

A PRODUÇÃO PROBATÓRIA POR MEIOS DIGITAIS NO ÂMBITO DO PROCESSO PENAL E NA ERA DO CAPITALISMO DE VIGILÂNCIA

Thiago Cantídio de Freitas¹

Camila Geraseev Fernandes²

Kauã Oliveira Rodrigues³

Guilherme Roedel Fernandez Silva⁴

RESUMO

O presente artigo analisa a produção probatória por meios digitais no processo penal brasileiro à luz do Recurso Extraordinário 1301250 do STF, que discute os limites constitucionais da quebra de sigilo de dados em investigações criminais. O objetivo central é compreender como articular os princípios constitucionais da privacidade, do devido processo legal e da legalidade aos desafios impostos pela digitalização massiva da vida social contemporânea. A pesquisa, de natureza qualitativa, emprega o método dedutivo e revisão bibliográfica, analisando doutrinas jurídicas, decisões judiciais e teorias contemporâneas sobre vigilância digital, mobilizando autores como Shoshana Zuboff, Byung-Chul Han e Michel Foucault para contextualizar a interpretação constitucional brasileira. O estudo demonstra

¹Graduando em Direito pela Universidade Estadual de Montes Claros. ORCID: <https://orcid.org/0009-0002-8457-8880> E-mail: thiagocantidiodefrees@gmail.com.

²Graduanda em Direito pela Universidade Estadual de Montes Claros. ORCID: <https://orcid.org/0009-0005-5909-6478>. E-mail: camilageraseev@gmail.com.

³Graduando em Direito pela Universidade Estadual de Montes Claros. ORCID: <https://orcid.org/0009-0008-8417-4513>. E-mail: kauaolioli@gmail.com.

⁴Doutorando em Direito pela Universidade Estadual de Montes Claros. ORCID: <https://orcid.org/0009-0007-1478-0051>. E-mail: guilherme.silva@unimontes.br.

que a sociedade contemporânea, marcada pelo capitalismo de vigilância, transformou radicalmente a natureza da prova penal, exigindo regime jurídico específico que supere a aplicação analógica de diplomas legislativos concebidos em contextos tecnológicos distintos. A análise revela a tensão entre eficiência investigativa e proteção de direitos fundamentais, evidenciando que a vigilância digital opera através de três elementos centrais: informação, banco de dados e perfis comportamentais. Conclui-se pela necessidade urgente de adequação do processo penal brasileiro aos desafios da era digital, estabelecendo limites constitucionais claros para a quebra de sigilo de dados que conciliam segurança pública e proteção da privacidade, considerando que a decisão do STF terá aplicação vinculante a casos futuros análogos.

Palavras-chave: Capitalismo de vigilância; Prova digital; Hipermassificação informativa; Garantismo penal.

*EVIDENCE PRODUCTION THROUGH DIGITAL MEDIA IN CRIMINAL
PROCEEDINGS: LIMITS OF BREACHING INTERNET USER PRIVACY IN THE ERA
OF SURVEILLANCE CAPITALISM*

ABSTRACT

This article analyzes the production of evidence through digital means in Brazilian criminal proceedings in light of the Supreme Federal Court's Extraordinary Appeal 1301250, which discusses the constitutional limits of breaching data confidentiality in criminal investigations. The central objective is to understand how to articulate the constitutional principles of privacy, due process, and legality with the challenges posed by the massive digitization of contemporary social life. The research, qualitative in nature, employs the deductive method and bibliographic review, analyzing legal doctrines, judicial decisions, and contemporary theories on digital surveillance, drawing on authors such as Shoshana Zuboff, Byung-Chul Han, and Michel Foucault to contextualize the Brazilian constitutional interpretation. This study demonstrates that contemporary society, marked by surveillance capitalism, has radically transformed the nature of criminal evidence, demanding a specific legal regime that overcomes the analogical application of legislative instruments conceived in distinct technological contexts. The analysis reveals the tension between investigative efficiency and the protection of fundamental rights, highlighting that digital surveillance operates through three central elements: information, databases, and behavioral profiles. It concludes that there is an urgent need to adapt the Brazilian criminal procedure to the challenges of the digital age, establishing



clear constitutional limits for the breach of data confidentiality that reconcile public security and privacy protection, considering that the Supreme Court's decision will have binding application to analogous future cases.

Keywords: Surveillance capitalism; Digital evidencer; Information hyper-distribution; Criminal law guarantees.

*PRODUCCIÓN DE PRUEBAS POR MEDIOS DIGITALES EN PROCESOS PENALES:
LÍMITES DE LA VIOLACIÓN DE LA PRIVACIDAD DE LOS USUARIOS DE
INTERNET EN LA ERA DEL CAPITALISMO DE VIGILANCIA*

RESUMEN

Este artículo analiza la producción de pruebas digitales en los procesos penales brasileños a la luz del Recurso Extraordinario 1301250 del Supremo Tribunal Federal, que aborda los límites constitucionales de la confidencialidad de los datos en las investigaciones penales. El objetivo principal es comprender cómo articular los principios constitucionales de privacidad, debido proceso y legalidad con los desafíos que plantea la digitalización masiva de la vida social contemporánea. La investigación, de carácter cualitativo, emplea el método deductivo y la revisión bibliográfica, analizando doctrinas jurídicas, decisiones judiciales y teorías contemporáneas sobre vigilancia digital, recurriendo a autores como Shoshana Zuboff, Byung-Chul Han y Michel Foucault para contextualizar la interpretación constitucional brasileña. Este estudio demuestra que la sociedad contemporánea, marcada por el capitalismo de vigilancia, ha transformado radicalmente la naturaleza de la prueba penal, exigiendo un régimen jurídico específico que supere la aplicación analógica de instrumentos legislativos concebidos en distintos contextos tecnológicos. El análisis revela la tensión entre la eficiencia investigativa y la protección de los derechos fundamentales, destacando que la vigilancia digital opera a través de tres elementos centrales: información, bases de datos y perfiles conductuales. Concluye que existe una necesidad urgente de adaptar el procedimiento penal brasileño a los desafíos de la era digital, estableciendo límites constitucionales claros para la violación de la confidencialidad de los datos que concilien la seguridad pública y protección de la privacidad, considerando que la decisión de la Corte Suprema tendrá aplicación vinculante en casos futuros similares.



Palabras clave: Capitalismo de vigilancia; Pruebas digitales; Hiperdistribución de información; Garantías penal.

INTRODUÇÃO

O Recurso Extraordinário (RE) 1301250, atualmente sob análise do Supremo Tribunal Federal (STF) discute os limites constitucionais da quebra de sigilo de dados em investigações criminais, situando-se na interseção entre segurança pública e direitos fundamentais. O julgamento questiona a constitucionalidade da decretação judicial da quebra de sigilo de dados de conexão e de registros de acesso a aplicações de internet, no âmbito de procedimentos penais, em relação a pessoas indeterminadas e, ainda, se essa medida pode ocorrer mediante requisição direta da autoridade policial ou se exige, invariavelmente, autorização judicial prévia.

Desse modo, esta pesquisa parte da relevância temática que a era digital impôs ao sistema jurídico brasileiro, especialmente no que concerne à proteção da privacidade e ao sigilo de dados pessoais dos usuários da internet. O problema central que orienta este estudo consiste em discutir a produção probatória por meios digitais no processo penal brasileiro, considerando o contexto de uma sociedade marcada pela virtualização extrema das relações interpessoais.

A pesquisa justifica-se pela necessidade de adequar o processo penal aos desafios da era digital. Trata-se, especialmente, da convergência temática com o RE 1301250 do STF, que teve reconhecida sua repercussão geral. Consequentemente, a tese jurídica firmada neste recurso será aplicada de forma vinculante a todos os casos futuros análogos.

A presente investigação se vale da interdisciplinaridade das teorias contemporâneas sobre vigilância, controle e poder como instrumento analítico para contextualizar a interpretação constitucional dos limites da quebra de sigilo de dados

no ordenamento jurídico brasileiro. Autores como Shoshana Zuboff (2020) e sua teoria acerca do capitalismo de vigilância, bem como Byung-Chul Han (2022) e sua concepção de sociedade do controle e da transparência e Michel Foucault (1996), por meio de sua teoria sobre o biopoder, são mobilizados para direcionar a discussão sociojurídica deste estudo.

Metodologicamente, a pesquisa é de natureza qualitativa através do qual se concentra na interpretação de leis, textos, decisões judiciais, dentre outros. Ademais, foi empregado o método de revisão bibliográfica, com a leitura e análise de doutrinas jurídicas, artigos e notícias com temática crítica e diversa. Quanto ao método de abordagem, utilizou-se o método dedutivo, que parte de premissas gerais para chegar a conclusões específicas, permitindo apresentar esclarecimentos e conclusões sobre a temática.

O objetivo geral deste trabalho é compreender como articular os princípios constitucionais, como a privacidade, o devido processo legal e a legalidade, aos desafios impostos pela digitalização massiva da vida social contemporânea.

1. A CIVILIZAÇÃO DA INFORMAÇÃO E A VIGILÂNCIA DIGITAL

A formação social brasileira contemporânea, assim como da sociedade global, é profundamente marcada pela influência digital. No contexto da expansão da rede mundial de computadores, a sua atuação concentra-se nos sistemas de hipermídias como textos, imagens e vídeos, conectados por meio da internet. Desse modo, afirma Byung-Chul Han (2022) que o acúmulo de dados, seus acessos e processamentos exercem um poder expressamente maior do que o típico capitalismo industrial do século XIX e XX.

Nesse sentido, a sua disseminação e seu estabelecimento mundial, geridos por empresas privadas, alcunhadas de *big techs*, foi impactante e com



consequências sociopolíticas ainda sob análise. Em outras palavras, há a ascensão de uma nova modalidade de produzir o capitalismo, não mais especializada na intensificação dos meios de produção.

De acordo com a análise de Zuboff (2020), a experiência humana contemporânea, por meio da utilização reiterada dos meios virtuais, transforma os dados digitais dos usuários em matéria prima gratuita que, posteriormente, são comercializados em uma nova modalidade de mercado que utiliza fontes cada vez mais preditivas capazes de criar um comércio de comportamentos. A sua atuação é superior ao anúncios online direcionados, mas concentra-se na influência do comportamento dos usuários desde o que consumir até em quem se deve votar.

Assim, essa nova faceta do capitalismo do século XXI se concentra principalmente na extração dos dados digitais dos usuários, matéria prima do mercado digital de dados.

Desse modo, os usuários das tecnologias digitais estão sob efeito de uma constante vigilância que não é física nem palpável, mas resultado de uma nova espécie de poder que, conforme Zuboff (2020):

Em vez de armamentos e exércitos faz valer sua vontade através do meio automatizado de uma arquitetura computacional cada vez mais ubíqua composta de dispositivos, coisas e espaços “inteligentes” conectados em rede. (Zuboff, 2020, p.19).

Dessa forma, sem esgotar o tema, as proposições de Foucault (1996) sobre a vigilância e o exercício do poder colaboram para interpretar as disposições da atualidade. Nesse contexto, para o filósofo francês, poder e saber são atitudes interligadas, pois quanto mais se conhece mais se controla. Assim, o saber é definido pelo conhecimento da conduta e do comportamento de quem se pretende vigiar (Foucault, 1996).

A vigilância, portanto, possibilita o domínio do sujeito sem uso de violência, funcionando permanentemente e em grande parte em silêncio (Foucault, 1996,



p.158). No contexto da vigilância digital, a discrição deliberada e imperceptível é proposital, uma vez que a discrição ofusca os métodos de funcionamento e destinação dos dados dos usuários pelas empresas de tecnologia, transformando a vigilância em um modelo virtualmente onipresente e contínuo (Dal Castel; Gonçalves, 2025).

Nesse sentido, a vigilância digital edifica-se em três elementos centrais: a informação, o banco de dados e os perfis comportamentais. (Bruno, 2008, p. 170). Em primeiro lugar, a tríade de elementos se converge quando os bancos de dados são criados com base no registro das informações dos usuários e nos rastros deixados no ciberespaço. Logo após ocorre o recolhimento, análise e armazenamento desses dados, formando os perfis comportamentais. Os referidos perfis se tornam matéria prima e produto nos chamados “mercados comportamentais” (Zuboff, 2020), que abrange diversos setores, tais como lojas de varejo, ramo de finanças e setores de seguros.

Entretanto, apesar de parecer uma prática típica das relações privadas e das *big techs*, o uso da vigilância digital também tem sido instrumentalizado pelo Estado e pelos sujeitos de Direito Público. Atualmente, estima-se que mais de 75% das forças policiais em todo o mundo utilizem algum tipo de tecnologia de vigilância digital (Bischoff, 2021).

No contexto brasileiro, transportar práticas de vigilância digital para a segurança pública e para persecução penal, sob a justificativa de maior eficiência, inaugura debates necessários acerca de seus limites no processo penal do Estado Democrático de Direito. Esse tema, central no direito processual penal contemporâneo, figura hoje tanto como tema de julgamentos perante os tribunais superiores no Brasil e matéria de debate social.

2. A NOVA ERA DA PRODUÇÃO PROBATÓRIA NO PROCESSO PENAL BRASILEIRO

A revolução digital transformou radicalmente a natureza, o volume e as possibilidades de produção probatória no processo penal brasileiro. Enquanto no modelo tradicional as provas eram, em sua maioria, físicas, testemunhais ou documentais, todas sujeitas a limitações de volume, persistência e capacidade de análise, na era digital a prova adquire contornos qualitativamente distintos.

Nesse contexto, conforme preceitua Eilberg (2024), os desafios e dilemas tornam-se evidentes ao constatar que determinados avanços tecnológicos passaram a gerar transformações significativas nos métodos de investigação criminal em âmbito global, especialmente no que se refere ao processamento e à armazenagem em larga escala de dados. Tal avanço impacta diretamente em aspectos específicos da produção de provas digitais.

Dessa forma, Paul Virilio (1999) e Jean Baudrillard (2003) já traziam à ideia da “hipermassificação informativa processual”, consistente no fenômeno de geração, difusão e acesso em larga escala de informações relacionadas a processos judiciais, impulsionado pelo avanço da internet e pela implementação dos sistemas eletrônicos de justiça. Esse processo ampliou significativamente o volume e a velocidade de circulação dos dados processuais, redefinindo a forma como as informações judiciais são produzidas, compartilhadas e consultadas.

A polissemia da palavra “prova” assume, portanto, novos contornos que são fruto da massificação virtual. A prova digital é definida como qualquer expressão capaz de representar uma ideia ou um fato encaminhada ou produzida em ambiente virtual, caracterizado pela imaterialidade e volatilidade (Saad, Costa Rossi, Partata, 2024). Desse modo, o termo “prova digital” enquadra-se na categoria de fonte de prova, pois, consoante leciona Brasileiro (2022), esta se constitui de tudo aquilo que



possa contribuir para o esclarecimento da ocorrência ou não de um crime, sendo incorporada ao processo penal através dos meios de prova.

Nesse sentido, os dados digitais representados por endereço de protocolo de internet (IP), dados de localização, informações de navegação, pesquisa na internet, histórico de compras, interações em redes sociais podem assumir um duplo caráter no processo penal brasileiro: ser meio de provas ou meio de obtenção de provas.

A distinção central entre as duas categorias é que

Os meios de obtenção da prova são instrumentos que servem para investigar e recolher meios de prova. Os meios de prova, por sua vez, caracterizam-se pela sua aptidão para serem por si mesmos fonte de convencimento (Silva, 1999, p. 189-190).

Logo, os dados digitais podem figurar tanto como o objeto da prova quanto como um instrumento para a obtenção da prova desejada.

Esses novos contornos da atividade probatória na persecução penal ampliam a capacidade das forças investigativas. Entretanto, o processo penal brasileiro por excelência é regido pelo princípio da legalidade, que demanda tanto a regulamentação, por lei, dos direitos exercitáveis durante o processo, como também a autorização e a regulamentação de qualquer intromissão na esfera dos direitos e liberdades dos cidadãos (Lima, 2022, p.82).

À vista disso, a ausência de parâmetros legais claros para a coleta de dados digitais no processo penal entra em tensão com o direito à autodeterminação informativa, caracterizada pelo elo entre proteção à privacidade e aos dados pessoais. Ademais, a ausência de parâmetros mínimos acarreta em autorizações judiciais frágeis que possibilitam impugnações sob a justificativa de medidas abusivas. (Saad, Costa Rossi, Partata, 2024).

Dessa maneira, a complexa realidade tecnológica, característica da sociedade em rede contemporânea, não pode ser adequadamente regulada pela aplicação analógica de diplomas legislativos concebidos em contextos tecnológicos

distintos, como a Lei das Interceptações Telefônicas (Lei nº 9.296/1996) e o Código de Processo Penal (Decreto-Lei nº 3.689/1941), mas evidencia a urgência de um regime jurídico específico para a produção de provas digitais. (Jezler Jr., 2019).

Nesse cenário de profundas transformações, surge a necessidade de equilibrar as garantias constitucionais do processo penal com as características próprias da prova digital, especialmente sua fragilidade, facilidade de cópia e potencial de invasão à privacidade (Oliveira, 2021). Portanto, para que a prova digital seja legítima no processo penal atual, é necessário construir um conjunto de normas que reconheça suas particularidades e estabeleça critérios claros para sua coleta, preservação e avaliação pelos juízes.

3. O RECURSO EXTRAORDINÁRIO 1301250 DO SUPREMO TRIBUNAL FEDERAL

O Recurso Extraordinário 1301250 do STF, que encontra-se ainda em julgamento, corresponde a um recurso interposto pelo Google Brasil Internet Ltda contra decisão do Superior Tribunal de Justiça (STJ) que manteve autorização judicial para quebra de sigilo do histórico de pesquisa de todas as pessoas que consultaram informações relacionadas a vereadora do Rio de Janeiro, Marielle Franco nos quatro dias anteriores ao seu assassinato, em 14 de março de 2018. A decisão permitiu a identificação de usuários por meio dos IPs em pesquisas relacionadas à agenda de trabalho da vereadora, endereços e suas informações pessoais (Brasil, 2024).

Posteriormente, com a manutenção da decisão pelo STJ, o Google impetrou recurso extraordinário no STF alegando que a quebra do sigilo da forma como foi autorizada afeta pessoas indeterminadas que não são parte no processo, além de afetar a privacidade e intimidade dos usuários.

Desse modo, a relevância do debate jurídico evidencia os novos contornos da produção probatória em tempos de vigilância digital. A tese jurídica que será firmada neste recurso será aplicada de forma vinculante a todos os casos futuros análogos, uma vez que não existe no Brasil uma legislação própria para o tema.

O Google, impetrante do recurso, conforme Zuboff (2020), foi o pioneiro na concepção e na prática do capitalismo de vigilância, por enfrentar poucos impedimentos jurídicos dos países no início do século XXI. Nesse cenário, as *big techs* conseguiram ampliar a coleta de informações com anúncios direcionados, moldando o mercado de comportamentos.

Nesse aspecto, a empresa aliada a outras do ramo de tecnologia digital foram pioneiras em desconsiderar normas sociais e anular direitos básicos associados à autonomia individual, os quais são essenciais para a própria possibilidade de uma sociedade democrática (Zuboff, 2020, p.27). Entretanto, o Google apesar de reiteradamente realizar práticas de vigilância digital, questiona se tais práticas são lícitas no ordenamento processual penal brasileiro.

O recurso fora acolhido por unanimidade e a Ministra Relatora, Rosa Weber, aposentada em 2023, apontou a linha tênue entre a quebra de sigilo e as garantias constitucionais, devendo toda autorização judicial basear-se na fundada suspeita específica dos alvos da obtenção de prova e na delimitação temporal (Brasil, 2024). Portanto, rejeitou a possibilidade de determinação judicial para a quebra de sigilo de pessoas não individualizadas, a fim de evitar decisões genéricas da quebra da privacidade de usuários inocentes.

Em contrapartida, o Ministro Alexandre de Moraes apresentou divergência e argumentou que os direitos fundamentais podem ser afastados em investigações criminais, desde que respeite critérios de razoabilidade, proporcionalidade e que sejam fundamentados em indícios de prática criminosa. Para o Ministro, a quebra de sigilo no caso em análise não mirou um número indiscriminado de pessoas, mas em

um grupo determinável de usuários que fizeram buscas específicas em um período de tempo. A relevância da medida para o andamento das investigações contou com o parecer favorável do Ministério Público e foi devidamente autorizada pelo Poder Judiciário (Brasil, 2024).

O julgamento ainda não se encerrou, restando votar a Ministra Cármen Lúcia e os ministros Edson Fachin, Dias Toffoli e Luiz Fux, o único que acompanhou o voto da relatora foi o Ministro André Mendonça (Brasil, 2025). Entretanto, muitos ministros têm feito pedidos de vistas considerando a relevância temática e sua repercussão na persecução penal.

O cenário de debates jurídicos incertos só existe, pois a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados), que ampla estrutura de proteção aos dados pessoais no Brasil, excluiu seus efeitos em se tratando de segurança pública, defesa nacional, segurança do Estado, atividades de investigação e repressão de infrações penais, pois orienta em seu artigo 4.º, § 1º que essas disposições serão regidas por legislação específica em conformidade com o devido processo legal (Brasil, 2018).

Nesse sentido, ainda não existe legislação própria para regular o tema e a carência de parâmetros legais mínimos e claros, como a definição dos crimes passíveis de tais medidas, sua gravidade, os prazos para a coleta probatória, o regime de registro e armazenamento de dados intensifica a insegurança jurídica. Essas lacunas refletem as consequências da dinâmica organizacional da sociedade contemporânea, marcada pela vigilância digital, cujos efeitos não se restringem à lógica do capitalismo e sua finalidade mercantil, mas também atingem o ordenamento jurídico brasileiro.

CONSIDERAÇÕES FINAIS

Portanto, observa-se que o capitalismo de vigilância transformou as relações privadas por meio dos mecanismos de controle social, bem como afetou a produção probatória no processo penal. A prova penal por meios digitais no processo penal brasileiro exige regime jurídico específico que supere a aplicação analógica de diplomas legislativos concebidos em contextos tecnológicos distintos.

Outrossim, o fenômeno da hipermassificação informativa e a ubiquidade dos dispositivos eletrônicos evidenciam a insuficiência das normas tradicionais para regular adequadamente a coleta, preservação e valoração de provas digitais, tornando imperativa a construção de marco regulatório que reconheça as particularidades desse novo tipo de evidência.

O Supremo Tribunal Federal, por meio do Recurso Extraordinário 1301250, tem buscado produzir jurisprudências que consigam pacificar o tema e trazer uma maior segurança jurídica para a população brasileira. Contudo, apenas isso não será suficiente, pois a temática impõe desafios que vão além da nova interpretação jurídica, demandando a criação de procedimentos específicos que representem a forma organizacional da sociedade digital e garantam, ao mesmo tempo, a eficiência da investigação criminal e o respeito aos direitos fundamentais.

Somente mediante regulamentação específica, capacitação dos operadores do direito e criação de procedimentos que garantam a cadeia de custódia digital que será possível harmonizar a eficiência investigativa com o garantismo penal. Assegura-se, assim, a proteção dos direitos fundamentais no novo contexto da produção probatória, aberto pela civilização da informação.

REFERÊNCIAS

BAUDRILLARD, Jean. **Tela total: mito-ironias do virtual e da imagem**. 3. ed. Porto Alegre: Sulina, 2003.



BISCHOFF, Paul. **Facial recognition technology (FRT): 100 countries analyzed**, 8 June 2021. Disponível em: <https://comparitech.com/blog/vpn--privacy/facial-recognition-statistics/#:~:text=Five%20countries>. Acesso em: 13 de agosto de 2025.

BRASIL. **Lei nº 9.296, de 24 de julho de 1996**. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Diário Oficial da União: seção 1, Brasília, DF, n. 143, p. 14753, 25 jul. 1996. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 10 nov. 2025.

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário n. 1.301.250**. Relatora: Ministra Rosa Weber. Julgamento iniciado em 09 jun. 2021 e prosseguido em sessões posteriores. Brasília, DF. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=5957252>. Acesso em: 15 nov. 2025.

BRASIL. Decreto-Lei nº 3.689, de 3 de outubro de 1941. **Código de Processo Penal**. Disponível em: <http://www.planalto.gov.br/CCIVIL/Decreto-Lei/Del3689.htm>. Acesso em: 10 nov. 2025.

BRASIL. Supremo Tribunal Federal. STF suspende julgamento sobre limites para quebra de sigilo de históricos de busca na internet. **Notícias STF**, 16 out. 2024. Disponível em: <https://noticias.stf.jus.br/postsnoticias/stf-suspende-julgamento-sobre-limites-para-quebra-de-sigilo-de-historicos-de-busca-na-internet/>. Acesso em: 20 nov. 2025.

BRASIL. Supremo Tribunal Federal. STF retoma julgamento sobre limites para quebra de sigilo de buscas na internet. **Notícias STF**, 24 set. 2025. Disponível em: <https://noticias.stf.jus.br/postsnoticias/stf-retoma-julgamento-sobre-limites-para-quebra-de-sigilo-de-buscas-na-internet/>. Acesso em: 20 nov. 2025.

BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União: Brasília, 15 ago. 2018. Disponível em:



https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 20 nov. 2025.

BRUNO, Fernanda. Monitoramento, classificação e controle nos dispositivos de vigilância digital. In: ANTOUN, Henrique (Org.). **Web 2.0: participação e vigilância na era da comunicação distribuída**. Rio de Janeiro: Mauad X, 2008. p. 167-182.

DAL CASTEL, Mauricio. GONÇALVES, Vanessa Chiari. O Controle Social na Era do Capitalismo Digital: Vigilância privada e pública, e seus custos ambientais. **Revista Justiça do Direito**, [S. l.], v. 38, n. 3, p. 162-181, 2025. DOI: 10.5335/rjd.v38i3.15278. Disponível em: <https://ojs.upf.br/index.php/rjd/article/view/15278>. Acesso em: 12 nov. 2025.

EILBERG, Daniela Dora. Fluxo de Dados, Prova e Processo Penal. **Revista da Faculdade Mineira de Direito - PUC Minas**, v. 27 n. 54, 2024. DOI: <https://doi.org/10.5752/P.2318-7999.2024v27n54p29-54>. Disponível em: <https://periodicos.pucminas.br/Direito/article/view/34785>. Acesso em: 08 nov. 2025

FOUCAULT, Michel. **Vigiar e punir: nascimento da prisão**. 14. ed. Petrópolis: Vozes, 1996.

HAN, Byung-Chul. **Infocracia: Digitalização e a crise da democracia**. Tradução de Gabriel S. Philipson. Petrópolis, RJ: Vozes, 2022.

JEZLER JR., Ivan. Prova Penal Digital: tempo, risco e busca telemática. Florianópolis: **Tirant Lo Blanch**, 2019.

LIMA, Renato Brasileiro de. **Manual de processo penal**: volume único / Renato Brasileiro de Lima - 11. ed. rev., ampl. e atual. - São Paulo: Ed. JusPodivm, 2022.

OLIVEIRA, Cássio Roberto Uruga. **A (in)constitucionalidade da prova penal obtida com violação da privacidade nos meios digitais** : uma análise sobre os dados de comunicação em aplicativos de mensagens instantâneas. Monografia (graduação em Direito) – Departamento em Direito, Centro de Ciências Sociais Aplicadas, Universidade Federal de Sergipe, São Cristóvão, SE, 2021. Disponível em: <https://ri.ufs.br/jspui/handle/riufs/15186>. Acesso em: 12 nov. 2025.

SAAD, Marta; COSTA ROSSI, Helena; PARTATA, Pedro Henrique. A obtenção das provas digitais no processo penal demanda uma disciplina jurídica própria? Uma análise do conceito, das características e das peculiaridades das provas digitais.



Revista Brasileira de Direito Processual Penal, [S. l.], v. 10, n. 3, 2024. DOI:
10.22197/rbdpp.v10i3.1071. Disponível em:
<https://revista.ibraspp.com.br/RBDPP/article/view/1071>. Acesso em: 16 nov. 2025.

SILVA, Germano Marques da. **Curso de processo penal** – vol. 2. 2. ed. Lisboa:
Verbo, 1999, p. 189-190.

VIRILIO, Paul. **A bomba informática**. São Paulo: Estação Liberdade, 1999.

ZUBOFF, Shoshana. **A Era do Capitalismo de Vigilância**: A Luta por um Futuro Humano na Nova Fronteira do Poder. Tradução de George Schlesinger. 1. ed. Rio de Janeiro, RJ: Intrínseca, 2020.