 30 out. 2024.

BRASIL. Supremo Tribunal Federal. *Inquérito n. 3.983, Relator: Min. Teori Zavascki,* Tribunal Pleno, 3 mar. 2016. Disponível em: https://www.stf.jus.br. Acesso em: 10 nov. 2024.

BRASIL. Supremo Tribunal Federal. *Inquérito n. 4781 AgR-quinto*. Relator: Min. Alexandre de Moraes, 03 jul. 2023. Acórdão eletrônico, DJe-s/n, 11 set. 2023. Disponível em: https://www.stf.jus.br. Acesso em: 10 nov. 2024.

BRASIL. Supremo Tribunal Federal. Mandado de Segurança n.º 23.452/RJ. Relator: Ministro Celso de Mello. Julgamento em: 16 set. 1999. Tribunal Pleno. *Diário da Justiça*, Rio de Janeiro, v. 1990-01, p. 20, 12 maio 2000, ementa p. 86.

BRASIL. Supremo Tribunal Federal. Mandado de Segurança n.º 23.452/RJ. Relator: Ministro Celso de Mello, 16 set. 1999. *Diário da Justiça*, Rio de Janeiro, v. 1990-01, p. 20, 12 maio 2000, ementa p. 86. Disponível em: https://www.stf.jus.br. Acesso em: 30 out. 2024.

BRASIL. Tribunal de Justiça do Distrito Federal e Territórios (Câmara Criminal). *Acórdão n.º 1180679, Processo n.º 0706689-86.2019.8.07.0000*. Relator: Desembargador Waldir Leôncio Lopes Júnior, 24 jun. 2019. Publicado no DJE em 3 jul. 2019.

BRASIL. Tribunal de Justiça do Distrito Federal e Territórios. *Acórdão n.º 1362687, Processo n.º 0719947-95.2021.8.07.0000*. Relatora: Desembargadora Vera Andrighi, 4 ago. 2021. Diário da Justiça Eletrônico, 23 ago. 2021.

BRASIL. Tribunal de Justiça do Distrito Federal e Territórios. *Acórdão n.º 1707514, Processo n.º 0707187-78.2021.8.07.0012.* Relator: Desembargador Silvânio Barbosa dos Santos, 25 maio 2023. Publicado no PJe em 3 jun. 2023.

BRASIL. Tribunal Regional Federal da 3ª Região (5. Turma). *Habeas Corpus n.º 5010696-19.2022.4.03.0000*. Relator: Desembargador Federal Mauricio Kato, 29 nov. 2022. Disponível em: https://www.trf3.jus.br. Acesso em: 30 out. 2024.

BRASIL. Tribunal Regional Federal da 4ª Região (7. Turma). *Acórdão n.º 5011869-62.2020.4.04.7100*. Relatora: Desembargadora Federal Salise Monteiro Sanchotene, 1 fev. 2022. Disponível em: https://www.trf4.jus.br. Acesso em: 30 out. 2024.

BREMS, Eva; LAVRYSEN, Laurens. Procedural justice in human rights adjudication: the European Court of Human Rights. *Human Rights Quarterly*, [*s. l.*], v. 35, n. 1, p. 176-200, 2013.

BRIÈRE, Chloé. EU Criminal Procedural Law onto the Global Stage: The e-Evidence Proposals and Their Interaction with International Developments. *European Papers*, [*s. l.*], v. 6, n. 1, p. 493-512, 2021. DOI: 10.15166/2499-8249/479.

BUJOSA VADELL, Lorenzo M.; BUSTAMANTE RÚA, Mónica M.; TORO GARZÓN, Luis O. La prueba digital producto de la vigilancia secreta: obtención, admisibilidad y valoración en el proceso penal en España y Colombia. *Revista Brasileira de Direito Processual Penal*, [*s. l.*], v. 7, n. 2, p. 1347-1384, maio/ago. 2021. https://doi.org/10.22197/rbdpp.v7i2.482. Acesso em: 26 jan. 2024.

BUNDESVERFASSUNGSGERICHT. Information regarding data protection in court proceedings and in matters of judicial administration. 2018. Disponível em: https://www.bundesverfassungsgericht.de/EN/Verfahren/Datenschutz%20f%C3%BCr%20den%20justiziellen%20Bereich/Datenschutz%20f%C3%BCr%20den%20justiziellen%20Bereich_node.html. Acesso em: 08 nov. 2024.

BUSTAMANTE RÚA, M. M.; MARÍN TAPIERO, J. I. Justicia digital, acceso a internet y protección de datos personales. *Revista Internacional de Derecho*, [*s. l.*], v. 2, n. 1, p. 5-22, 2021. Disponível em: https://doi.org/ISSN-e 2788-7448. Acesso em: 26 jan. 2024.

CABRERA, Fernando José Bellini. *O princípio da publicidade no direito processual penal*. 2005. 197 f. Dissertação (Mestrado em Direito) – Pontifícia Universidade Católica de São Paulo, São Paulo, 2005. Disponível em: https://repositorio.pucsp.br/jspui/handle/handle/6308. Acesso em: 15 out. 2024.

CAMARA, Alexandre Freitas. Dimensão processual do princípio do devido processo constitucional. *Revista de Estudos e Debates*, [*s. l.*], v. 2, p. 55-68, 2017.

CARDINI, Fernando. Eugéne François Vidocq: De criminal a investigador criminal. *Criminal Investigation Newsletter*, Ano 4, n. 1, 2007.

CARREIRA, Alvin. *Teoria Geral do Processo*. 11. ed. Rio de Janeiro: Forense, 2006.

CARVALHO, Francisco Proença de; GARCÍA, Oscar Morales; FEIJOO, Manuel Álvarez. Regulamentação supranacional sobre criminalidade informática e técnicas de transposição. O direito penal português e espanhol como paradigmas. *Actualidad Jurídica Uría Menéndez*, [*s. l.*] , n. 48, p. 48-64, 2018.

CELESTE, Edoardo. Digital constitutionalism: a new systematic theorisation. *International Review of Law, Computers & Technology*, [*s. l.*], v. 33, n. 1, p. 1-23, jan. 2019. Disponível em: https://www.researchgate.net/publication/330135709. Acesso em: 01 set. 2024.

CERRILLO I MARTÍNEZ, Agustí. El difícil equilibrio entre transparencia pública y protección de datos personales. *Cuadernos de Derecho Local*, [*s. l.*], n. 45, p. 127-156, out. 2017.

CHARLEAUX, Lupa; LIMA, Lucas. Deep Web e Dark Web: o que é, qual a diferença e o que dá para encontrar na internet invisível. Tecnoblog, [Is. l.I], 15 out. 2024. Disponível em: https://tecnoblog.net/responde/deep-web-e-dark-web-qual-a- diferenca/. Acesso em: 22 out. 2024.

CHIOVENDA, Giuseppe. *Instituições de Direito Processual Civil.* São Paulo: Saraiva, 1965.

CHOY, James P. Kompromat: A theory of blackmail as a system of governance. *Journal of Development Economics*, v. 147, p. 102535, nov. 2020. Disponível em: https://doi.org/10.1016/j.jdeveco.2020.102535. Acesso em: 04 out. 2024.

CINTRA, Antonio Carlos de Araújo; GRINOVER, Ada Pellegrini; DINAMARCO, Cândido Rangel. *Teoria geral do processo.* 17. ed. São Paulo: Malheiros, 2001.

CITRON, Danielle Keats; PASQUALE, Frank A. The scored society: due process for automated predictions. *Washington Law Review*, v. 89, p. 1, 2014. [University of Maryland Legal Studies Research Paper No. 2014-8.] Disponível em: https://ssrn.com/abstract=2376209. Acesso em: 20 ago. 2024.

CONSELHO DA EUROPA. *Convenção Europeia dos Direitos Humanos*. Council of Europe: France. Disponível em: https://www.echr.coe.int/documents/d/echr/convention_por. Acesso em: 30 out. 2024.

CONSELHO DA UNIÃO EUROPEIA. Decisão-Quadro 2004/757/JAI, de 25 de outubro de 2004, que estabelece disposições mínimas sobre os elementos constitutivos dos atos criminosos e as penas no campo do tráfico ilícito de drogas. Jornal Oficial da União Europeia, nº L 335/8, 25 out. 2004. Disponível em: https://eur-lex.europa.eu. Acesso em: 20 dez. 2023.

CONSELHO NACIONAL DE JUSTIÇA. *Histórico*. Brasília: CNJ, 2019. Disponível em: https://www.cnj.jus.br/programas-e-acoes/processo-judicial-eletronico-pje/historico/. Acesso em: 5 nov. 2024.

CONSELHO NACIONAL DE JUSTIÇA. *Justiça em Números* - 2021 Brasília: CNJ, 2024. Disponível em: cnj.jus.br/wp-content/uploads/201/09/relatório-justica-em-numero2021-12.pdf. Acesso em: 27 out. 2024.

CONSELHO NACIONAL DE JUSTIÇA. *Justiça em Números* - 2022 Brasília: CNJ, 2024. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2022/09/justica-em-numeros-2022-1.pdf. Acesso em: 27 out. 2024.

CONSELHO NACIONAL DE JUSTIÇA. *Justiça em Números*. Brasília: CNJ, 2024. Disponível em: https://www.cnj.jus.br/pesquisas-judiciarias/justica-em-numeros/. Acesso em: 27 out. 2024.

CONSELHO NACIONAL DE JUSTIÇA. *Resolução nº 121, de 5 de outubro de 2010*. Dispõe sobre a divulgação de dados processuais eletrônicos na rede mundial de computadores, expedição de certidões judiciais e dá outras providências. Brasília, DF: CNJ, 2010. Disponível em: https://atos.cnj.jus.br/atos/detalhar/92. Acesso em: 8 nov. 2024.

CONSELHO NACIONAL DE JUSTIÇA. *Serviços notariais não podem criar banco de dados pessoais em paralelo*. Brasília, DF: CNJ, 2024. Disponível em: https://www.cnj.jus.br/servicos-notariais-nao-podem-criar-banco-de-dados-pessoais-paralelo/. Acesso em 17 out. 2024.

CONTINI, Francesco; CORDELLA, Antonio. Law and technology in civil judicial procedures. *The Oxford Handbook of Law, Regulation and Technology*, [*s. l.*], Oct 2016. p. 246-268. DOI: 10.1093/oxfordhb/9780199680832.013.47. Acesso em: 13 fev. 2024.

CONTRERAS, Pablo. El derecho a la protección de datos personales y el reconocimiento de la autodeterminación informativa en la Constitución chilena. *Estudios Constitucionales*, [*s. l.*], v. 18, n. 2, p. 87-120, 2020.

CONVENÇÃO para a Proteção dos Indivíduos com Relação ao Tratamento Automatizado de Dados Pessoais (Convenção 108). Estrasburgo: Conselho da Europa, 1981. Disponível em: https://rm.coe.int/cm-convention-108-portuguese-version-2756-1476-7367-1/1680aa72a2. Acesso em: 4 out. 2024.

CORNELL LAW SCHOOL. Vagueness Doctrine. *Legal Information Institute*. Disponível em: https://www.law.cornell.edu/wex/vagueness_doctrine. Acesso em: 25 out. 2024.

CORTE INTERAMERICANA DE DIREITOS HUMANOS. *Caso Miembros De La Corporación Colectivo De Abogados "José Alvear Restrepo" Vs. Colombia.* Caso Corte IDH, Série C n.º 506. Sentencia de 18 de octubre de 2023. Disponível em: https://www.corteidh.or.cr/docs/casos/articulos/seriec_506_esp.pdf. Acesso em: 30 out. 2024.

COTEÑO MUÑOZ, Alejandro. Transparencia judicial. *Eunomía. Revista en Cultura de la Legalidad*, [*s. l.*], n. 16, p. 198-218, abr./set. 2019. Disponível em: https://doi.org/10.20318/eunomia.2019.4700. Acesso em: 26 jan. 2024.

CRAWFORD, Kate; SCHULTZ, Jason. Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms. *Boston College Law Review*, [*s. l.*],v. 55, n. 1, p. 93-128, 2014.

CUEVA, Ricardo Villas Bôas. A incidência da Lei Geral de Proteção de Dados Pessoais nas atividades do Poder Judiciário. *In*: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA; Ricardo Villas Bôas (coord.). *Lei Geral de Proteção de Dados (lei 13.709/18)*: a caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Thomson Reuters Brasil. 2020.

CZERNIAK, Dominika. Collection of Location Data in Criminal Proceedings – European (the EU and Strasbourg) Standards. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, v. 7, n. 1, p. 123-160, jan.-abr. 2021. Disponível em: https://doi.org/10.22197/rbdpp.v7i1.503. Acesso em: 29 jul. 2024.

DAMASCENO, Israel Felipe Martins. *Análise histórica do princípio da publicidade processual: sua aplicação da origem ao processo contemporâneo brasileiro*. 2020. 182 p. Dissertação (Mestrado em Ciências Histórico-Jurídicas) – Faculdade de Direito, Universidade de Lisboa, Lisboa, 2020.

DARWIN, Charles. *A origem das espécies*. 3. ed. São Paulo: Madras, 2005.

DE GREGORIO, G. *Digital Constitutionalism in Europe*: Reframing Rights and Powers in the Algorithmic Society (Cambridge Studies in European Law and Policy). Cambridge: Cambridge University Press. Disponível em: http://10.1017/9781009071215. Acesso em: 10 nov. 2024.

DEPARTAMENTO DE JUSTIÇA DOS EUA. Gabinete de Assuntos Internacionais, Divisão Criminal. *Uma breve explicação da causa provável para as autoridades estrangeiras*. Abril de 2022. Disponível em: https://www.justice.gov/criminal/criminal-oia/file/1501821/dl. Acesso em: 5 nov. 2024.

DHALIWAL, Jasdev. 26 billion records released: The mother of all breaches. *McAfee Blogs*, 27 fev. 2020. Disponível em: https://www.mcafee.com/blogs/internet-security/26-billion-records-released-the-mother-of-all-breaches/. Acesso em: 4 out. 2024.

DINAMARCO, Cândido Rangel. *Instituições de Direito Processual Civil.* 4. ed. São Paulo: Malheiros, 2019.

DINAMARCO, Cândido Rangel. *Nova Era do Processo Civil.* São Paulo: Malheiros, 2003.

DIXIT, Saumya Ranjan. *The Right to Privacy Under the Armour of Digitalisation*: Muddling Throught Trouble Waters. [*S. n, s. l.*], 14 jul. 2023. Disponível em: www.calj.in/post/the-right-to-privacy-under-the-armour-of-digitalisation-muddling-through-troubled-waters. Acesso em: 09 fev. 2024.

DOCTRINES of Closed Material Procedure. Justice, London, 2013. Disponível em: https://justice.org.uk/review-of-closed-material-procedure-in-the-justice-and-security-act-2013/. Acesso em: 1 nov. 2024.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. 2. ed. São Paulo: Thomson Reuters Brasil, 2021. *E-book.*

DURANTI, Luciana; STANFIELD, Allison. Authenticating electronic evidence. *In*: MASON, Stephen; SENG, Daniel (ed.). *Electronic Evidence and Electronic Signatures*. London: University of London Press, 2021. p. 237-278. Disponível em: https://www.jstor.org/stable/j.ctv1vbd28p.1. Acesso em: 13 ago. 2024.

EBLING, Cláudia Marlise da Silva Alberton. *Teoria geral do processo*: uma crítica à teoria unitária do processo através da abordagem da questão da sumarização e do tempo no/do processo penal. Porto Alegre: Livraria do Advogado, 2004.

ELIOT, T. S. *Little Gidding*. Disponível em: https://www.columbia.edu/itc/history/winter/w3206/edit/tseliotlittlegidding.html. Acesso em: 16 out. 2024.

ELTIS, Karen. The Judicial System in the Digital Age: Revisiting the Relationship Between Privacy and Accessibility in the cyber Context. *McGill Law Journal,* [*s. l.*], v. 56, n. 2, p. 289–316, Feb.2011. Disponível em: https://doi.org/10.7202/1002368ar. Acesso em: 10 nov. 2024.

EMERSON, Ralph Waldo. *Self-Reliance*. [*S. l.*]: Project Gutemberg, 1841. Disponível em: https://www.gutenberg.org/ebooks/16643. Acesso em: 17 out. 2024.

ESPAÑA. Agência Espanhola de Proteção de Dados. AEPD Resolución: R/01239/2007. Disponível em: https://www.aepd.es. Acesso em: 10 nov. 2024.

ESPAÑA. Audiencia Nacional, *San 14/2020*, de 10 de fevereiro de 2020 (ROJ: SAN 14/2020).

ESPAÑA. Ley de Enjuiciamiento Criminal, de 14 de septiembre de 1882. *Boletín Oficial del Estado*, 14 set. 1882. Disponível em: https://www.boe.es. Acesso em: 30 out. 2024.

ESPAÑA. Ley Orgánica n.º 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. *Boletín Oficial del Estado*, núm. 238, 6 oct. 2015. Disponível em: https://www.boe.es. Acesso em: 30 out. 2024.

ESPAÑA. *Real Decreto 1065, de 27 de noviembre de 2015*. Sobre comunicaciones electrónicas en la Administración de Justicia en el ámbito territorial del Ministerio de Justicia y por el que se regula el sistema LexNET. *Boletín Oficial del Estado*, n. 287, 01 dez. 2015. Disponível em: https://www.boe.es/eli/es/rd/2015/11/27/1065/con. Acesso em: 08 nov. 2024.

ESPAÑA. *Real Decreto 84, de 26 de enero de 2007*. Sobre implantación en la Administración de Justicia del sistema informático de telecomunicaciones Lexnet para la presentación de escritos y documentos, el traslado de copias y la realización de actos de comunicación procesal por medios telemáticos. *Boletín Oficial del Estado*, n. 38, p. 6239-6244, 13 feb. 2007. Disponível em: https://www.boe.es/eli/es/rd/2007/01/26/84. Acesso em: 8 nov. 2024.

ESPAÑA. Tribunal Constitucional. Acuerdo de 18 de febrero de 2021, del Pleno del Tribunal Constitucional, sobre tratamiento de datos de carácter personal. *Boletín Oficial del Estado*, n. 48, Sección III, p. 23047, 2940, 18 feb. 2021.

ESPAÑA. Tribunal Constitucional. *Constituição Española*. Disponível em: https://www.tribunalconstitucional.es/es/tribunal/normativa/Normativa/CEportugu%C3%A9s.pdf. Acesso em: 10 nov. 2024.

ESPAÑA. Tribunal Supremo. Sentencia n.º 342/2013, de 17 abr. 2013 — F.J. 8.º — e Sentencia n.º 462/2019, de 14 out. 2019 — F.J. 1.º. Disponível em: https://www.poderjudicial.es. Acesso em: 30 out. 2024.

ESPAÑA. Tribunal Supremo. Sentencia n.º 7179/2008. ECLI: ES:TS:2008:7179. Disponível em: https://www.poderjudicial.es. Acesso em: 30 out. 2024.

ESPANHA. *Real Decreto de 14 de setembro de 1882*. Aprova a Lei de Enjuiciamento Criminal. *Boletim Oficial do Estado*, n.º BOE-A-1882-6036. Disponível em: https://www.boe.es/eli/es/rd/1882/09/14/(1)/con. Acesso em: 22 out. 2024.

ESPANHA. Tribunal Supremo da Espanha. *Sentencia N.º 293/2011*. Sala de lo Penal.

ESTADOS UNIDOS. *Constituição dos Estados Unidos da América*. Washington: Library of Congress. Disponível em: https://constitution.congress.gov/constitution/amendment-1/. Acesso em: 24 ago. 2024. *Primeira Emenda.*

EUA e Alemanha espionaram 120 países por décadas. *DW*, [*s. l.*], 12 fev. 2020. Disponível em: https://www.dw.com/pt-br/eua-e-alemanha-espionaram-120-pa%C3%ADses-por-d%C3%A9cadas/a-52352884. Acesso em: 29 out. 2024.

EUROPA. European Court of Human Rights. *Klass and others v. Germany. Application no. 5029/71.* Judgment, 6 set. 1978. Disponível em: https://hudoc.echr.coe.int/eng?i=001-57510. Acesso em: 26 out. 2024.

EUROPEAN COURT OF HUMAN RIGHTS. Affaire Dumitru Popescu c. Roumanie (No 2), requête no 71525/01. Arrêt, Strasbourg, 26 avril 2007. Disponível em: https://hudoc.echr.coe.int/eng?i=001-80353. Acesso em: 29 out. 2024.

EUROPEAN COURT OF HUMAN RIGHTS. *Case Of Centrum För Rättvisa V. Sweden* (Application no. 35252/08). Strasbourg, 25 May 2021. Available at: https://hudoc.echr.coe.int. Accessed on: 7 nov. 2024.

EUROPEAN COURT OF HUMAN RIGHTS. Case of Kostovski v. The Netherlands. Application no. 11454/85, Strasbourg, 20 nov. 1989. Disponível em: https://hudoc.echr.coe.int/eng?i=001-57615. Acesso em: 18 out. 2024.

EUROPEAN COURT OF HUMAN RIGHTS. Case of P.G. and J.H. v. the United Kingdom (Application no. 44787/98). Judgment, Strasbourg, 25 set. 2001. Disponível em: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-59665%22]}. Acesso em: 29 out. 2024.

EUROPEAN COURT OF HUMAN RIGHTS. Case of Snijders v. The Netherlands. Application no. 56440/15, Third Section, Strasbourg, 6 fev. 2024. Disponível em: https://hudoc.echr.coe.int/eng?i=001-230706. Acesso em: 18 out. 2024.

EUROPEAN COURT OF HUMAN RIGHTS. *Case of Uzun v. Germany (Application no. 35623/05)*. 2 Sep. 2010. Disponível em: https://hudoc.echr.coe.int/eng?i=001-100293. Acesso em: 10 ago. 2024.

EUROPEAN COURT OF HUMAN RIGHTS. *Guide to the Case-Law of the European Court of Human Rights - Data Protection*. Corte Europeia de Direitos Humanos, 31 de agosto de 2022. Disponível em: https://rm.coe.int/guide-data-protection-eng-1-2789-7576-0899-v-1/1680a20af0. Acesso em: 6 nov. 2024.

EUROPEAN COURT OF HUMAN RIGHTS. Judgment of 2 September 2010, Uzun v Germany, case no. 35623/05. https://hudoc.echr.coe.int/. Acesso em: 16 ago. 2024.

EUROPEAN COURT OF HUMAN RIGHTS. Judgment of 4 December 2015, *Roman Zakharov v. Russia*, case no. 47143/06, § 231. Disponível em: https://hudoc.echr.coe.int/. Acesso em: 7 nov. 2024.

EUROPOL. *Do criminals dream of electric sheep?* How technology shapes the future of crime and law enforcement. Europol, 11 June 2024. Disponível em: https://www.europol.europa.eu/publications-documents/do-criminals-dream-of-electric-sheep-how-technology-shapes-future-of-crime-and-law-enforcement. Acesso em: 25 jan. 2024.

EXCLUSIVO: as mensagens secretas da Lava Jato. *The Intercept Brasil,* 9 jun. 2019. Disponível em: https://theintercept.com/series/mensagens-lava-jato/. Acesso em: 4 out. 2024.

FABBRINI, F.; CELESTE, E. The Right to Be Forgotten in the Digital Age: The Challenges of Data Protection Beyond Borders. *German Law Journal*, [*s. l.*], v. 21, p. 55–65, 2020. Disponível em: https://doi.org/10.1017/glj.2020.14. Acesso em: 20 ago. 2024.

FALEIRO E SILVA, L. M.; MUCELLI REZENDE VELOSO, N. E. O princípio da publicidade e os desafios aos direitos do réu no processo civil na contextura do contraterrorismo: um paralelo entre a situação brasileira e a do Reino Unido. *Cadernos de Dereito Actual*, n. 22, p. 217–231, 2023. Disponível em: https://www.cadernosdedereitoactual.es/ojs/index.php/cadernos/article/view/1026. Acesso em: 12 fev. 2024.

FERNANDES, Antonio Scarance. *Processo Penal Constitucional*. 2. ed. São Paulo: Revista dos Tribunais, 2000.

FERNÁNDEZ GONZÁLEZ, Miguel Ángel. El acceso a información pública en la jurisprudencia del Tribunal Constitucional y su incidencia en la justicia ordinaria. *Derecho Público Iberoamericano*, n. 19, p. 55-94, out. 2021.

FERNÁNDEZ, Ana Isabel González. Inteligencia artificial al servicio del proceso penal y la protección de los datos personales. *Anuario de la Facultad de Derecho*, Universidad de Extremadura, v. 38, p. 503-516, 2022.

FIGUEIREDO, Lúcia Valle. Estado de direito e devido processo legal. *Revista de Direito Administrativo*, Rio de Janeiro, n. 209, p. 7-18, jul./set. 1997.

FOUCAULT, Michel. *Vigiar e Punir:* Nascimento da prisão. Tradução de Raquel Ramalhete. 36. ed. Petrópolis: Vozes, 2008.

FRANCE. *Code de procédure pénale*. Última atualização: 1º nov. 2024. Disponível em: https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006071154/. Acesso em: 7 nov. 2024.

FRANCE. Cour de Cassation, Chambre Civile 1. *Caso Fernande Segret*. Paris, Publié au bulletin, p. 14482, 4 de outubro de 1965. Disponível em: https://www.courdecassation.fr. Acesso em: 30 out. 2024.

GALÁN MUÑOZ, Alfonso. La protección de datos de carácter personal en los tratamientos destinados a la prevención, investigación y represión de delitos: hacia una nueva orientación de la política criminal de la Unión Europea. *In*: COLOMER HERNÁNDEZ, Ignacio (Dir.). *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea*. Cizur Menor: Aranzadi, 2015.

GANDHI, Amisha. California County Oversight of Use Policies For Surveillance Technology. *California Law Review*, [*s. l.*], v. 108, n. 3, p. 1011-1045, 2020. Disponível em: https://www.jstor.org/stable/10.2307/26977929. Acesso em: 13 ago. 2024.

GERMANY. Bundesgesetzblatt. *Komplette Ausgabe, n. 7, 1977*. Disponível em: https://www.bgbl.de/xaver/bgbl/start.xav?start=//*%5B@attr_id=%27bgbl177i0201.pdf%27%5D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl177007.pdf%27%5D__1711023794148. Acesso em: 30 out. 2024.

GERMANY. Bundesverfassungsgericht (BVerfG). Decisão em BVerfGE 120, 274. Disponível em: https://www.bundesverfassungsgericht.de. Acesso em: 30 out. 2024.

GERMANY. Bundesverfassungsgericht (Federal Constitutional Court). BVerfGE 27.

GERMANY. Bundesverfassungsgericht (Federal Constitutional Court). *Order of the First Senate of 15 December* 1983 - 1 BvR 209/83, paras. 1-214. Disponível em: https://www.bverfg.de/e/rs19831215_1bvr020983en.html. Acesso em: 10 nov. 2024.

GERMANY. Strafprozessordnung. Disponível em: https://www.gesetze-im-internet.de/stpo/. Acesso em: 10 nov. 2024.

GERMANY. *Zivilprozessordnung* (Código de Processo Civil). Disponível em: https://www.gesetze-im-internet.de/zpo/. Acesso em: 8 nov. 2024.

GIACOMOLLI, Felipe. *Gerenciamento tecnológico do sistema de justiça penal*: as novas tecnologias no âmbito do policiamento, da investigação e da decisão. Rio de Janeiro: Marcial Pons, 2023.

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.

GÓMEZ RODRÍGUEZ, Álvaro. *Aspectos procesales de los delitos informáticos y tecnológicos*. 2021. 403 f. Tese (Doutorado em Ciências Sociais e Jurídicas) – Universidad Rey Juan Carlos, Escuela Internacional de Doctorado, Madrid, 2021.

GONZÁLEZ CANO, M.ª Isabel. Cesión y tratamiento de datos personales en el proceso penal. Avances y retos inmediatos de la Directiva (UE) 2016/680. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, v. 5, n. 3, p. 1331-1384, set./dez. 2019. Disponível em: https://doi.org/10.22197/rbdpp.v5i3.279. Acesso em: 1 nov. 2024.

GONZÁLEZ PULIDO, Irene. *Diligencias de Investigación Tecnológicas para la Lucha contra la Ciberdelincuencia Grave*: Especial Referencia a la Utilización del Registro Remoto para la Investigación de Ciberataques contra Infraestructuras Críticas y Estratégicas. 2022. Tese (Doutorado em Direito) — Universidade de Salamanca, Salamanca, Espanha, 2022.

GONZÁLEZ REYES, José Miguel. La prueba pericial digital y la cadena de custodia. *Anales de la Facultad de Derecho*, [*s. l.*], v. 38, p. 43-79, sept. 2021. Disponível em: https://doi.org/10.25145/j.anfade.2021.38.03. Acesso em: 26 jan. 2024.

GORDON, Diana R., 1987. The Electronic Panopticon: A Case Study of the Development of the National Criminal Records System. *Politics & Society*, [*s. l.*], v. 15, n. 4, p. 483-511, Dec. 1987. Disponível em: https://doi.org/10.1177/003232928701500404. Acesso em: 26 jan. 2024.

GRASSBERGER, Roland. Pioneers in Criminology XIII: Hans Gross (1847-1915). *Journal of Criminal Law and Criminology,* v. 47, n. 4, p. 397-422, 1957.

GRECO, Luís; GLEIZER, Orlandino. A infiltração online no processo penal – Notícia sobre a experiência alemã. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, v. 5, n. 3, p. 1483-1518, set./dez. 2019. Disponível em: https://doi.org/10.22197/rbdpp.v5i3.278. Acesso em: 20 ago. 2024.

GRINOVER, Ada Pellegrini; FERNANDES, Antonio Scarance; GOMES FILHO, Antonio Magalhães. *As nulidades no processo penal*. 9. ed. São Paulo: Revista dos Tribunais, 2006.

GUERRERO GUERRERO, Beatriz. Protección de datos personales en el Poder Judicial: Una nueva mirada al principio de publicidad de las actuaciones judiciales. *Rev. chil. derecho tecnol.,* [*s. l.*]. 2020, v. 9, n. 2, p. 33-56. Disponível em: http://dx.doi.org/10.5354/0719-2584.2020.54372. Acesso em: 8 nov. 2024.

GUO, Meirong. Internet court's challenges and future in China. *Computer Law & Security Review*, [*s. l.*], v. 40, p. 1-13, 2021. Disponível em: https://doi.org/10.1016/j.clsr.2020.105522. Acesso em: 26jan. 2024.

GUTIÉRREZ ZARZA, Ángeles. La protección de las personas físicas en lo que respecta a su derecho a la intimidad y los datos personales por las autoridades de emissão y ejecución de las órdenes europeas de investigación. *In*: ARANGÜENA FANEGO, Coral; DE HOYOS SANCHO, Montserrat (Dir.). *Garantías procesales de investigados y acusados*: Situación actual en el ámbito de la Unión Europea. Valencia: Tirant lo Blanch, 2017.

HALAHAN, Oleksandr; KRYTSKA, Iryna; TUMANYANTS, Anush; DUBIVKA, Iryna. Digitalization of the criminal process: is simplification always for the better? *Journal promoted by the Department of Law and Political Science*, [*s. l.*], n. 38, p. 1-12, 2022. Disponível em: http://dx.doi.org/10.7238/idp.v0i38.408495. Acesso em 26 jan. 2024.

HAMMOUDI, Sabrina. Law and "Smart Videoprotection": the French Case. *European Review of Digital Administration & Law - Erdal*, [*s. l.*], v. 2, n. 2, p. 205-210, 2021. Disponível em: https://doi.org/10.5281/zenodo.5094234. Acesso em: 4 out. 2024.

HARDING, Luke. What are the Panama Papers? A guide to history's biggest data leak. *The Guardian*, 5 abr. 2016. Disponível em: https://www.theguardian.com/news/2016/apr/03/what-you-need-to-know-about-the-panama-papers. Acesso em: 4 out. 2024.

HECK, J. N. O princípio kantiano da publicidade na moral e no direito. *Síntese: Revista De Filosofia*, [ *s. l.*], v. 36, n. 115, p. 285–300, 2009. Disponível em: https://doi.org/10.20911/21769389v36n115p285-300/2009. Acesso em: 8 nov. 2024.

HENRIQUES, Tarcísio. Dados pessoais, consentimento e privacidade: considerações sobre a Lei Geral de Proteção de Dados. *In*: ARAS, Vladimir Barros; MENDONÇA, Andrey Borges de; CAPANEMA, Walter Aranha; SILVA, Carlos Bruno Ferreira da; COSTA, Marcos Antônio da Silva (org.). *Proteção de dados pessoais e investigação criminal*. Brasília: ANPR, 2020. Disponível em: https://www.anpr.org.br/images/2020/Livros/protecao_dados_pessoais_versao_eletronica.pdf. Acesso em: 3 nov. 2024.

HIJMANS, Hielke; RAAB, Charles. Ethical dimensions of the GDPR, AI regulation, and beyond. *Revista de Direito Público (RDP)*, Brasília, v. 18, n. 100, p. 56-80, out./dez. 2021.

HILGENDORF, Eric. *Digitalização e direito*. Organização e tradução de Orlandino Gleizer. São Paulo: Marcial Pons, 2020.

HOFFMANN-RIEM, Wolfgang. *Teoria geral do direito digital*: transformação digital: desafios para o direito. 2 ed. Rio de Janeiro: Forense, 2022.

IMENTA, Marcus Vinícius. Processo constitucional: consonâncias e dissonâncias entre as proposições de Couture, Fix-Zamudio, Baracho, Andolina e Vignera. *Revista da Faculdade Mineira de Direito*, Belo Horizonte, v. 23, n. 45, p. 256-274, 2020.

INFORMATION COMMISSIONER'S OFFICE. What is personal information: a guide. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/. Acesso em: 12 ago. 2024.

JACOBS, James; CREPET, Tamara. The expanding scope, use, and availability of criminal records. *New York University Journal of Legislation and Public Policy*, [*s. l.*], v. 11, n. 2, p. 177-214, 2008.

JIMÉNEZ-CASTELLANOS BALLESTEROS, Inmaculada. *El derecho al olvido digital del pasado penal*. 2018. 388 f. Tese (Doutorado em Direito) — Universidade de Sevilla, Sevilla, 2018.

JONG, L.; M'CHAREK, A. The high-profile case as "fire object": Following the Marianne Vaatstra murder case through the media. *Crime, Media, Culture*, [*s. l.*], v. 14, n. 3, p. 347-363, dez. 2018. Disponível em: https://doi.org/10.1177/1741659017718036. Acesso em: 20 ago. 2024.

JOVE VILLARES, Daniel. La importancia de los contextos. Datos personales y tratamiento. *Nuevos Horizontes del Derecho Constitucional*, n. 4, p. 5-23, 2023.

KAFKA, Franz. *O processo*. Tradução de Modesto Carone. São Paulo: Companhia das Letras, 2005.

KALKMANN, Tiago. O Encontro fortuito de provas no processo penal brasileiro e as correspondentes restrições na legislação alemã. *Revista de Doutrina Jurídica,* Brasília, DF, v. 110, n. 1, p. 46–64, 2019. Disponível em: https://revistajuridica.tjdft.jus.br/index.php/rdj/article/view/291. Acesso em: 20 out. 2024.

KANT, Immanuel. *Metafísica dos costumes.* Tradução: Edson Bini. Petrópolis: Vozes, 2013.

KENNEDY, Russ. The New Era Of Big Data. *Forbes*, 24 maio 2023. Disponível em: https://www.forbes.com/councils/forbestechcouncil/2023/05/24/the-new-era-of-big-data/. Acesso em: 4 out. 2024.

KLEINBERG, Jon; LUDWIG, Jens; MULLAINATHAN, Sendhil; SUNSTEIN, Cass R. Discrimination in the Age of Algorithms. *Journal of Legal Analysis*, Oxford, v. 10, p. 113-174, 2019. Disponível em: https://doi.org/10.1093/jla/laz001. Acesso em: 27 jan. 2024.

KLOZA, Dariusz. *Privacy Impact Assessments as a Means to Achieve the Objectives of Procedural Justice*. Jusletter IT. Die Zeitschrift für IT und Recht, 20 fev. 2014. Disponível em: https://jusletter-it.weblaw.ch/en/issues/2014/IRIS/2524.html. Acesso em: 5 nov. 2024.

KURLYCHEK, M. C.; BRAME, R.; BUSHWAY, S. D. Enduring risk? Old criminal records and predictions of future criminal involvement. *Crime & Delinquency*, [*s, l.*], v. 53, n. 1, p. 64-83, 2007. Disponível em: https://doi.org/10.1177/0011128706294439. Acesso em: 26 jan. 2024.

L'ORGANISATION INTERNATIONALE DE LA FRANCOPHONIE. Disponível em: http://www.ahjucaf.org/spip.php?article6131. Acesso em: 25 jan. 2024.

LAI, Sauvei. *Policeware*: Infecção de Software em sistema Informático do Investigado para Fins de Vigilância Eletrônica. São Paulo: JusPodivm, 2024.

LARO GONZÁLEZ, María Elena. Nuevos horizontes para el derecho de protección de datos personales, al amparo del nuevo reglamento general de protección de datos y de la directiva relativa al tratamiento de datos personales en el ámbito penal. *Anuario de la Facultad de Derecho*, Universidad de Extremadura, n. 38, p. 503-516, 2022. Disponível em: https://www.unex.es/contenido/artigo/Laro_nuevos_horizontes_para_el_derecho.pdf. Acesso em: 4 out. 2024.

LARO GONZÁLEZ, María Elena. Principio de proporcionalidad y tratamiento de datos personales en el proceso penal. *In*: MARTÍN OSTOS, José. *La administración de justicia en España y en América: Liber amicorum*. Sevilla: Astigi, 2021. p. 1075-1088. Disponível em: https://hdl.handle.net/11441/132338. Acesso em: 25 jan. 2024.

LARRAURI, Elena; JACOBS, James B. ¿Son las sentencias públicas? ¿Son los antecedentes penales privados? Una comparación de la cultura jurídica de Estados Unidos y España. *InDret*, 2010, p. 16-53. Disponível em: http://www.raco.cat/index.php/InDret/article/view/22668. Acesso em: 26 jan. 2024.

LARRAURI, Elena; ROVIRA, Martí. Publicidad, solicitud y cancelación de los antecedentes penales en los tribunales españoles. *Revista Electrónica de Ciencia Penal y Criminología*, [*s. l.*], n. 23-01, pp. 1- 32, 2021. Disponível em: http://criminet.ugr.es/recpc/23/recpc23-01.pdf. Acesso em: 26 jan. 2024.

LEÓN EXPÓSITO, Ana María**.** Transparencia y protección de datos. *Cosmológica*, Santa Cruz de La Palma, n. 2, 2022.

LIMA, Francisco Jozivan Guedes de. *Justiça e publicidade em Immanuel Kant: uma reconstrução socionormativa.* 2016. 121 p. Tese (Doutorado em Filosofia) – Programa de Pós-Graduação em Filosofia, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2016.

LIMA, Renato Brasileiro de. *Manual de processo penal.* 8. ed. Salvador: JusPodivm, 2020.

LINS DA SILVA, Carlos Eduardo. Novo caso amoroso ameaça Clinton. *Folha de S. Paulo*, São Paulo, 22 jan. 1998. Disponível em: https://www1.folha.uol.com.br/fsp/mundo/ft220107.htm. Acesso em: 20 out. 2024.

LOJÁN-CARRILLO, Sebastián Vicente; VÁZQUEZ-CALLE, José Luis. La discriminación y pasado judicial. Estudio del Sistema Informático de Trámites Judiciales SATJE. *Revista Arbitrada Interdisciplinaria KOINONIA*, [*s. l.*], v. 7, n. 2, edición especial, p. 737-752, 2022. Disponível em: http://dx.doi.org/10.35381/r.k.v7i2.2197. Acesso em: 8 nov. 2024.

LOPES, João Batista. Provas atípicas e efetividade do processo. *Revista Eletrônica de Direito Processual – REDP*, Rio de Janeiro, v. 5, p. 389. Disponível em: http://www.redp.com.br. Acesso em: 25 out. 2024.

LÓPEZ MEDINA, Carolina. Protección de datos personales en la Administración de Justicia española: Protocolo de Comunicación de la Justicia 2018. *Derecom*, [*s. l.*], n. 26, p. 115-130, 2019. Disponível em: http://www.derecom.com/derecom. Acesso em: 2 out. 2024.

LUCAS MARTÍN, F. Javier de. Democracia y transparencia. Sobre poder, secreto y publicidad. *Anuario de Filosofía del Derecho*, [*s. l.*], n. 7, p. 131-146, 1990.

MANN, Steve; NOLAN, Jason; WELLMAN, Barry. Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments. *Surveillance & Society*, [*s. l.*], v. 1, n. 3, p. 331-355, 2003. Disponível em: http://www.surveillance-and-society.org. Acesso em: 26 jan. 2024.

MANNHEIMER, Michael J. Z. Original Understandings and Four Problems of Modern Policing. *In*: MANNHEIMER, Michael J. Z. *The Fourth Amendment*: Original Understandings and Modern Policing. Ann Arbor: University of Michigan Press, 2023. p. 227-251. Disponível em: https://www.jstor.org/stable/10.3998/mpub.12158575.15. Acesso em: 13 ago. 2024.

MARCACINI, Augusto Tavares Rosa. *Processo e Tecnologia*: garantias processuais, efetividade e a informatização processual. 2011. 456 f. Tese (Livre Docência em Direito) – Universidade do Estado de São Paulo (USP), São Paulo, 2011.

MARIANO JUNIOR, Raul. *E-due process*: devido processo digital e acesso à justiça. São Paulo: Almedina, 2023.

MÁRQUEZ, Gabriel García. *Cem anos de solidão.* Tradução de Eliane Zagury. 28. ed. Rio de Janeiro: Record, 2008.

MARTIN, Kirsten; NISSENBAUM, Helen. What Is It About Location? *Berkeley Technology Law Journal*, [*s. l.*], v. 35, n. 1, p. 251-326, 2020. Disponível em: https://www.jstor.org/stable/10.2307/26954424. Acesso em: 13 ago. 2024.

MARTIN, Kirsten; NISSENBAUM, Helen. What Is It About Location? *Berkeley Technology Law Journal*, [*s. l.*], v. 35, n. 1, p. 251-326, 2020. Disponível em: https://www.jstor.org/stable/10.2307/26954424. Acesso em: 13 ago. 2024.

MARTÍNEZ GALINDO, Gemma. Problemática jurídica de la prueba digital y sus implicaciones en los principios penales. *Revista Electrónica de Ciencia Penal y Criminología*, [*s. l.*], v. 24, n. 23, 2022. Disponível em: http://criminet.ugr.es/recpc. Acesso em: 26 jan. 2024.

MARTINS, Robson; CALIL, Mário Lúcio Garcez; MARTINS, Erika Silvana Saquetti. O direito ao esquecimento e a proteção de dados: dados de consulta nas ações de improbidade administrativa. *In*: ARAS, Vladimir Barros; MENDONÇA, Andrey Borges de; CAPANEMA, Walter Aranha; SILVA, Carlos Bruno Ferreira da; COSTA, Marcos Antônio da Silva (org.). *Proteção de dados pessoais e investigação criminal.* São Paulo: Editora XYZ, 2020. p. 248-264.

MARX, Karl; ENGELS, Friedrich**.** *Manifesto Comunista*. São Paulo: Boitempo, 2010.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. *Curso de direito constitucional.* 13. ed. São Paulo: Saraiva, 2018.

MENDES, Gilmar Ferreira; COELHO, Inocêncio Mártires; BRANCO, Paulo Gustavo Gonet. *Hermenêutica constitucional e direitos fundamentais*. Brasília: Brasília Jurídica, 2002.

MENDES, Gilmar Ferreira; FERNANDES, Victor Oliveira. Constitucionalismo digital e jurisdição constitucional: uma agenda de pesquisa para o caso brasileiro. *Justiça do Direito*, [*s. l.*], v. 34, n. 2, p. 06-51, maio/ago. 2020.

MENDES, Gilmar Ferreira; OLIVEIRA FERNANDES, Victor. Constitucionalismo digital e jurisdição constitucional: uma agenda de pesquisa para o caso brasileiro. *Revista Brasileira de Direito*, Passo Fundo, v. 16, n. 1, p. 1-33, out. 2020. Disponível em: https://doi.org/10.18256/2238-0604.2020.v16i1.4103. Acesso em: 28 fev. 2022.

MENDES, Laura Schertel. Autodeterminação informativa: a história de um conceito. *Pensar Revista de Ciências Jurídicas Universidade de Fortaleza*, Fortaleza, v. 25, n. 4, 2020. p. 1-18.

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

MENDES, Paulo de Sousa. A privacidade digital posta à prova no processo penal. *Quaestio facti - Revista Internacional sobre Razonamiento Probatorio*, [*s. l.*], n. 2, p. 225-250, 2021. Disponível em: https://doi.org/10.33115/udg_bib/qf.i2.22487. Acesso em: 20 jun. 2024.

MENKE, Fabiano. As origens alemãs e o significado da autodeterminação informativa. *In*: MENKE, Fabiano; DRESCH, Rafael de Freitas Valle. *Lei Geral de Proteção de Dados*. Indaiatuba: FOCO, 2021.

MERCER, David. 33 Billion Internet Devices by 2020: Four Connected Devices for Every Person in World. *Strategy Analytics*, 2019. Disponível em: https://www4.strategyanalytics.com/default.aspx?mod=pressreleaseviewe r&a0=5609. Acesso em: 10 ago. 2024.

MICROSOFT. *What is ransomware?* Disponível em: https://www.microsoft.com/pt-br/security/business/security-101/what-is-ransomware. Acesso em: 22 out 2024.

MILLER, Greg; MUELLER, Peter F. CIA teve acesso direto a dados sobre violações de ditaduras sul-americanas. *O Estado de S. Paulo*, São Paulo, n. 46144, 18 fev. 2020. Internacional, p. A7. Disponível em: https://www2.senado.leg.br/bdsf/bitstream/handle/id/603678/noticia.html?sequence=1&isAllowed=y. Acesso em: 29 out. 2024.

MIRANDA, Pontes de. *Comentários do Código de Processo Civil.* 2. ed. Rio de Janeiro: Forense, 1958.

MIRANDA, Pontes. *Direito Processual Civil Brasileiro*. Rio de Janeiro: Forense, 1974.

MITIDIERO, Daniel; MARINONI, Luiz Guilherme; SARLET, Ingo Wolfgang. *Curso de direito constitucional.* 12. ed. São Paulo: SaraivaJur, 2023.

MITSILEGAS, Valsamis; GUILD, Elspeth; KUSKONMAZ, Emre; VAVOULA, Niovi. Data retention and the future of large-scale surveillance: The evolution and contestation of judicial benchmarks. *European Law Journal*, [*s. l.*], v. 29, n. 1-2, p. 176-211, 2023. DOI: 10.1111/eulj.12417.

MOLINA LUNA, Maryori; BENFELD, Johann S. Surgimiento y evolución del derecho de supresión de datos personales en motores de búsqueda de internet (derecho al olvido): Una mirada desde el derecho español y su proyección hacia el derecho comunitario europeo. *Revista Chilena de Derecho y Tecnología*, [*s. l.*], v. 12, 2023, p. 1-35.

MONTEIRO, Renato Leite. *Desafios para a efetivação do direito à explicação na Lei Geral de Proteção de Dados do Brasil.* 2021. 385 f. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2021.

MONTORO SÁNCHEZ, Juan Alejandro. La aportación de datos de carácter personal de terceros al proceso penal. *Revista Derecho y Proceso*, n. 1, jun. 2022. ISSN 2951-844X. Disponível em: jamonsan@upo.es. Acesso em: 26 jan. 2024.

MONTORO SÁNCHEZ, Juan Alejandro. La orden de conservación de datos: una medida de aseguramiento de fuentes de prueba imprescindible para la investigación de los delitos de odio cometidos en línea. *Revista Iberoamericana de Derecho Informático*, [*s. l.*], n. 13, p. 119-132, 2023.

MONTORO SÁNCHEZ, Juan Alejandro. Los principios rectores del tratamiento de datos de carácter personal y sus implicaciones en el proceso penal. *Revista Acta Judicial*, [*s. l.*], n. 10, p. 37-73, jul./dez. 2022.

MOREIRA, Rodrigo Pereira; ALVES, Rubens Valtecides. Direito ao esquecimento e o livre desenvolvimento da personalidade da pessoa transexual. *Revista de Direito Privado*, São Paulo, v. 64, out./dez. 2015, p. 81-102.

MORENO BOBADILLA, Ángela. The right to be forgotten in the US and Europe: same origin, different development. *Revista Chilena de Derecho*, [*s. l.*], v. 49, n. 2, p. 1-18, 2022. Disponível em: https://www.jstor.org/stable/10.2307/27206555. Acesso em: 27 jan. 2024.

MOURA, Maria Inês Dias. *A Base de Dados de Perfis de ADN em Portugal*: Questões emergentes. 2023. 92 f. Dissertação (Mestrado em Medicina Legal) — Instituto de Ciências Biomédicas Abel Salazar, Universidade do Porto, 2023.

MURDOCH, Steven J.; SENG, Daniel; SCHAFER, Burkhard; MASON, Stephen. The sources and characteristics of electronic evidence and artificial intelligence. *In*: MASON, Stephen; SENG, Daniel (ed.). *Electronic Evidence and Electronic Signatures*. London: University of London Press, 2021. Disponível em: https://www.jstor.org/stable/j.ctv1vbd28p.8. Acesso em: 27 jan. 2024

N.Y. Gov. Spitzer Resigns Amid Sex Scandal. PBS, [*s. l.*], 12 Mar. 2008. Disponível em: https://www.pbs.org/newshour/politics/politics-jan-june08-spitzer_03-12. Acesso em: 10 out. 2024.

NACIONES UNIDAS. *Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente:* Viena, 10 a 17 de abril de 2000. Viena: [*s. n.*], 2000. Disponível em: https://www.unodc.org/documents/congress/Previous_Congresses/10th_Congress_2000/030_ACONF.187.15_Report_of_the_Tenth_United_Nations_Congress_on_the_Prevention_of_Crime_and_the_Treatment_of_Offenders_S.pdf. Acesso em: 5 nov. 2024.

NATIONAL PARK SERVICE. *Jim Crow Laws*. Disponível em: https://www.nps.gov/malu/learn/education/jim_crow_laws.htm. Acesso em: 26 jan. 2024.

NERY JUNIOR, Nelson; NERY, Rosa Maria de Andrade. *Código de Processo Civil Comentado*. 18. ed. São Paulo: Revista dos Tribunais, 2019.

NETO, Antônio. Apontamentos no Direito Brasileiro dentro do contexto da Sociedade da Informação. *Revista Esmat*, Palmas, v. 5, n. 6, p. 11-30, jul./dez. 2013. Disponível em: http://esmat.tjto.jus.br/publicacoes/index.php/revista_esmat/article/view/57/63. Acesso em: 20 ago. 2024.

NIETZSCHE, Friedrich. *Assim falou Zaratustra*. Tradução de Mário da Silva. São Paulo: Companhia das Letras, 2011.

NISSENBAUM, Helen. Protecting privacy in an information age: the problem of privacy in public. *Princeton University, Law and Philosophy,* [*s. l.*], v. 17, p. 559-596, 1998.

O PODEROSO chefão. Direção: Francis Ford Coppola. Produção: Albert S. Ruddy. Intérpretes: Marlon Brando, Al Pacino, James Caan, Diane Keaton, Richard S. Castellano. Roteiro: Mario Puzo e Francis Ford Coppola. Estados Unidos: Paramount Pictures, 1972. 175 min.

OFFICIAL Journal of the European Union. Volume 59, 4 May 2016, L 119. Disponível em: https://publications.europa.eu/resource/cellar/99caafe9-11bc-11e6-ba9a-01aa75ed71a1.0006.03/DOC_1. Acesso em: 7 nov. 2024.

OMERTÀ. *In*: TRECCANI. Roma: Treccani, 2021. Disponível em: https://www.treccani.it/vocabolario/omerta. Acesso em: 6 jun. 2024.

O'NEIL, Cathy. *Weapons of math destruction*: how big data increases inequality and threatens democracy. Nova Iorque, 2016.

ORDEM DOS ADVOGADOS DO BRASIL. *Institucional/Quadro da advocacia*. Brasília, DF: OAB, 2024. Disponível em: https://www.oab.org.br/institucionalconselhofederal/quadroadvogados. Acesso em: 29 out. 2024.

ORLANDI, Renzo. La lucha procesal penal contra la criminalidad organizada en Italia. *In:* GÓMEZ COLOMER, Juan Luis, GONZÁLEZ CUSSAC, José Luis. *Terrorismo y proceso penal acusatorio*. Valencia: Tirant lo Blanch, 2006.

OROMÍ I VALL-LLORERA, Susanna. Acceso a datos personales conservados por proveedores de servicios de comunicaciones electrónicas en investigaciones penales según el Tribunal de Justicia de la UE. *Revista de Internet, Derecho y Política*, [*s. l.*], n. 31, out. 2020. Disponível em: http://dx.doi.org/10.7238/idp.v0i31.3206. Acesso em: 18 ago. 2024.

ORWELL, George. *1984*. São Paulo: Companhia das Letras, 2009.

PANAMA Papers: The secrets of dirty money. *BBC News*, 6 abr. 2016. Disponível em: https://www.bbc.com/news/world-35954224. Acesso em: 4 out. 2024.

PARLAMENTO EUROPEU E CONSELHO DA UNIÃO EUROPEIA. Diretiva (UE) 2011/92 de 13 de dezembro de 2011 sobre o combate ao abuso sexual e exploração sexual de crianças e pornografia infantil, substituindo a Decisão-Quadro 2004/68/JAI do Conselho. Jornal Oficial da União Europeia, nº L 335/1, 17 dez. 2011. Disponível em: https://eur-lex.europa.eu. Acesso em: 20 dez. 2023.

PARLAMENTO EUROPEU; CONSELHO DA UNIÃO EUROPEIA. Diretiva (UE) 2015/849 de 20 de maio de 2015 sobre a prevenção do uso do sistema financeiro para fins de lavagem de dinheiro ou financiamento do terrorismo, que altera o Regulamento (UE) nº 648/2012 do Parlamento Europeu e do Conselho, e revoga a Diretiva 2005/60/CE do Parlamento Europeu e do Conselho e a Diretiva 2006/70/CE da Comissão. Jornal Oficial da União Europeia, nº L 141/73, 5 jun. 2015. Disponível em: https://eur-lex.europa.eu. Acesso em: 20 dez. 2023.

PARLAMENTO EUROPEU; CONSELHO DA UNIÃO EUROPEIA. Diretiva (UE) 2011/36 de 5 de abril de 2011 sobre a prevenção e o combate ao tráfico de seres humanos e a proteção de suas vítimas, substituindo a Decisão-Quadro 2002/629/JAI do Conselho. Jornal Oficial da União Europeia, nº L 101/1, abr. 2011. Disponível em: https://eur-lex.europa.eu. Acesso em: 20 dez. 2023.

PASQUALE, Frank. *The black box society*: The secrets algorithms that control money and information. Cambridge: [*s. l.*], 2015.

PEÑA LABRIN, Daniel Ernesto. Ciberdelitos y criminalidad informática: rol de la prevención en la expansión de la ciberdelincuencia. *Informática y Derecho: Revista Iberoamericana de Derecho Informático (Segunda Época)*, Federação Iberoamericana de Associações de Direito e Informática, n. 13, 2023, p. 57-72.

PÉREZ ESTRADA, Miren J. La protección de los datos personales en el registro de dispositivos de almacenamiento masivo de información. *Revista Brasileira de Direito Processual Penal,* Porto Alegre, v. 5, n. 3, p. 1297-1330, set./dez. 2019. Disponível em: https://doi.org/10.22197/rbdpp.v5i3.253. Acesso em: 27 jan. 2024.

PÉREZ GIL, Julio. Medidas de investigación tecnológica en el proceso penal español: privacidad vs. eficacia en la persecución. *In*: BRIGHI, Raffaella; PALMIRANI, Monica; SÁNCHEZ JORDÁN, María Elena (ed.). *Informatica giuridica e informatica forense al servizio della società della conoscenza*: scritti in onore di Cesare Maioli. Rome: Aracne, 2018. p. 187-198.

PERŠAK, Nina. Procedural Justice Elements of Judicial Legitimacy and their Contemporary Challenges. *Oñati Socio-legal Series*, v. 6, n. 3, 2016

PESQUEIRA ZAMORA, María Jesús. Diligencias de investigación, cesión de datos y principio de proporcionalidad. *Revista de Estudios Jurídicos*, [*s. l.*], n. 20, p. 1-27, 2020. Disponível em: https://doi.org/10.31009/InDret.2020.i4.11. Acesso em: 18 ago. 2024.

PLATERO ALCÓN, Alejandro. LEXNET como máximo exponente del sistema de justicia electrónica en España: especial referencia a su tratamiento de datos personales. *Revista de Ciencias Jurídicas*, [*s. l*], n. 152, p. 13-42, maio/set. 2020.

POLO ROCA, Andoni. La regulación sobre la conservación de datos en el sector de las comunicaciones electrónicas o telecomunicaciones: estado de la cuestión. *Revista de Internet, Derecho y Política*, [*s. l.*], n. 33, octubre 2021. Disponível em: http://dx.doi.org/10.7238/idp.v0i33.373811. Acesso em: 18 abr. 2024.

PORTUGAL. *Decreto-Lei n.º 345/87*. Diário da República, 1987. Disponível em: https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/1987-34570075-50559675. Acesso em: 30 out. 2024.

PORTUGAL**.** Lei n.º 109/2009, de 15 de setembro. Estabelece o regime jurídico da alteração de nacionalidade portuguesa. *Diário da República*, 1.ª série, n.º 179, 15 set. 2009, p. 6319-6325. Disponível em: https://diariodarepublica.pt/dr/detalhe/lei/109-2009-489693. Acesso em: 30 out. 2024.

RAMÍREZ ARTAVIA, L. Acceso a la información pública: El principio es la publicidad y el secreto la excepción. *Revista Centroamericana de Administración Pública*, *[s. l.]*, n. 56-57, p. 31–98, 2009. Disponível em: https://ojs.icap.ac.cr/index.php/RCAP/article/view/271. Acesso em: 12 feb. 2024.

RATHI, Mohit. Rethinking reverse location search warrants. *The Journal of Criminal Law and Criminology*, [*s. l.*], v. 111, n. 3, p. 805-837, primavera 2021. Disponível em: https://www.jstor.org/stable/10.2307/4861779. Acesso em: 13 ago. 2024.

RAYÓN BALLESTEROS, María Concepción. Medidas de investigación tecnológica en el proceso penal: la nueva redacción de la Ley de Enjuiciamiento Criminal operada por la Ley Orgánica 13/2015. *Anuario Jurídico y Económico Escurialense*, [*s. l.*], v. LII, p. 179-204, 2019.

REINO UNIDO. *Justice and Security Act 2013*. Londres, 25 abr. 2013. Disponível em: https://www.legislation.gov.uk/ukpga/2013/18/contents. Acesso em: 8 nov. 2024.

RICHTER, André. Um ano após tentativa de golpe, STF mantém 66 presos. *Agência Brasil*, Brasília, 07 jan. 2024. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2024-01/um-ano-apos-tentativa-de-golpe-stf-mantem-66-presos. Acesso em: 5 nov. 2024.

RIZZO, Giuseppe. *Derecho a la privacidad y seguridad en el espacio público europeo*. 2023. Tese (Doutorado em Direito) — Universidad Carlos III de Madrid, 2023.

ROBERTS, J. V. Public Opinion, Criminal Record, and the Sentencing Process. *American Behavioral Scientist*, [*s. l.*], v. 39, n. 4, p. 488-499, 1996. Disponível em: https://doi.org/10.1177/0002764296039004011. Acesso em: 26 jan. 2024.

ROBL FILHO, Ilton Norberto. Alguns apontamentos sobre o constitucionalismo digital. *Consultor Jurídico*, São Paulo, 22 de janeiro de 2022. Disponível em: https://www.conjur.com.br/2022-jan-22/observatorio-constitucional-alguns-apontamentos-constitucionalismo-digital. Acesso em: 26 fev. 2022.

ROCHA, Cláudio Iannotti da; MANSUR, Maria Júlia Ferreira. O estabelecimento do devido processo informacional pela Lei Geral de Proteção de Dados no tratamento de dados pessoais. *Revista Direito das Relações Sociais e Trabalhistas*, v. 8, n. 2, p. 109-122, jul. 2022.

ROSA, Alexandre Morais da. Devido processo (penal) substancial: 25 anos depois da CR/88. *Revista Brasileira de Direito*, [*s. l.*], v. 9, n. 1, p. 25-56, jan./jun. 2013.

ROSALES LEAL, Miguel Ángel. *Los derechos fundamentales como límite de las medidas de investigación tecnológica*: especial referencia a la captación y grabación de comunicaciones orales directas. 2021. Tese (Doutorado em Ciências Jurídicas) - Universidad de Granada, Granada, 2021. Disponível em: http://hdl.handle.net/10481/71619. Acesso em: 26 jna. 2024.

ROVELLI, Sophia. Case Prokuratuur: Proportionality and the Independence of Authorities in Data Retention. *European Papers*, v. 6, n. 1, p. 199-210, 2021. Disponível em: http://www.europeanpapers.eu/en/content/e-journal/EP_eJ_2021_1. Acesso em: 20 ago. 2024.

RUSSELL, Lauren. "*The New Jim Crow:*" Employer Access to Criminal Record Information and Racial Differences in Labor Market Outcomes. Harvard University, 2022. Disponível em: https://scholar.harvard.edu/files/laurenrussell/files/jmp_12.21.2022.pdf. Acesso em: 26 jan. 2024.

RUSSIA spy poisoning: What we know so far. *BBC News*, 20 mar. 2018. Disponível em: https://www.bbc.com/news/uk-43480978. Acesso em: 4 out. 2024.

SAAD, Marta. Editorial do dossiê "Investigação preliminar: desafios e perspectivas". *Revista Brasileira de Direito Processual Penal*, Porto Alegre, v. 6, n. 1, p. 29-40, jan./abr. 2020. Disponível em: https://doi.org/10.22197/rbdpp.v6i1.348. Acesso em: 22 out. 2024.

SÁNCHEZ ARISTI, Rafael. El derecho al olvido y las hemerotecas digitales. La Sentencia del Tribunal Constitucional 58/2018, de 4 de junio. *Actualidad Jurídica Uría Menéndez*, n. 50, p. 124-131, 2018.

SÁNCHEZ MEDRANO, Francisco de Paula. O registro de dispositivos de armazenamento massivo de informação. *Revista Derecho y Proceso*, [*s. l.*], n. 1, jun. 2022, p. 99-101.

SANTIAGO NETO, José de Assis. O devido processo legal e o (in)devido processo penal brasileiro: entre a acusatoriedade constitucional e o inquisitorial modelo do Código de Processo Penal. *RDFG – Revista de Direito da Faculdade Guanambi*, Guanambi, v. 3, n. 1, p. 164-178, jul.-dez. 2016.

SANTOS, Célio Jacinto dos. Teoria da Investigação Criminal. Belo Horizonte: Del Rey, 2020.

SANTOS, Ives Nahama Gomes dos; SILVA, Dhean Lucca Alves da. A necessidade de segurança dos dados sensíveis no Sistema Processual Penal. *Revista Científica do CPJM*, Rio de Janeiro, v. 2, n. 7, p. 177-189, 2023. Disponível em: https://doi.org/10.55689/rcpjm.2023.07.010. Acesso em: 28 out. 2024.

SÃO PAULO. Tribunal de Justiça. Agravo n.º 16.886. Rel. Des. Antonino Vieira, 27 set. 1930. Revista dos Tribunais, São Paulo, n. 76, p. 100-101.

SARAMAGO, José. *Ensaio sobre a cegueira*. São Paulo: Companhia das Letras, 1995.

SARLET, Ingo Wolfgang; CUNDA, Daniela Zago Gonçalves da; RAMOS, Rafael (coord.). *Lei de acesso à informação*: estudos em homenagem aos 10 anos da Lei nº 12.527/2011. Porto Alegre: Fundação Fênix, 2022. (Série Direito; 59).

SARLET, Ingo Wolfgang; FERREIRA NETO, Arthur M. *O direito ao esquecimento na sociedade da informação*. Porto Alegre: Livraria do Advogado, 2019.

SARLET, Ingo Wolfgang; SARLET, Gabrielle Bezerra Sales. Algumas notas sobre a relação entre inteligência artificial, proteção de dados pessoais e os direitos fundamentais na ordem constitucional brasileira. *Revista Jurídica de Asturias*, [*s. l.*], n. 45, p. 85-103, 2022.

SARLET, Ingo Wolfgang; SARLET, Gabrielle Bezerra Sales. Direitos Fundamentais: Separação informacional de poderes e devido processo informacional. *Consultor Jurídico*, São Paulo, 13 maio 2022. Disponível em: https://www.conjur.com.br/2022-mai-13/separacao-informacional-poderes-devido-processo-informacional. Acesso em: 8 set. 2024.

SCHWAB, Klaus. *A Quarta Revolução Industrial*. São Paulo: Edipro, 2016.

SEYYAR, M. Bas; GERADTS, Z.J.M.H. Privacy impact assessment in large-scale digital forensic investigations. *Forensic Science International: Digital Investigation*, [*s. l.*], v. 33, p. 1-9, June 2020. Disponível em: https://www.elsevier.com/locate/fsidi. Acesso em: 25 jan. 2024.

SHI, Changqing; SOURDIN, Tania; LI, Bin. The Smart Court – A New Pathway to Justice in China? *International Journal for Court Administration*, v. 12, n. 1, 2021. Disponível em: https://doi.org/10.36745/ijca.367. Acesso em: 26 jan. 2024.

SILVA, Gabriela Buarque Pereira; MOURA, Tâmara. Prisão em flagrante e acesso a dados de celular: desafios entre a privacidade e a investigação criminal. *In*: ARAS, Vladimir Barros; MENDONÇA, Andrey Borges de; CAPANEMA, Walter Aranha; SILVA, Carlos Bruno Ferreira da; COSTA, Marcos Antônio da Silva (org.). *Proteção de Dados Pessoais e Investigação Criminal.* Brasília: ANPR, 2020. p. 399-431.

SILVA, R. G.; SILVA, L. G.; SILVA, K. T. P. de O. Impacto da LGPD na legitimação dos atos judiciais sob o prisma do princípio da publicidade. *Revista Jurídica Direito & Paz*, São Paulo, v. 16, n. 46, p. 230-248, 1º Semestre 2022.

SILVA, Virgílio Afonso da. *Direitos Fundamentais*: conteúdo essencial, restrições e eficácia. 2. ed. São Paulo: Malheiros, 2017.

SILVA, Virgílio Afonso da. O conteúdo essencial dos direitos fundamentais e a eficácia das normas constitucionais. *Revista de Direito do Estado*, Rio de Janeiro, 4, p. 23-51, 2006. Disponível em: https://constituicao.direito.usp.br/wp-content/uploads/2006-RDE4-Conteudo_essencial.pdf. Acesso em: 3 nov. 2024.

SNYDER, David L. Nonparty remote electronic access to plea agreements in the Second Circuit. *Fordham Urban Law Journal,* v. 35, n. 5, art. 7, 2008. Disponível em: https://core.ac.uk/download/pdf/144228589.pdf. Acesso em: 10 nov. 2024.

SPOSATO, Karyna Batista; CARDOSO, Henrique Ribeiro; SOUSA JÚNIOR, Eliezer Siqueira de. Devido processo legal e o conceito de justo: o consenso para a gestão de conflitos em um devido processo penal ético e dialogado. *Revista de Estudos Constitucionais, Hermenêutica e Teoria do Direito (RECHTD)*, [*s. l.*], v. 14, n. 1, p. 101-118, jan.-abr. 2022. Disponível em: https://doi.org/10.4013/rechtd.2022.141.07. Acesso em: 05 ago. 2024

STRECK, Lenio Luiz. *As interceptações telefônicas e os Direitos Fundamentais*: Constituição, Cidadania, Violência: a Lei 9.296/96 e seus reflexos penais e processuais. 2. ed. rev. ampl. Porto Alegre: Livraria do Advogado, 2001.

SUPREME COURT OF THE UNITED STATES. Burns Baking Co. v. Bryan, 269 U.S. 385 (1926). Disponível em: https://supreme.justia.com/cases/federal/us/269/385/. Acesso em: 30 out. 2024.

SUSSKIND, Jamie. The Digital Republic. New York: Pegasus Books, 2022.

SUXBERGER, Antonio H. G.; FURTADO, Valtan T. M. M. Investigação criminal genética – banco de perfis genéticos, fornecimento compulsório de amostra biológica e prazo de armazenamento de dados. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, v. 4, n. 2, p. 809-842, maio/ago. 2018. Disponível em: https://doi.org/10.22197/rbdpp.v4i2.122. Acesso em: 20 ago. 2024.

TABORDA, Maren Guimarães. O princípio da publicidade e a participação na administração pública. 2006. p. 65. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2006.

THE ECONOMIST. The world's most valuable resource is no longer oil, but data. *The Economist*, 6 May 2017. Disponível em: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. Acesso em: 4 out. 2024.

THE POLITICS of whitewater. Congressional Record, v. 142, n. 113, July 1996, p. S9082-S9083. Disponível em: https://www.govinfo.gov/content/pkg/CREC-1996-07-29/html/CREC-1996-07-29-pt1-PgS9082-2.htm. Acesso em: 29 out. 2024.

THE WORLD'S most valuable resource is no longer oil, but data. *The economist,* [*s. l.*], 6 maio 2017. Disponível em: www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. Acesso em: 27 jan. 2024.

TRINDADE, Rodrigo. Grande irmão: China proibiu 23 milhões de viagens de avião ou trem em 2018. *UOL Tilt*, 3 mar. 2019. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2019/03/03/grande-irmao-china-proibiu-23-milhoes-de-viagens-de-aviao-ou-trem-em-2018.htm. Acesso em: 4 out. 2024.

TURNER, Paul. Management During the Third Industrial Revolution: Asian Tigers and Global Players. *In*: TURNER, Paul. *The Making of the Modern Manager*. Cham: Palgrave Macmillan, 2021. Disponível em: https://doi.org/10.1007/978-3-030-81062-7_4. Acesso em: 29 ago. 2024.

UNIÃO EUROPEIA. *Carta dos Direitos Fundamentais da União Europeia (CDFUE)*. Jornal Oficial da União Europeia, [*s. l.*], 7 jun. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT. Acesso em: 30 out. 2024.

UNIÃO EUROPEIA. *Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016*. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680. Acesso em: 30 out. 2024.

UNIÃO EUROPEIA. *Diretiva 2002/21/CE do Parlamento Europeu e do Conselho, de 7 de março de 2002.* Estabelece um quadro regulamentar comum para as redes e serviços de comunicações eletrônicas (Diretiva-Quadro). Disponível em: https://eur-lex.europa.eu. Acesso em: 30 out. 2024.

UNIÃO EUROPEIA. *Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995*. Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: https://eur-lex.europa.eu. Acesso em: 30 out. 2024.

UNIÃO EUROPEIA. Tratado sobre o Funcionamento da União Europeia (TFUE*)*. *Jornal Oficial da União Europeia*, [*s. l.*], 7 jun. 2016. Disponível em: https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_3&format=PDF. Acesso em: 30 out. 2024.

UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia (Grande Sala). *Tele2 Sverige e Watson e outros* (Processos C-203/15 e C-698/15, EU:C:2016:970), julgamento em 21 de dezembro de 2016, parágrafo 115. Luxemburgo: TJUE, 2016.

UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia (Grande Sala). *Decisão de 2 de outubro de 2018* (Processo C-207/16, EU:C:2018:788). Luxemburgo: TJUE, 2018.

UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia. Asuntos acumulados C-511/18, C-512/18 y C-520/18, La Quadrature du Net y otros contra Premier ministre y otros. 6 de octubre de 2020.

UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia. Caso C-207/16 Ministerio Fiscal, 2 de octubre de 2018.

UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia. *Processo C-131/12.* Google Spain v. Agencia Española de Protección de Datos (APED). 13 maio 2014. ECLI:EU:C:2014:317. Disponível em: https://eur-lex.europa.eu. Acesso em: 30 out. 2024.

UNITED KINGDOM. House of Lords. *Judgments - Helow (Ap) V Secretary of State for the Home Department and Another (Scotland) Appellate.* Sessão 2007-08. Disponível em: https://publications.parliament.uk/pa/ld200708/ldjudgmt/jd081022/helow-1.htm. Acesso em: 8 nov. 2024.

UNITED KINGDOM. House of Lords. Scott (Otherwise Morgan) and Another Appellants; and Scott Respondent. *Lords' Journals*, 5 maio 1913. Disponível em: http://www.bailii.org/uk/cases/UKHL/1913/2.html. Acesso em: 08 nov. 2024.

UNITED NATIONS. *Draft United Nations convention against cybercrime*: Strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes. A/AC.291/L.15, August, 2024. Disponível em: https://documents.un.org/doc/undoc/gen/v24/055/06/pdf/v2405506.pdf. Acesso em: 22 out. 2024.

UNITED STATES CONGRESS. Fifth Amendment: Overview. *Constitution Annotated*. Washington: Library of Congress. Disponível em: https://constitution.congress.gov/browse/essay/amdt5-8-1/ALDE_00013739/. Acesso em: 30 out. 2024.

UNITED STATES. *Brady Handgun Violence Prevention Act*, Pub. L. No. 103-159, 107 Stat. 1536 (1993) (codified as amended at 18 U.S.C. § 921).

UNITED STATES. Court of Appeals (4th Circuit). United States v. Moussaoui, 483 F.3d 220 (2007).

UNITED STATES. Court of Appeals (9th Cir.). *858 F.2d 1427.* [*S. l.: s. n.*], 1988.

UNITED STATES. Department of Justice. Bureau of Justice Statistics (BJS). Jan. 2020. Disponível em: https://www.ojp.gov/about/offices/bureau-justice-statistics-bjs. Acesso em: 8 nov. 2024.

UNITED STATES. *E-Government Act of 2002*, Pub. L. No. 107-347, § 205, 116 Stat. 2899, 2913-14 (codified as amended at 44 U.S.C. § 3501 (2000).

UNITED STATES. Fourth Amendment to the United States Constitution. *Constitution Annotated*. Disponível em: https://constitution.congress.gov/constitution/amendment-4/. Acesso em: 7 nov. 2024.

UNITED STATES. Presley v. Geórgia, 558 EUA, 130 S. Ct. 721, 724, 2010.

UNITED STATES. Supreme Court. Visitors Guide to oral argument. Dispnível em: https://www.supremecourt.gov/visiting/visitorsguidetooralargument.aspx. Acesso em: 19 out. 2024.

UNIVERSIDADE DE COIMBRA. Privacidade e proteção de dados. *Universidade de Coimbra*, Coimbra, 2024. Disponível em: https://www.uc.pt/protecao-de-dados-e-informacao-administrativa/protecao-de-dados-pessoais/privacidade-e-protecao-dados/. Acesso em: 4 out. 2024.

VALENTE, Manuel Monteiro Guedes. *Teoria geral do direito policial*. 2. ed. Coimbra: Almedina, 2009.

VALIER, Claire. True Crime Stories: Scientific Methods of Criminal Investigation, Criminology and Historiography. *The British Journal of Criminology*, [*s. l.*], v. 38, n. 1, p. 88-105, Winter 1998. Disponível em: https://www.jstor.org/stable/23638584. Acesso em: 26 jan. 2024.

VAN DEN HOOGEN, Ronald. Will e-justice still be justice? Principles of a fair electronic trial. *International Journal for Court Administration*, [*s. l.*], v. 1, n. 1, p. 65-[ii], 2008.

WHO is a rat. 2024. Disponível em: whosarat.com. Acesso em: 10 nov. 2024.

WILSON, Nigel; SHELDON, Andrew; DRIES, Hein; SCHAFER, Burkhard; MASON, Stephen. Proof: the technical collection and examination of electronic evidence. *In*: MASON, Stephen; SENG, Daniel (ed.). *Electronic Evidence and Electronic Signatures*. London: University of London Press, 2021. p. 429-487. Disponível em: https://www.jstor.org/stable/j.ctv1vbd28p.16. Acesso em: 13 ago. 2024.

WOLTER, Jurgen. *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. São Paulo: Marcial Pons, 2018.

XAVIER, J. T. N.; SANTOS, A. L. L. dos. A aplicabilidade do direito ao esquecimento às pessoas condenadas penalmente. *Revista da Faculdade de Direito da UFRGS*, Porto Alegre, n. 50, p. 126–149, 2022. Disponível em: https://seer.ufrgs.br/index.php/revfacdir/article/view/113622. Acesso em: 25 set. 2024

ZAMBRANA, Lorenzo Luna. Consecuencias de la anulación de la directiva europea de conservación de metadatos de las comunicaciones electrónicas. Una encrucijada en la lucha contra la delincuencia grave. *Revista de Derecho de la UNED (RDUNED)*, [*s. l.*], n. 30, p. 183-222, 2023. Disponível em: https://doi.org/10.5944/rduned.30.2022.36848. Acesso em: 29 jan. 2024.

ZAMBRANO MEZA, Francisco. Notas para una reforma constitucional sobre acceso a la información pública, publicidad y transparencia. *Revista de Derecho Público*, número especial, p. 127-148, 2018.