



PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO
ARTIGO CIENTÍFICO

A CIBERSEGURANÇA NA ADVOCACIA:
ENTRE A INVESTIGAÇÃO LÍCITA E A PRÁTICA DE PERSEGUIÇÃO
CONTINUADA (*STALKING*) NA COLETA DE DADOS

ORIENTANDO: ERICK FREITAS AGUIAR
ORIENTADOR: PROF. ME. LUIZ PAULO BARBOSA DA CONCEIÇÃO

GOIÂNIA-GO
2026

ERICK FREITAS AGUIAR

A CIBERSEGURANÇA NA ADVOCACIA:
ENTRE A INVESTIGAÇÃO LÍCITA E A PRÁTICA DE PERSEGUIÇÃO
CONTINUADA (*STALKING*) NA COLETA DE DADOS

Artigo Científico apresentado à disciplina
de Trabalho de Curso II, da Escola de
Direito, Negócios e Comunicação da
Pontifícia Universidade Católica de Goiás.
Prof. Orientador: Me. Luiz Paulo Barbosa
da Conceição.

ERICK FREITAS AGUIAR

A CIBERSEGURANÇA NA ADVOCACIA:
ENTRE A INVESTIGAÇÃO LÍCITA E A PRÁTICA DE PERSEGUIÇÃO
CONTINUADA (*STALKING*) NA COLETA DE DADOS

Data da Defesa: ____ de _____ de 2026.

BANCA EXAMINADORA

Orientador: Prof. Me. Luiz Paulo Barbosa da Conceição

Nota

Examinador Convidado: Prof. Me. Júlio Anderson Alves Bueno

Nota

Agradecimentos

É com enorme satisfação, que concluo este trabalho com o apoio de pessoas tão queridas que demonstraram e incentivaram a minha trajetória acadêmica. Trabalho este, que com certeza impactou nas minhas escolhas e caminho a ser tomado na minha vida profissional. Agradeço aos bons profissionais da saúde, que me deram estrutura para conciliar minhas atividades.

Não posso deixar de mencionar dois nomes também, que foram fundamentais para que eu continuasse enfrentando as adversidades do dia-a-dia. A Jessyca Aguiar, minha querida irmã, que me apoiou desde o primeiro momento, sempre me reforçando positivamente para que não cedesse ao cansaço. E Luiza Moura, minha revisora principal, parceira, mulher de inteligência singular que me auxiliou enquanto também redigia sua própria pesquisa. Sem vocês, não haveria ganhos, grato pela jornada.

SUMÁRIO

RESUMO.....	5
ABSTRACT.....	6
INTRODUÇÃO	7
1. A CIBERSEGURANÇA E A ADVOCACIA CONTEMPORÂNEA.....	8
1.1 DA DATIFICAÇÃO DA SOCIEDADE	9
1.2 O CONCEITO E OS FUNDAMENTOS DA CIBERSEGURANÇA	11
1.3 O DEVER DE SIGILO E A PROTEÇÃO DA INFORMAÇÃO JURÍDICA	12
1.4 A LEI GERAL DE PROTEÇÃO DE DADOS E SUA APLICAÇÃO NA ADVOCACIA	13
2. O STALKING DIGITAL E A PROTEÇÃO DA PRIVACIDADE NO AMBIENTE VIRTUAL	17
2.1 O STALKING DIGITAL E OS ELEMENTOS JURÍDICOS DA PERSEGUIÇÃO ONLINE.....	19
2.2 A COLETA INDEVIDA DE DADOS E OS LIMITES ÉTICOS DA INVESTIGAÇÃO	20
2.3 A RELAÇÃO ENTRE STALKING DIGITAL, CIBERSEGURANÇA E A PRÁTICA ADVOCATÍCIA.....	21
2.4 O CYBERSTALKING COMO EXPRESSÃO DIGITAL DO CRIME DE PERSEGUIÇÃO	22
3. OS LIMITES ENTRE INVESTIGAÇÃO LÍCITA E PERSEGUIÇÃO ILÍCITA NA ERA DIGITAL	24
3.1 A INVESTIGAÇÃO DEFENSIVA E O USO DE DADOS E TECNOLOGIAS.....	25
3.1.1 OS LIMITES JURÍDICOS DA COLETA DE DADOS E A VEDAÇÃO À <i>FISHING EXPEDITION</i>	26
3.1.2 A PROTEÇÃO DA PRIVACIDADE E DOS DIREITOS FUNDAMENTAIS NA INVESTIGAÇÃO.....	27
3.2 A RESPONSABILIDADE DO ADVOGADO E OS RISCOS DE VIOLAÇÃO DE DIREITOS	29
3.3 A ÉTICA PROFISSIONAL, A CIBERSEGURANÇA E A CONFIANÇA SOCIAL NA ADVOCACIA	29
CONCLUSÃO	31
REFERÊNCIAS	33

**A CIBERSEGURANÇA NA ADVOCACIA:
ENTRE A INVESTIGAÇÃO LÍCITA E A PRÁTICA DE PERSEGUIÇÃO
CONTINUADA (STALKING) NA COLETA DE DADOS**

Erick Freitas Aguiar

RESUMO

O presente artigo analisou a interseção entre cibersegurança, proteção de dados e prática advocatícia, tendo como problema central a identificação dos critérios jurídicos e éticos que distinguem a investigação autônoma legítima do advogado da perseguição digital ilícita. A pesquisa adotou método hipotético-dedutivo, com abordagem qualitativa e técnica bibliográfico-documental, apoiando-se em doutrina especializada, legislação vigente e jurisprudência dos Tribunais Superiores. Verificou-se que a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) impõe ao advogado, como agente de tratamento de dados, deveres de segurança, transparência e finalidade, cuja inobservância pode acarretar responsabilidade civil objetiva. Constatou-se, ainda, que a Lei nº 14.132/2021, ao tipificar o crime de perseguição no art. 147-A do Código Penal, alcança as modalidades digitais de stalking, inclusive aquelas praticadas no contexto de investigações advocatícias. Concluiu-se que a investigação defensiva regulamentada pelo Provimento OAB nº 188/2018 é legítima quando observados os princípios da necessidade, proporcionalidade e finalidade, convertendo-se em ilícito penal, civil e disciplinar quando instrumentalizada para fins persecutórios. A cibersegurança, portanto, não é acessório técnico, mas componente ético-jurídico estruturante da advocacia contemporânea

Palavras-chave: cibersegurança; advocacia; Lei Geral de Proteção de Dados; stalking digital; investigação defensiva.

***CYBERSECURITY IN LEGAL PRACTICE: BETWEEN LAWFUL INVESTIGATION
AND DIGITAL STALKING IN DATA COLLECTION***

Erick Freitas Aguiar

ABSTRACT

This article analyzed the intersection between cybersecurity, data protection, and legal practice, focusing on the legal and ethical criteria that distinguish legitimate autonomous investigation by lawyers from unlawful digital stalking. The research adopted a hypothetical-deductive method with a qualitative approach and bibliographic-documentary technique, drawing on specialized doctrine, current legislation, and case law from the Superior Courts. It was found that the General Data Protection Law (Law No. 13,709/2018) imposes on lawyers, as data controllers, duties of security, transparency, and purpose, the non-compliance with which may result in strict civil liability. It was also verified that Law No. 14,132/2021, by criminalizing the offense of stalking in Art. 147-A of the Penal Code, covers digital modalities of stalking, including those practiced in the context of legal investigations. It was concluded that defensive investigation regulated by OAB Provision No. 188/2018 is legitimate when the principles of necessity, proportionality, and purpose are observed, becoming a criminal, civil, and disciplinary offense when instrumentalized for persecutory purposes. Cybersecurity, therefore, is not a technical accessory, but an ethical-legal structural component of contemporary legal practice.

Keywords: cybersecurity; legal practice; General Data Protection Law; digital stalking; defensive investigation.

INTRODUÇÃO

A transformação digital das últimas décadas reconfigurou profundamente a forma como a advocacia é exercida no Brasil. Escritórios jurídicos tornaram-se centros de processamento de dados sensíveis, custodiando informações que transitam entre segredos industriais, estratégias processuais e dados pessoais de clientes. Nesse cenário, a proteção dessas informações deixou de ser questão meramente técnica para se tornar uma dimensão ética, jurídica e constitucional incontornável da prática profissional.

A sociedade da informação, caracterizada pela datificação massiva das relações sociais e pela circulação contínua de dados, criou um paradoxo inerente à advocacia contemporânea. Ao mesmo tempo em que o advogado dispõe de ferramentas digitais cada vez mais sofisticadas para investigar, reunir provas e defender seus clientes, ele também se vê exposto a riscos inéditos. Tais riscos incluem a possibilidade de ser vítima de ataques cibernéticos, de violar inadvertidamente direitos fundamentais de terceiros ou, em casos mais graves, de transitar da diligência legítima para a perseguição ilícita.

É justamente nesse limiar que se situa o problema central deste artigo: quais critérios jurídicos e éticos permitem distinguir a investigação autônoma realizada por escritórios de advocacia como diligência legítima no exercício da defesa técnica, e em que circunstâncias tal prática se converte em violação à Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e à Lei de Perseguição (Lei nº 14.132/2021)?

A relevância do tema é inequívoca. A promulgação da Lei Geral de Proteção de Dados (LGPD) impôs ao advogado a condição de agente de tratamento de dados, sujeito a deveres de segurança, transparência e finalidade. Paralelamente, a Lei nº 14.132/2021 tipificou o crime de perseguição no art. 147-A do Código Penal, estendendo sua incidência às modalidades digitais. A conjugação dessas normas com o Provimento OAB nº 188/2018, que regulamentou a investigação defensiva autônoma, criou um campo normativo complexo que ainda é insuficientemente explorado pela doutrina.

O objetivo geral deste trabalho é analisar as práticas de investigação autônoma realizadas por escritórios de advocacia, identificando quando essas

condutas configuram diligências legítimas e quando se aproximam da perseguição digital e da coleta clandestina de dados. Os objetivos específicos compreendem os seguintes pontos: mapear os principais meios de obtenção de dados utilizados na investigação advocatícia e sua compatibilidade com o ordenamento jurídico; diferenciar os limites impostos pela LGPD e pela Lei de Perseguição em relação à investigação autônoma; e propor parâmetros jurídicos e éticos para a aferição da licitude das informações obtidas.

A pesquisa adotou o método hipotético-dedutivo, com abordagem qualitativa e técnica bibliográfico-documental. Foram consultadas obras doutrinárias especializadas em direito digital e proteção de dados, com destaque para os trabalhos de Danilo Doneda e Laura Schertel Mendes. Além disso, a fundamentação baseou-se na legislação nacional vigente, nas normas éticas da Ordem dos Advogados do Brasil (OAB) e na jurisprudência do Superior Tribunal de Justiça e do Supremo Tribunal Federal.

O artigo está estruturado em três seções. Na primeira, examina-se a cibersegurança e a advocacia contemporânea, abordando seus fundamentos conceituais, o dever de sigilo profissional e a aplicação da LGPD ao exercício da advocacia. Na segunda seção, analisa-se o *stalking* digital e a proteção da privacidade no ambiente virtual, com destaque para a tipificação do art. 147-A do Código Penal e os limites éticos da investigação advocatícia. A terceira seção integra as análises anteriores para tratar da responsabilidade do advogado na advocacia contemporânea, examinando a investigação autônoma, o desvio da função investigativa, a caracterização do *stalking* jurídico e as implicações éticas e disciplinares decorrentes.

1 A CIBERSEGURANÇA E A ADVOCACIA CONTEMPORÂNEA

A informatização dos processos e a digitalização dos fluxos informacionais transformaram os escritórios de advocacia em núcleos estratégicos de tratamento de dados sensíveis, exigindo do advogado atuação técnica e preventiva na proteção dessas informações.

A literatura especializada aponta que, na sociedade da informação, a crescente "datificação" das relações sociais transformou os dados pessoais e profissionais em insumos centrais da economia digital, permitindo que interações

sejam constantemente monitoradas, processadas e armazenadas. Conforme Doneda (2021, p. 16), esse processo alterou estruturalmente a forma como as pessoas se relacionam com as instituições, tornando o dado pessoal uma moeda de poder. Ambientes que concentram informações estratégicas, como a advocacia, tornam-se particularmente sensíveis à exploração indevida desses dados, inserindo-se na lógica da chamada sociedade da vigilância, caracterizada por mecanismos de monitoramento muitas vezes invisíveis ao próprio indivíduo (Doneda, 2021, p. 18).

Esse cenário ampliou a dependência de sistemas digitais e, simultaneamente, a exposição a riscos decorrentes da circulação massiva de informações. Falhas na segurança de dados permitem a coleta, o rastreamento e a utilização indevida de informações pessoais, transformando o rastro digital em instrumento de violação de direitos (Greco, 2024, p. 12). Nesse contexto, a cibersegurança deixa de ser compreendida como mero conjunto de ferramentas tecnológicas voltadas para proteção, e ganha contornos mais profundos, ao se apresentar como dimensão ética, jurídica e técnica indispensável. Para Doneda (2021, p. 150), a proteção de dados consolida-se como mecanismo de garantia da dignidade humana e das liberdades fundamentais na era digital.

A proteção da informação relaciona-se diretamente com a preservação do sigilo profissional, com a segurança das comunicações e com a própria credibilidade da Justiça, sobretudo porque a LGPD impõe a necessidade de adoção de medidas que assegurem a inviolabilidade da vida privada e previnam acessos não autorizados a dados sensíveis (Mendes, 2014, p. 175). Assim, a integração entre segurança informacional e atividade jurídica torna-se imperativa, evidenciando que a advocacia contemporânea opera em um ambiente no qual a proteção digital é parte estruturante da função social do advogado.

1.1 DA DATIFICAÇÃO DA SOCIEDADE

A transformação digital das últimas décadas deu origem ao fenômeno da datificação, compreendido como a conversão de aspectos da vida social em dados quantificáveis e passíveis de tratamento automatizado. Trata-se de um processo estruturante da sociedade contemporânea, no qual comportamentos, interações e relações humanas passam a ser traduzidos em informações digitais suscetíveis de

coleta, armazenamento e análise sistemática (Mayer-Schönberger; Cukier, 2013, p. 30).

Nesse sentido, a datificação não se limita à digitalização de informações previamente existentes, mas implica uma reconfiguração profunda da forma como a realidade social é compreendida e explorada. Ao permitir o monitoramento contínuo e a análise preditiva, os dados passam a desempenhar papel central na organização das relações sociais, econômicas e institucionais, influenciando processos decisórios em múltiplas esferas (Mayer-Schönberger; Cukier, 2013, p. 30).

A doutrina contemporânea destaca que esse fenômeno foi consolidado com o advento das plataformas digitais e das redes sociais, responsáveis por transformar atividades humanas antes intangíveis, como emoções, vínculos sociais e preferências individuais, em dados estruturados e mensuráveis. Conforme leciona José van Dijck, a datificação constitui um novo paradigma científico e social, marcado pela crescente confiança na capacidade de quantificação do comportamento humano por meio de tecnologias digitais (Van Dijck, 2014, p. 198).

Ainda segundo a autora, a datificação tornou-se um princípio central tanto na academia quanto no mercado, sendo utilizada como ferramenta para compreender, prever e influenciar comportamentos individuais e coletivos. Esse movimento está diretamente relacionado ao desenvolvimento do chamado dataísmo, que atribui aos dados um estatuto de verdade objetiva e legitima sua utilização como base para decisões econômicas, políticas e jurídicas (Van Dijck, 2014, p. 199).

No contexto da sociedade informacional, a datificação também implica uma mudança estrutural na lógica econômica, na medida em que os dados passam a ser tratados como ativos estratégicos de elevado valor. Organizações públicas e privadas exploram grandes volumes de dados para fins de vigilância, personalização de serviços e tomada de decisões automatizadas, consolidando um modelo baseado na extração e monetização de informações pessoais (Van Dijck, 2014, p. 200).

Essa realidade apresenta implicações diretas no campo jurídico, especialmente no que se refere à proteção de dados pessoais e ao sigilo profissional. No âmbito da advocacia, a intensificação da datificação amplia significativamente o volume de informações sensíveis sob guarda dos profissionais, exigindo não apenas um dever passivo de confidencialidade, mas também uma atuação ativa na proteção e segurança desses dados (Doneda, 2021, p. 45).

Como destaca a doutrina nacional, a proteção de dados pessoais surge justamente como resposta à intensificação da coleta e tratamento de informações no ambiente digital, impondo limites ao uso desses dados e garantindo a tutela dos direitos fundamentais da personalidade diante da expansão das tecnologias informacionais (Doneda, 2021, p. 46).

Dessa forma, a datificação deve ser compreendida como fenômeno central para a análise das transformações jurídicas atuais, pois redefine não apenas a forma de produção e circulação de informações, mas também os próprios contornos dos direitos fundamentais à privacidade, à intimidade e à proteção de dados, exigindo respostas normativas e éticas compatíveis com os riscos inerentes à sociedade digital (Mayer-Schönberger; Cukier, 2013, p. 30).

1.2 O CONCEITO E OS FUNDAMENTOS DA CIBERSEGURANÇA

O termo "cibersegurança" possui origem etimológica na junção do prefixo "*ciber*", derivado do grego *kybernetes* e utilizado por Norbert Wiener na teoria da cibernética em 1948, com o substantivo "segurança", oriundo do latim *securitas*. Sua consolidação na língua portuguesa foi formalizada com a inclusão do vocábulo na 6ª edição do Vocabulário Ortográfico da Língua Portuguesa, legitimando seu uso técnico para designar práticas e políticas voltadas à proteção de sistemas, redes e dados (Academia Brasileira de Letras, 2021). Dicionários especializados descrevem a cibersegurança como o campo dedicado à defesa de infraestruturas informáticas contra acessos indevidos, danos e ataques, evidenciando sua dimensão tecnológica, jurídica e ética (Infopédia, 2021; Priberam, 2021).

A cibersegurança, embora estruturada a partir dos pilares da confidencialidade, integridade e disponibilidade, ultrapassa a dimensão meramente técnica para assumir papel central na tutela de direitos fundamentais no ambiente digital. Para Doneda (2021, p. 25), a proteção de dados pessoais funciona como instrumento de garantia da dignidade humana e da autonomia informacional, exigindo que o tratamento de informações seja pautado por critérios de finalidade, segurança e transparência. Em uma sociedade marcada pela vigilância e pela circulação massiva de dados, Doneda (2021, p. 102) observa que a concentração de informações sensíveis em setores como a advocacia intensifica a necessidade de mecanismos

robustos de proteção, uma vez que a fragilidade na segurança informacional pode permitir o acesso indevido, a manipulação e o uso abusivo de dados, comprometendo não apenas interesses privados, mas também a própria efetividade da proteção jurídica, ponto reforçado por Mendes (2014, p. 175) ao tratar do direito fundamental à proteção de dados.

Essa estrutura conceitual encontra respaldo no arcabouço constitucional e profissional. A Constituição Federal de 1988 consagra a inviolabilidade da vida privada e o direito à reparação por danos decorrentes de sua transgressão, conforme o art. 5º, X, do texto constitucional¹ (Brasil, 1988). A legislação própria da advocacia complementa essa proteção ao estabelecer a inviolabilidade do escritório, dos instrumentos de trabalho e dos meios de comunicação do advogado, nos termos do art. 7º, II, da Lei nº 8.906/1994². O Código de Ética e Disciplina da OAB reforça, ainda, que o sigilo profissional constitui dever fundamental, cuja violação configura infração ética.³

Verifica-se, portanto, que a cibersegurança integra a ética, a governança informacional e os direitos fundamentais, constituindo obrigação técnica e jurídica indispensável à preservação do sigilo, da confiança e da integridade da atividade advocatícia. A omissão nessa área não configura mera negligência gerencial, mas representa, em rigor, descumprimento de dever profissional com potenciais repercussões disciplinares e civis.

1.3 O DEVER DE SIGILO E A PROTEÇÃO DA INFORMAÇÃO JURÍDICA

O sigilo profissional é elemento estruturante da advocacia e constitui garantia institucional da Justiça. Seu cumprimento assegura que o cliente possa revelar fatos, estratégias e informações sensíveis sem receio de exposição ou retaliação,

¹ Art. 5º, X, da Constituição Federal de 1988: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação."

² Art. 7º, II, da Lei nº 8.906/1994: "São direitos do advogado: II – a inviolabilidade de seu escritório ou local de trabalho, bem como de seus instrumentos de trabalho, de sua correspondência escrita, eletrônica, telefônica e telemática, desde que relativas ao exercício da advocacia."

³ Art. 25 do Código de Ética e Disciplina da OAB: "O sigilo profissional é inerente à profissão, impondo-se ao advogado como dever fundamental, cuja violação constitui infração ética, ressalvadas apenas hipóteses excepcionais de grave ameaça à vida ou à honra."

preservando a relação de confiança que sustenta o exercício da defesa. Conforme Oliveira (2022), a violação do sigilo compromete não apenas a esfera individual, mas a própria legitimidade do processo, uma vez que fragiliza a ampla defesa e o contraditório. No ambiente digital, o sigilo exige a adoção de mecanismos tecnológicos que impeçam acessos indevidos e preservem a integridade das comunicações.

Com o aumento da circulação e do valor estratégico das informações no ambiente digital, a proteção do sigilo profissional passou a exigir medidas contínuas de segurança da informação. Nesse cenário, Doneda (2021, p. 102) destaca que mecanismos como controle de acessos, autenticação e práticas de proteção tecnológica tornam-se essenciais para mitigar os riscos inerentes à sociedade da informação, marcada pela constante coleta e processamento de dados. A ausência dessas medidas potencializa vulnerabilidades estruturais e pode resultar na exposição indevida de informações, comprometendo diretamente a proteção da privacidade e a autonomia do titular dos dados (Mendes, 2014, p. 175).

Importa ressaltar que a proteção da informação jurídica não é somente um imperativo ético, é igualmente uma exigência jurídica que se manifesta em múltiplos diplomas normativos. A integração entre ética profissional, proteção tecnológica e governança informacional consolida-se, assim, como dever cujo descumprimento gera repercussões éticas, disciplinares e jurídicas para o advogado.

1.4 A LEI GERAL DE PROTEÇÃO DE DADOS E SUA APLICAÇÃO NA ADVOCACIA

A Lei Geral de Proteção de Dados Pessoais representou uma inflexão paradigmática no ordenamento jurídico brasileiro ao deslocar a proteção da informação de uma lógica meramente patrimonial para uma dimensão vinculada aos direitos fundamentais da personalidade. A partir da promulgação da Lei nº 13.709/2018, o tratamento de dados pessoais passou a ser estruturado por princípios como finalidade, adequação, necessidade, transparência e segurança, impondo aos agentes de tratamento o dever de atuar de forma diligente na proteção das informações sob sua responsabilidade (Brasil, 2018).

No âmbito da advocacia, a incidência da LGPD revela-se particularmente sensível, na medida em que o advogado atua como agente de tratamento ao coletar, armazenar, acessar e utilizar dados pessoais de clientes e de terceiros no exercício

da atividade profissional. Conforme destacam Guariento e Martins, o profissional da advocacia não apenas manipula dados, mas o faz em contextos de elevada sensibilidade informacional, o que intensifica seu dever de cuidado e reforça a necessidade de observância rigorosa dos princípios legais que regem o tratamento de dados (Guariento; Martins, 2021, p. 120).

A aplicação da LGPD à advocacia impõe, ainda, a adoção de medidas técnicas e administrativas aptas a prevenir acessos não autorizados, vazamentos e usos indevidos das informações, nos termos do art. 46 da referida lei (Brasil, 2018). Nesse sentido, a proteção de dados deixa de ser compreendida como obrigação acessória e passa a constituir elemento estruturante da atuação profissional, integrando o próprio conteúdo do dever de sigilo. Para Doneda, a proteção de dados pessoais assume função central na garantia da dignidade humana, exigindo que o tratamento informacional seja realizado de forma segura, proporcional e orientada por finalidades legítimas (Doneda, 2021, p. 150).

A inobservância dessas diretrizes pode gerar consequências jurídicas relevantes, uma vez que a LGPD estabelece regime de responsabilização dos agentes de tratamento por danos causados em decorrência do tratamento irregular de dados. O art. 42 da lei prevê que o controlador ou operador que causar dano patrimonial, moral, individual ou coletivo em violação à legislação de proteção de dados é obrigado a repará-lo, o que evidencia a relevância da adoção de medidas preventivas eficazes no âmbito da advocacia (Brasil, 2018).

Além disso, a atuação do advogado no ambiente digital exige a harmonização entre o dever de proteção de dados e as prerrogativas profissionais asseguradas pelo Estatuto da Advocacia. O exercício da defesa técnica não autoriza a coleta indiscriminada de informações nem a utilização de meios ilícitos ou abusivos para obtenção de dados, sendo imprescindível que a atuação profissional observe os limites impostos pela legalidade, pela ética e pela proteção da privacidade. Como observa Mendes, o direito fundamental à proteção de dados impõe ao intérprete a necessidade de equilibrar o fluxo informacional com a tutela da autonomia individual, evitando que a utilização de tecnologias resulte em violações indevidas de direitos da personalidade (Mendes, 2014, p. 175).

Nesse contexto, a análise da licitude das provas obtidas por meio de dados pessoais exige a verificação da conformidade do procedimento adotado com os

princípios da LGPD e com o ordenamento jurídico como um todo. A obtenção de informações deve estar vinculada a uma finalidade legítima, ser realizada de forma proporcional e respeitar os limites impostos à atuação privada, sob pena de invalidação da prova e responsabilização do agente. A partir dessa perspectiva, torna-se fundamental examinar a forma como a jurisprudência tem enfrentado a utilização de dados pessoais no contexto de litígios, especialmente no que se refere à validade das provas e à eventual violação de direitos fundamentais (Brasil, 2018).

Colacionam-se, a seguir, dois precedentes do Tribunal de Justiça de São Paulo que corroboram o entendimento doutrinário exposto:

AGRAVO DE INSTRUMENTO - AÇÃO DE EXECUÇÃO DE TÍTULO EXTRAJUDICIAL - Insurgência do executado contra decisão que determinou expedição de ofício e ensejou em consequente juntada de contrato de locação aos autos de origem - PRESCRIÇÃO INTERCORRENTE - Inadmissibilidade - Artigo 932, inciso III, do Código de Processo Civil - Inexistência de análise na decisão recorrida, pelo juiz natural da causa, da pretensão posta em sede recursal - Dialeticidade - Questão que já fora analisada em momento anterior na origem, mas cujo prazo para interposição de recurso transcorreu in albis - Impossibilidade de enfrentamento nesta sede recursal, mesmo em se tratando de questão de ordem pública - Vedação legal - NULIDADE DE PROVA OBTIDA E DESENTRANHAMENTO - Descabimento - Não restou comprovada a violação aos arts. 6º e 7º, da LGPD, e aos arts. 20 e 21, do Código de Ética e Disciplina da OAB, uma vez que não há comprovação de que as diligências realizadas pela parte exequente são decorrentes de obtenção de informações por meio ilícito e antiético - Expedição de ofício que foi determinada pelo Juízo de Primeiro Grau justamente para aferir a situação de residência do executado e possibilidade de penhora de bens - RECURSO NÃO CONHECIDO, em parte, e, na parte conhecida, NÃO PROVIDO. (TJ-SP - Agravo de Instrumento: 23275014520258260000 Avaré, Relator: LAVINIO DONIZETTI PASCHOALÃO, Data de Julgamento: 16/10/2025, 38ª Câmara de Direito Privado, Data de Publicação: 16/10/2025)

APELAÇÃO CÍVEL. RESPONSABILIDADE CIVIL. AÇÃO DE INDENIZAÇÃO POR DANOS MORAIS. VIOLAÇÃO DE SIGILO PROFISSIONAL. PATROCÍNIO DE AÇÃO CONTRA EX-CLIENTE. SENTENÇA DE IMPROCEDÊNCIA. INCONFORMISMO DA AUTORA. DESACOLHIMENTO. Alegação de cerceamento de defesa em razão do indeferimento da prova testemunhal. Inocorrência. Suposta violação de sigilo profissional e da LGPD. Inexistência. Atuação do advogado contra ex-cliente. Possibilidade desde que preservadas informações confidenciais e ausente conexão entre as demandas. Art. 19 do Código de Ética e Disciplina da OAB. Informações utilizadas pelo advogado. Cópia de Requisição de pequeno valor. Natureza pública. Consulta acessível a qualquer interessado. Pesquisa realizada nos limites da defesa de novo cliente. Interesse pela demonstração da capacidade econômica da autora para adimplir com os aluguéis pretendidos em ação promovida pelo ex-marido. Inexistência de conduta ilícita. Ausência de identidade das ações ou prejuízo a autora. Ação de imissão na posse e cobrança de aluguéis. Imóvel de copropriedade das partes, utilizado exclusivamente pela apelante. Situação sem relação com benefício assistencial discutido em demanda anterior. Sentença mantida. Recurso a que se NEGA PROVIMENTO. (TJ-SP - Apelação Cível:

10078044820248260038 Araras, Relator: Fatima Cristina Ruppert Mazzo, Data de Julgamento: 30/09/2025, 4ª Câmara de Direito Privado, Data de Publicação: 30/09/2025)

A Lei Geral de Proteção de Dados (Lei nº 13.709/2018) alterou profundamente o regime jurídico de tratamento da informação no Brasil ao instituir princípios, bases legais e obrigações de segurança aplicáveis aos diversos setores, incluindo a advocacia. Ao qualificar advogados e escritórios como agentes de tratamento, a LGPD impõe ao profissional deveres de prevenção, transparência e adoção de medidas técnicas e administrativas que assegurem a proteção dos dados pessoais sob sua responsabilidade (Guariento; Martins, 2021, p. 120). A negligência no cumprimento dessas obrigações pode acarretar sanções relevantes e comprometer o sigilo profissional.

A LGPD estabelece que a proteção de dados deve ocorrer por meio de mecanismos aptos a evitar acessos não autorizados, perdas, alterações ou difusões indevidas. O art. 46 da lei determina que os agentes de tratamento adotem medidas de segurança técnicas e administrativas para proteção dos dados pessoais⁴. Essa exigência desloca a proteção da informação de uma postura meramente ética para um modelo de segurança ativa e auditável, que demanda políticas internas, revisão de fluxos informacionais e padronização de práticas de segurança (Mattos Filho, 2024). Verifica-se que o advogado que trata dados pessoais sem adotar essas medidas não apenas descumpre a lei, viola também o seu dever ético de proteção ao cliente.

O Marco Civil da Internet (Lei nº 12.965/2014) complementa esse arcabouço ao proteger a inviolabilidade das comunicações e a privacidade dos usuários, reforçando que a segurança das interações eletrônicas é extensão direta do sigilo profissional. A inviolabilidade e o sigilo das comunicações por internet, ressalvada a ordem judicial⁵, formam, em conjunto com as demais proteções da LGPD e do

⁴ Art. 46 da Lei nº 13.709/2018 (LGPD): "Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas, de destruição, perda, alteração, comunicação ou difusão."

⁵ Art. 7º, I e III, da Lei nº 12.965/2014 (Marco Civil da Internet): "O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: I – a inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; [...] III – a inviolabilidade e sigilo de suas comunicações pela internet, salvo por ordem judicial."

Estatuto da Advocacia, um sistema normativo coeso que posiciona o advogado imperativamente como agente de segurança.

Verifica-se, assim, que a LGPD representou mudança estrutural na advocacia, que passa a atuar em ambiente regulatório orientado à prevenção, transparência e responsabilidade no tratamento das informações. Escritórios que não internalizarem essa cultura de conformidade com a proteção de dados incorrerão em riscos crescentes, tanto no plano disciplinar quanto no plano da responsabilidade civil objetiva (Mendes, 2014, p. 175).

2 O STALKING DIGITAL E A PROTEÇÃO DA PRIVACIDADE NO AMBIENTE VIRTUAL

A consolidação da sociedade digital ampliou significativamente a capacidade de vigilância e monitoramento de indivíduos, possibilitando a coleta contínua de dados pessoais e a identificação de padrões comportamentais com elevado grau de precisão. Segundo Doneda (2021, p. 18), a chamada sociedade da vigilância é marcada pela constante captação e processamento de informações por meio de tecnologias digitais, revelando um cenário em que o fluxo informacional se torna elemento central das relações sociais e jurídicas, alterando as condições de exercício da autonomia individual.

A interconexão entre redes sociais, aplicativos e bases de dados permite o acompanhamento de rotinas e interações de forma silenciosa e persistente, muitas vezes sem a plena consciência do titular das informações. Esse contexto potencializa riscos à privacidade e à autonomia individual, na medida em que a circulação massiva de dados fragiliza o controle sobre o uso das informações pessoais, exigindo respostas jurídicas adequadas à proteção de direitos fundamentais (Mendes, 2014, p. 175).

A perseguição continuada, especialmente no ambiente digital, configura-se pela reiteração de condutas que invadem a esfera privada do indivíduo e comprometem sua tranquilidade e liberdade. Trata-se de comportamento que pode se manifestar por meio de insistência comunicacional, monitoramento constante de perfis, utilização de perfis falsos e coleta indevida de dados pessoais, práticas que

evidenciam a intensificação da violência psicossocial no ciberespaço (Greco, 2024, p. 12).

A doutrina penal reconhece que o crime de perseguição exige habitualidade e repetição de atos que causem perturbação à vítima, sendo o ambiente digital um fator de amplificação dessas condutas (Nucci, 2024, p. 615).

A criminalização da perseguição foi consolidada no ordenamento jurídico brasileiro com a promulgação da Lei nº 14.132/2021, que inseriu o art. 147-A no Código Penal. Ao estabelecer que o crime pode ocorrer "por qualquer meio", o legislador ampliou a incidência da norma para abranger as modalidades digitais de perseguição, reconhecendo sua gravidade e seus impactos sobre direitos fundamentais.⁶ Essa abertura típica é especialmente relevante para a advocacia, pois o ambiente de litígio frequentemente gera situações de elevada tensão entre as partes, propiciando condutas que, quando repetidas, podem enquadrar-se no tipo penal.

O fenômeno do *stalking* digital apresenta singularidades importantes em relação à perseguição tradicional. Meios tecnológicos permitem vigilância contínua por aplicativos de localização, *scraping*⁷ de dados, monitoramento de redes sociais e manipulação de contas, criando um ambiente de controle permanente. A repetição dessas condutas, associada ao uso estratégico da tecnologia, amplia a potencialidade lesiva do fenômeno e exige abordagem jurídica que considere sua complexidade e as especificidades do meio digital (Guariento; Martins, 2021, p. 122).

No âmbito da advocacia, os impactos decorrentes da perseguição digital revelam-se especialmente sensíveis. O advogado pode figurar como vítima de condutas persecutórias em razão de sua atuação profissional. Ao mesmo tempo, a utilização de ferramentas digitais para obtenção de informações pode conduzir, ainda que inadvertidamente, à superação dos limites éticos e jurídicos da atuação

⁶ Art. 147-A do Código Penal (incluído pela Lei nº 14.132/2021 – Brasil, 2021): “Perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade. Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa. § 1º A pena é aumentada de metade se o crime é cometido: I – contra criança, adolescente ou idoso; II – contra mulher por razões da condição de sexo feminino; III – mediante concurso de 2 (duas) ou mais pessoas ou com o emprego de arma. § 2º As penas deste artigo são aplicáveis sem prejuízo das correspondentes à violência. § 3º Somente se procede mediante representação.

⁷ Linguee – Scraping: Termo do inglês que traduzido ao português fica = Raspagem

profissional, aproximando-se de práticas de monitoramento indevido ou vigilância abusiva.

2.1 O STALKING DIGITAL E OS ELEMENTOS JURÍDICOS DA PERSEGUIÇÃO ONLINE

A evolução das tecnologias de informação ampliou significativamente o alcance das condutas de perseguição continuada, possibilitando que práticas invasivas sejam realizadas à distância, de forma reiterada e, muitas vezes, sob anonimato. Nesse contexto, Doneda (2021, p. 102) observa que o ambiente digital oferece instrumentos que facilitam o monitoramento e a observação contínua das atividades individuais, tornando a proteção da privacidade um desafio crescente na sociedade da vigilância.

O *stalking* digital caracteriza-se pela utilização de dispositivos eletrônicos, redes sociais e outras ferramentas tecnológicas com o objetivo de vigiar, monitorar ou constranger a vítima, instaurando um cenário de controle e invasão de sua esfera privada (Guariento; Martins, 2021, p. 123). Tais condutas são potencializadas pela dinâmica do meio virtual, que permite atuação constante e ampla disseminação de informações, intensificando os danos causados à vítima (Greco, 2024, p. 12). O caráter silencioso dessas práticas, aliado à velocidade e à abrangência da internet, reforça seu potencial lesivo, sobretudo em razão da capacidade de produzir impactos psicológicos relevantes, afetando a liberdade, a tranquilidade e a autodeterminação do indivíduo.

A tipificação legal da perseguição, introduzida pela Lei nº 14.132/2021, alcança atividades digitais como o envio reiterado de mensagens, a criação de perfis falsos, o monitoramento de redes sociais ou a vigilância remota. A norma representou avanço ao adaptar o ordenamento brasileiro às formas contemporâneas de violência baseada em tecnologia (Brasil, 2021). A doutrina identifica como elementos característicos do *stalking* digital a repetição do ato, a intenção de intimidar ou controlar, o uso de tecnologias de rastreamento e a invasão contínua da esfera privada. Plataformas digitais permitem rastrear presença online, horários de acesso, preferências e interações, criando ambiente que facilita práticas persecutórias por meio de recursos tecnológicos sem precedentes (Guariento; Martins, 2021, p. 123).

No campo jurídico, o *stalking* digital exige reflexão sobre autoria, cadeia de custódia de provas digitais, finalidade do comportamento e distinção entre monitoramento legítimo e conduta abusiva. A atuação advocatícia nesse contexto demanda compreensão técnica e ética, pois diligências realizadas sem base legal adequada podem configurar violação de privacidade ou mesmo integrar o tipo penal de perseguição quando reiteradas ou excessivas (Guariento; Martins, 2021, p. 124).

2.2 A COLETA INDEVIDA DE DADOS E OS LIMITES ÉTICOS DA INVESTIGAÇÃO

O ambiente digital expandiu a capacidade de coleta e processamento de informações, criando uma zona cinzenta entre investigação lícita e coleta abusiva de dados. No contexto jurídico, essa fronteira torna-se sensível, pois a utilização de ferramentas digitais para fins probatórios pode, quando desproporcional ou reiterada, configurar prática persecutória e violação de direitos fundamentais. A coleta indevida de dados, especialmente quando sistemática, representa risco à dignidade da pessoa e à segurança informacional (Oliveira; Minto, 2021).

A LGPD estabelece bases legais e princípios que regulam o tratamento de dados, impondo que qualquer coleta seja restrita, necessária e fundamentada em critérios legítimos. A norma exige finalidade específica, transparência e proporcionalidade — elementos essenciais para distinguir uma diligência jurídica válida de conduta que configure perseguição, abuso ou violação de informação sensível (Brasil, 2018). Entende-se que esses princípios funcionam como limites objetivos à atuação investigativa do advogado: ultrapassá-los significa, em essência, converter a investigação em ilícito.

O Código de Ética e Disciplina da OAB reforça que o advogado deve atuar dentro de padrões de lealdade profissional e respeito aos direitos fundamentais. A obtenção de informações por meios ilícitos ou abusivos pode configurar infração disciplinar, além de violar o sigilo profissional e comprometer a integridade do processo (OAB, 2016). Cabe ao advogado identificar com precisão os limites da investigação admissível, utilizando apenas instrumentos legalmente autorizados e evitando práticas repetitivas, invasivas ou desproporcionais. A negligência na observância dessas regras pode resultar na nulidade de provas, em sanções

disciplinares e na violação do dever de proteção à privacidade dos envolvidos (Oliveira, 2022).

2.3 A RELAÇÃO ENTRE *STALKING* DIGITAL, CIBERSEGURANÇA E PRÁTICA ADVOCATÍCIA

A relação entre *stalking* digital e cibersegurança é direta, já que ambas as categorias envolvem riscos associados ao acesso, manipulação e difusão indevida de informações. O ambiente digital cria oportunidades para práticas persecutórias quando mecanismos de proteção são insuficientes ou inexistentes. Para Doneda (2021, p. 150), a fragilidade na segurança informacional não é apenas um problema técnico: trata-se de uma ruptura no sistema de proteção da autonomia informacional que pode ser explorada por agentes mal-intencionados para finalidades persecutórias. Falhas como ausência de criptografia, senhas fracas, equipamentos desatualizados e armazenamento inseguro tornam o profissional e seus clientes vulneráveis a ataques que podem ser utilizados para práticas de vigilância, intimidação ou manipulação estratégica de informações (Oliveira; Minto, 2021).

A legislação sobre proteção de dados exige que advogados adotem medidas robustas de segurança para mitigar riscos, sob pena de violar não apenas a LGPD, mas também deveres éticos e prerrogativas profissionais. A proteção tecnológica não é facultativa, mas elemento essencial da prática jurídica contemporânea. A ausência de medidas adequadas pode comprometer comunicações sigilosas, expor dados sensíveis e facilitar condutas persecutórias, ampliando o dano causado às vítimas (Mattos Filho, 2024).

Quando o comportamento persecutório é direcionado ao advogado, compromete prerrogativas essenciais, afeta a liberdade profissional e coloca em risco o exercício da defesa. Da mesma forma, quando praticado por advogados, ainda que sem intenção explícita de dano, viola o sigilo profissional, afronta a ética da advocacia e caracteriza conduta ilícita grave. Por isso, a compreensão das intersecções entre *stalking* digital, segurança da informação e prática jurídica é fundamental para assegurar que a atuação advocatícia ocorra de forma ética, segura e juridicamente responsável (Guariento; Martins, 2021, p. 127).

2.4 O CYBERSTALKING COMO EXPRESSÃO DIGITAL DO CRIME DE PERSEGUIÇÃO

O termo *cyberstalking* designa a prática de perseguição continuada realizada por meios eletrônicos e digitais, constituindo a modalidade virtual do *stalking* tradicional. A expressão resulta da combinação do prefixo *cyber*, associado ao ambiente informático e conectado, com o vocábulo *stalking*, que em língua inglesa significa perseguir ou espreitar. Trata-se, portanto, do mesmo fenômeno de perseguição obsessiva e reiterada, com a especificidade de que o meio de execução é o ciberespaço, composto por redes sociais, aplicativos de mensagens, plataformas digitais e demais ferramentas tecnológicas de comunicação (Guariento; Martins, 2021, p. 122).

A diferença entre o *stalking* convencional e o *cyberstalking* reside exclusivamente no meio utilizado para a prática das condutas persecutórias. Enquanto o *stalking* tradicional pressupõe a presença física do agressor ou meios analógicos de contato, o *cyberstalking* opera de forma remota, muitas vezes anônima, e com alcance potencialmente ilimitado, uma vez que as ferramentas digitais permitem vigilância contínua independentemente da localização geográfica da vítima. Essa característica amplia significativamente o potencial lesivo da conduta, pois o agressor pode monitorar perfis em redes sociais, rastrear localizações por aplicativos, enviar mensagens reiteradas por múltiplas plataformas e até criar perfis falsos para continuar o assédio mesmo após ser bloqueado (Greco, 2024, p. 12).

No ordenamento jurídico brasileiro, o *cyberstalking* não recebeu tipificação autônoma, sendo abrangido pela figura do crime de perseguição previsto no art. 147-A do Código Penal, introduzido pela Lei nº 14.132/2021 (Brasil, 2021). A norma, ao prever que a perseguição pode ocorrer “por qualquer meio”, abrange expressamente as modalidades digitais de conduta, o que inclui o monitoramento eletrônico, o envio reiterado de mensagens, a invasão de contas e perfis e o uso de ferramentas de rastreamento. A ausência de tipificação específica para o *cyberstalking* é criticada pela doutrina, que aponta a necessidade de majorante para as hipóteses em que o meio virtual amplia substancialmente o alcance e a lesividade da conduta persecutória (Nucci, 2024, p. 615).

No contexto da advocacia, a distinção entre *stalking* digital e *cyberstalking* é relevante sob perspectiva conceitual, mas irrelevante para fins de enquadramento penal: ambas as expressões descrevem a mesma conduta tipificada no art. 147-A do Código Penal (Brasil, 2021). O que importa, para a análise jurídica da atuação advocatícia, é compreender que qualquer atividade investigatória realizada por meios digitais que se torne reiterada, invasiva e sem finalidade legítima pode configurar perseguição, independentemente de o operador do direito a chamar de monitoramento, diligência ou investigação. A proteção da privacidade da parte investigada impõe ao advogado o dever de delimitar com precisão o objeto, o prazo e os meios de cada diligência digital, evitando que a investigação se converta em *cyberstalking* (Doneda, 2021, p. 102).

3 OS LIMITES ENTRE INVESTIGAÇÃO LÍCITA E PERSEGUIÇÃO ILÍCITA NA ERA DIGITAL

A transformação digital remodelou profundamente o ofício da advocacia e tornou os escritórios de todas as dimensões verdadeiros centros de processamento de dados sensíveis e estratégicos. Essa mudança exige que a cibersegurança deixe de ser encarada como mero suporte técnico para integrar o núcleo ético e jurídico da profissão. A Lei nº 13.709/2018 (LGPD) aplica-se a todos os controladores de dados, inclusive escritórios de advocacia, e impõe a adoção de medidas técnicas e administrativas para proteger informações e prevenir vazamentos (Doneda, 2021, p. 102).

O art. 42 da LGPD fixa a responsabilidade objetiva e solidária do controlador e do operador pelos danos causados aos titulares, de modo que a comprovação do vazamento e do nexo causal é suficiente para legitimar a indenização. Para além da obrigação de reparar danos, o art. 46 determina que o tratamento de dados pessoais ocorra em meios seguros. A falha em adotar essas medidas constitui violação ao dever de cuidado e pode ser enquadrada como culpa *in vigilando* ou *in eligendo* (Mendes; Doneda, 2018, p. 570).

No contexto da advocacia digital, a confiança do cliente é alicerçada no sigilo profissional. A ética impõe ao advogado o dever de preservar a intimidade, a vida

privada e os segredos do constituinte também em ambientes virtuais. Pesquisas demonstram que ataques a escritórios de advocacia têm aumentado por serem estas organizações custodiantes de documentos financeiros, estratégias de negociação e dados pessoais sensíveis. A ausência de investimentos em segurança expõe informações confidenciais e viola o dever de sigilo, o que gera riscos reputacionais e responsabilidades disciplinares (Oliveira; Minto, 2021).

Ao mesmo tempo, a busca por paridade de armas no processo penal levou o Conselho Federal da OAB a editar o Provimento nº 188/2018. Esse provimento conceitua a investigação defensiva como o conjunto de atividades investigatórias desenvolvidas pelo advogado, com ou sem assistência de consultores técnicos, visando à obtenção de elementos de prova lícitos para a tutela de direitos (Mazzoco do Nascimento, 2022).

3.1 A INVESTIGAÇÃO DEFENSIVA E O USO DE DADOS E TECNOLOGIAS

A investigação autônoma regulamentada pelo Provimento nº 188/2018 busca equilibrar a assimetria entre acusação e defesa ao permitir que o advogado produza provas sem depender exclusivamente do aparato estatal. A medida se justifica com base nos princípios constitucionais da igualdade, do devido processo legal e do contraditório, os quais são destacados pela doutrina como fundamentos da investigação defensiva (Mazzoco do Nascimento, 2022).

O advogado pode promover diligências investigatórias, colher depoimentos, requisitar informações disponíveis em órgãos públicos ou privados e realizar reconstituições de fatos. Essas atividades devem observar a licitude e a reserva de jurisdição. Interceptações telefônicas, quebras de sigilo bancário ou fiscal, buscas domiciliares e acesso a dispositivos eletrônicos exigem autorização judicial, sob pena de nulidade e ilicitude da prova. Verifica-se que o advogado não dispõe de poderes de polícia e o desrespeito a esses limites configura infração disciplinar e crime de invasão de dispositivo informático conforme o art. 154-A do Código Penal (Brasil, 1940; Greco, 2024, p. 12).

3.1.1 OS LIMITES JURÍDICOS DA COLETA DE DADOS E A VEDAÇÃO À *FISHING EXPEDITION*

O Provimento nº 188/2018 autoriza o advogado a valer-se de consultores técnicos, detetives particulares, peritos e outros auxiliares para a coleta de elementos. A colaboração de terceiros implica responsabilidade solidária do advogado pelos atos praticados. A falha de supervisão, denominada culpa in vigilando, pode gerar responsabilidade civil e disciplinar caso os investigadores adotem métodos ilícitos (OAB Campinas, 2021).

A investigação defensiva é um meio de assegurar a paridade de armas e não um fim em si. Por isso, a doutrina recomenda que as diligências sejam cirúrgicas e focadas no objeto da defesa para evitar o devassamento indiscriminado de dados pessoais. A falta de delimitação precisa do objeto de cada diligência investigativa é o principal vetor de risco de responsabilização do advogado, pois abre espaço para a prática da *fishing expedition*, também conhecida como pesca probatória (Lopes Jr., 2022).

O conceito de *fishing expedition* refere-se à busca indiscriminada de provas sem objeto específico na esperança de encontrar alguma evidência incriminadora. Essa prática viola o princípio da legalidade, o direito à privacidade e o devido processo legal ao autorizar devassa geral sem justa causa. Segundo Lopes Jr. (2022), a investigação deve ser pautada pela estrita legalidade e pela necessidade, de modo que buscas genéricas sem fundamento fático prévio comprometem a integridade do sistema acusatório. Rosa (2020) reforça que a pescaria probatória transforma o processo em um jogo de azar onde o Estado ou a defesa buscam fundamentos para uma acusação ou defesa que ainda não possui lastro probatório mínimo (Rosa, 2020).

RECURSO EM HABEAS CORPUS. CUMPRIMENTO DE MANDADO DE PRISÃO PREVENTIVA. REALIZAÇÃO DE DILIGÊNCIA DE BUSCA E APREENSÃO. AUSÊNCIA DE PRÉVIA AUTORIZAÇÃO JUDICIAL. DESVIO DE FINALIDADE E FISHING EXPEDITION. ILICITUDE DAS PROVAS OBTIDAS. TEORIA DOS FRUTOS DA ÁRVORE ENVENENADA. TRANCAMENTO DO INQUÉRITO POLICIAL. RECURSO EM HABEAS CORPUS PROVIDO. [...] 4. A obtenção de elementos de convicção ou de possíveis instrumentos utilizados na prática de crime - ainda que seja ao tempo do cumprimento da ordem de prisão no domicílio do réu - exige autorização judicial prévia, mediante a expedição do respectivo mandado de busca e apreensão (art. 241 do CPP), no qual devem ser especificados, dentre outros, o endereço a ser diligenciado, o motivo e os fins da diligência (art. 243 do CPP), o que, no entanto, não ocorreu. É de se destacar, também,

que muitos dos bens apreendidos se encontravam em outras residências do condomínio e que o local onde o recorrente foi detido nem sequer era sua residência. 5. Por se tratar de medida invasiva e que restringe sobremaneira o direito fundamental à intimidade, o ingresso em morada alheia deve se circunscrever apenas ao estritamente necessário para cumprir a finalidade da diligência. É o que se extrai da exegese do art. 248 do CPP, segundo o qual, "Em casa habitada, a busca será feita de modo que não moleste os moradores mais do que o indispensável para o êxito da diligência". 6. É ilícita a prova colhida em caso de desvio de finalidade após o ingresso em domicílio, seja no cumprimento de mandado de prisão ou de busca e apreensão expedido pelo Poder Judiciário, seja na hipótese de ingresso sem prévia autorização judicial, como ocorre em situação de flagrante delito. O agente responsável pela diligência deve sempre se ater aos limites do escopo - vinculado à justa causa - para o qual excepcionalmente se restringiu o direito fundamental à intimidade, ressalvada a possibilidade de encontro fortuito de provas. [...] (STJ - RHC: 153988 SP 2021/0296876-6, Relator: Ministro ROGERIO SCHIETTI CRUZ, Data de Julgamento: 11/04/2023, T6 - SEXTA TURMA, Data de Publicação: DJe 19/04/2023)

O Supremo Tribunal Federal e o Superior Tribunal de Justiça consolidaram jurisprudência contrária à pesca probatória e declararam ilícitas as provas colhidas nessas condições. O STJ tem anulado provas obtidas por meio de varredura indiscriminada de dispositivos eletrônicos sem prévia autorização judicial e delimitação clara do escopo da busca. Tais decisões reforçam a necessidade de que a investigação defensiva observe rigorosamente os limites legais e constitucionais para evitar a nulidade dos elementos de prova obtidos (Lopes Jr., 2022).

3.1.2 A PROTEÇÃO DA PRIVACIDADE E DOS DIREITOS FUNDAMENTAIS NA INVESTIGAÇÃO

Os limites constitucionais à atividade investigativa do advogado derivam dos direitos fundamentais consagrados no art. 5º da Constituição Federal. A inviolabilidade da intimidade, da vida privada, do domicílio e das comunicações constitui barreira intransponível à

atuação do particular. Esses direitos não cedem diante de interesses processuais sem prévia autorização judicial, o que significa que a diligência investigativa não pode atropelar o núcleo essencial da privacidade dos investigados (Brasil, 1988).

A LGPD reforça essa proteção ao exigir que o tratamento de dados pessoais seja fundamentado em uma das bases legais do art. 7º e observe o princípio da finalidade sem extrapolar os limites necessários ao propósito perseguido. Segundo

Doneda (2021), a autodeterminação informacional exige que o indivíduo tenha controle efetivo sobre seus próprios dados, o que só é possível quando os agentes de tratamento atuam dentro de limites legítimos e transparentes. O advogado que coleta dados além do necessário para a defesa de seu cliente viola a LGPD e pode caracterizar o ilícito penal de *stalking* quando essa coleta for reiterada e invasiva (Doneda, 2021, p. 150).

3.2 A RESPONSABILIDADE DO ADVOGADO E OS RISCOS DE VIOLAÇÃO DE DIREITOS

A responsabilidade do advogado no exercício da atividade investigatória é multidimensional e abrange as esferas ética, civil, penal e administrativa. O descumprimento dos deveres profissionais impostos pelo Estatuto da Advocacia (Lei nº 8.906/1994 – Brasil, 1994), pelo Código de Ética e Disciplina da OAB e pela LGPD pode resultar em sanções disciplinares que vão desde a censura até a exclusão dos quadros da ordem profissional. A jurisprudência dos tribunais pátrios evidencia que a violação reiterada de deveres éticos, ainda que sem configurar crime, é suficiente para fundamentar a aplicação das penalidades mais graves previstas no estatuto da classe. Nesse sentido, o Tribunal Regional Federal da 1ª Região reconheceu a legitimidade da exclusão de advogado dos quadros da OAB diante de condutas graves e reincidentes, consolidando o entendimento de que a atividade advocatícia impõe padrão elevado de conduta profissional cujo desatendimento acarreta responsabilização na esfera disciplinar (TRF-1, AC: 00174430720114013300, julgado em 26/02/2021):

ADMINISTRATIVO. ORDEM DOS ADVOGADOS DO BRASIL - OAB. EXERCÍCIO PROFISSIONAL. PROCESSO DISCIPLINAR INCIDENTAL DE INIDONEIDADE: EXCLUSÃO, APÓS SUSPENSÃO APLICADA TRÊS VEZES. LEI 8.906 (ART. 38, I). PRESCRIÇÃO: PRAZO QUINQUENAL NÃO CONSUMADO. NOTIFICAÇÕES ENCAMINHADAS AO ENDEREÇO PROFISSIONAL CONSTANTE DO CADASTRO DA OAB. PRESUNÇÃO DE CORREÇÃO. DEVER DO ADVOGADO DE MANTER O REGISTRO ATUALIZADO. CIÊNCIA DO ADVOGADO ACERCA DOS PROCEDIMENTOS DISCIPLINARES COMPROVADA PELA JUDICIALIZAÇÃO DE QUESTÕES CORRELATAS. PROVA DO FATO CONSTITUTIVO DO DIREITO. ÔNUS DO AUTOR (CPC: ART. 373, I). 1. Ação ordinária ajuizada contra o Conselho Federal da Ordem dos Advogados do Brasil requerendo a declaração de nulidade de todo e qualquer ato punitivo do réu contra o autor, em especial (...) o ato que excluiu o autor dos quadros da OAB, determinando a sua reinclusão em definitivo àquela instituição. 1.1 -

Postula o demandante, adicionalmente, a condenação da parte adversa ao pagamento de indenização por danos morais. Sugere suposta violação aos princípios da ampla defesa e do contraditório, uma vez que os procedimentos disciplinares teriam tramitado sem observar a necessidade de intimação/notificação pessoal. 2. A exclusão do autor dos quadros do órgão de classe não se deu por um fato isolado, mas em razão de 3 suspensões que ocorreram nos anos de 1999 e 2000. A instauração do processo incidental de inidoneidade se deu no ano de 2002, interrompendo o curso do prazo prescricional, conforme o § 2º, I, do art. 43 da Lei 8.906/94. Não se tem notícia de paralisação do feito por mais de 3 (três) anos. Tendo sido julgado em 2005, afasta-se a alegação de prescrição da pretensão punitiva. 3. O autor, ora apelante, sustenta que sua punição foi, em verdade, motivada por desejos persecutórios e vingativos de inimigos pessoais existentes na OAB, bem como por racismo, mas nenhuma prova apresenta. 4. A exclusão se deu por decisão do Pleno do Conselho Seccional/BA em Sessão Ordinária realizada no dia 5 de agosto de 2005. Por maioria, o colegiado declarou a inidoneidade do representado. 5. Conforme o voto do relator na Representação nº 5840/99, que transcorreu perante o Tribunal de Ética e Disciplina da OAB/BA, as representações envolvem fatos graves, com reincidências, tais como recebimento de valores sem repasse a clientes, retenção abusiva de autos, fraude à Caixa de Assistência dos Advogados, utilizando indevidamente o plano OAB-SALUS, ainda em fase de carência para parto de sua companheira, não pagando ao hospital, que está cobrando da Caixa, recebimento de valores sem proposição de processo e tratamento à parte sem urbanidade, etc. No referido processo, o colegiado suspendeu o advogado preventivamente por 90 (noventa) dias em setembro de 1999, com base no art. 70 da Lei 8.906/94. 6. No Processo Disciplinar nº 9289/98, o Tribunal de Ética e Disciplina da OAB/BA encaminhou ao endereço do autor notificação com AR/ECT para oferecer sustentação oral na sessão marcada para apreciação do feito, tendo o expediente sido recebido no dia 27/4/2000 (consta do autos). A decisão pela procedência da representação transitou em julgado, sendo aplicada ao autor nova pena de suspensão de 90 (noventa) dias, pelo cometimento da infração tipificada no art. 34, inciso XXII, da Lei 8.906/94. 7. Nos autos do Processo Ético-Disciplinar nº 2303/96, o autor foi, em julho de 1999, notificado para apresentar defesa prévia no prazo de 15 (quinze) dias, nos termos do art. 52 do Código de Ética e Disciplina da OAB, em razão de outra representação contra ele apresentada. 8. Posteriormente, em outubro de 2000, o Tribunal de Ética e Disciplina encaminhou novo ofício ao endereço do autor, também com A.R., comunicando a inclusão do aludido processo na pauta de julgamentos do dia 26/10/2000, notificando-o para, querendo, oferecer sustentação oral. No mesmo mês, foi notificado para tomar ciência da decisão colegiada proferida no Processo Ético-Disciplinar nº 2303/96, pela qual foi julgada procedente a representação e aplicada a pena de suspensão do exercício da advocacia pelo prazo de 180 (cento e oitenta) dias cumulada com multa de 03 (três) anuidades. 9. Em razão das 03 suspensões cominadas ao autor, o Tribunal de Ética e Disciplina decidiu instaurar o já citado procedimento para apuração de inidoneidade para o exercício da profissão, que culminou em sua exclusão. 10. As notificações foram enviadas, de regra, ao endereço constante da base de dados da OAB/BA, cuja atualização é de responsabilidade do próprio advogado. 11. O autor, apesar de não se manifestar apresentando defesa a tempo e modo nos inúmeros processos disciplinares que tramitaram na OAB/BA, não deixou de judicializar as questões tratadas naqueles procedimentos, manejando diversas ações perante o Poder Judiciário - como ele próprio afirma - na tentativa de suspender ou anular as sanções disciplinares aplicadas pelo Tribunal de Ética e Disciplina, o que afasta qualquer alegação de desconhecimento por suposta ausência de intimação. 12. Nos termos do art. 373, I, do CPC, é do autor o ônus da prova do fato constitutivo do direito que persegue. A alegação de ausência de notificação pessoal poderia ser demonstrada mediante juntada de cópia do processo administrativo

disciplinar, documento não trazido aos autos pelo demandante. O autor não comprovou - nem sequer alegou - eventual resistência da OAB/BA no fornecimento de cópia do processo disciplinar, situação que poderia ensejar a inversão do ônus da prova, com arrimo no § 1º do art. 373 do CPC: o autor muito alega e nada prova. 13. Não demonstrada ilegalidade (ato ilícito) na conduta do Tribunal de Ética e Disciplina da OAB/BA no que tange aos atos sancionatórios disciplinares trazidos à apreciação judicial, incabível - logicamente - a pretendida condenação da parte ré ao pagamento de indenização por danos morais e lucros cessantes. 14. Apelação do autor não provida. (TRF-1 - AC: 00174430720114013300, Relator: DESEMBARGADORA FEDERAL GILDA SIGMARINGA SEIXAS, Data de Julgamento: 26/02/2021, 7ª Turma, Data de Publicação: PJe 26/02/2021 PAG PJe 26/02/2021 PAG)

A Lei nº 14.132/2021 introduziu no Código Penal o crime de perseguição, que pune a conduta de perseguir alguém reiteradamente por qualquer meio. O tipo penal exige a ameaça à integridade física ou psicológica, a restrição da liberdade de locomoção ou a invasão da esfera de privacidade. O crime é habitual e exige a reiteração de um padrão de conduta obsessivo para sua configuração. A criminalização do *stalking* atende à necessidade de tutelar a liberdade individual e a integridade psicológica na sociedade hiperconectada (Nucci, 2024, p. 615).

No âmbito da advocacia, o desvio da função investigativa ocorre quando a coleta de provas é utilizada para intimidar a parte contrária ou assediar testemunhas. Essa prática é denominada *stalking* jurídico e representa abuso do direito de ação, podendo configurar tanto o crime de perseguição quanto ilícitos civis. O advogado que permite que seus auxiliares adotem práticas de perseguição ou pesca probatória incorre em responsabilidade civil e penal pelos danos morais decorrentes do sofrimento psicológico imposto às vítimas. Verifica-se que a responsabilidade do advogado é multidimensional e abrange as esferas ética, civil, penal e administrativa (Guariento; Martins, 2021, p. 127).

3.3 A ÉTICA PROFISSIONAL, A CIBERSEGURANÇA E A CONFIANÇA SOCIAL NA ADVOCACIA

A Constituição de 1988 define a advocacia como função essencial à administração da Justiça e impõe ao profissional elevado padrão de conduta. O Código de Ética e Disciplina da OAB consagra o dever de sigilo e a dignidade da profissão. Na era digital, esses deveres exigem a implementação de políticas de

governança de dados e de cibersegurança como extensão do sigilo profissional (OAB Campinas, 2021).

Pesquisas demonstram que escritórios de advocacia se tornaram alvos preferenciais de ataques cibernéticos em razão do grande volume de dados estratégicos que armazenam. A falta de investimento em segurança coloca em risco informações sigilosas e afeta os deveres éticos do advogado. Conforme Oliveira e Minto (2021), a segurança cibernética deixou de ser opcional para se tornar um requisito de sobrevivência e ética na advocacia moderna. Experiências estrangeiras recomendam a criação de protocolos de trabalho remoto para assegurar a confidencialidade de dados (American Bar Association, 2017).

A análise sistêmica das normas revela que o advogado contemporâneo atua sob um regime de vigilância mútua. Ao mesmo tempo em que dispõe de maior poder investigativo pelo Provimento nº 188/2018, está sujeito a controles rigorosos pelo Poder Judiciário e pela Autoridade Nacional de Proteção de Dados. A transição da proteção passiva para a proteção ativa configura o principal desafio da advocacia na presente década (Mattos Filho, 2024)

A ética profissional também se manifesta na responsabilidade proativa perante a Lei Geral de Proteção de Dados. Nesse contexto, a Autoridade Nacional de Proteção de Dados (ANPD) exerce papel fundamental na consolidação da cultura de proteção informacional no Brasil, atuando como órgão responsável pela fiscalização, regulamentação e orientação quanto ao tratamento adequado de dados pessoais. A atuação da ANPD revela-se essencial para garantir maior segurança jurídica aos agentes de tratamento, inclusive aos profissionais da advocacia, promovendo diretrizes voltadas à conformidade normativa, à prevenção de incidentes de segurança e à efetivação dos direitos fundamentais relacionados à privacidade e à proteção de dados pessoais. Assim, o descumprimento das obrigações previstas na LGPD pode ensejar sanções administrativas, responsabilização disciplinar e danos à reputação profissional, evidenciando a necessidade de observância contínua das diretrizes estabelecidas pela autoridade reguladora (Encarnação, 2025).

CONCLUSÃO

A análise empreendida ao longo deste artigo demonstrou que a cibersegurança na advocacia é muito mais do que uma obrigação técnica, consistindo em uma dimensão ética e jurídica estruturante do exercício profissional contemporâneo. O advogado que opera no ambiente digital assume simultaneamente os papéis de guardião da informação de seus clientes, agente de tratamento de dados sob a LGPD e, quando atua na investigação defensiva, potencial vetor de riscos à privacidade de terceiros.

A primeira seção revelou que a cibersegurança, compreendida em seus pilares de confidencialidade, integridade e disponibilidade, articula-se diretamente com o dever constitucional de proteção à intimidade e à vida privada e com o sigilo profissional. Conforme Doneda (2021, p. 150), a proteção de dados pessoais é instrumento de garantia da dignidade humana e das liberdades fundamentais na era digital. Essa premissa aplica-se com especial intensidade ao ambiente advocatício, no qual o dado tratado pode determinar o destino de pessoas em situações de extrema vulnerabilidade jurídica. A LGPD consolidou o advogado como agente de segurança da informação, impondo obrigações que vão além do âmbito ético-disciplinar e alcançam a responsabilidade civil objetiva prevista no art. 42 da lei.

A segunda seção evidenciou que o *stalking* digital apresenta características próprias que o distinguem das formas tradicionais de perseguição, como a possibilidade de atuação à distância, a facilidade de acesso a dados pessoais, o potencial de anonimato e a reiteração sistemática por meio de ferramentas tecnológicas. A tipificação do art. 147-A do Código Penal, ao prever que o crime pode ocorrer por qualquer meio, adaptou o ordenamento brasileiro às formas contemporâneas de violência baseada em tecnologia. Verificou-se que a coleta indevida e sistemática de dados pode configurar não apenas infração ética, mas crime contra a liberdade individual.

A terceira seção integrou essas dimensões para examinar a tênue fronteira entre investigação legítima e perseguição ilícita no exercício da advocacia. Constatou-se que o Provimento OAB nº 188/2018, ao regulamentar a investigação defensiva autônoma, não criou espaço de imunidade. O advogado que realiza monitoramento sistemático, acessa dados sem base legal legítima ou usa auxiliares sem supervisão

adequada pode incorrer em responsabilidade civil, disciplinar e penal. O conceito de *stalking* jurídico, entendido como o desvio funcional da investigação defensiva para fins de intimidação ou controle, representa categoria analítica relevante para delimitar os abusos no exercício da defesa técnica.

A hipótese central deste trabalho foi confirmada: a investigação advocatícia é legítima quando realizada em conformidade com os princípios da LGPD de finalidade, necessidade, transparência e segurança, além de respeitar o Estatuto da Advocacia e a Constituição Federal. O monitoramento abusivo, sistemático e sem base jurídica legítima aproxima-se da prática criminosa de *stalking* e pode resultar em responsabilização nas esferas civil, penal e disciplinar.

Como limitação desta pesquisa, reconhece-se a escassez de jurisprudência específica sobre *stalking* jurídico praticado por advogados, o que indica a necessidade de estudos empíricos e de acompanhamento das decisões dos Tribunais de Ética e Disciplina da OAB. Pesquisas futuras poderiam investigar casos concretos de investigação defensiva que ultrapassaram os limites legais, bem como analisar o impacto do uso de inteligência artificial na coleta de dados em contexto advocatício, tema emergente que a regulação atual ainda não alcança de forma satisfatória.

Conclui-se que a confiança social na advocacia, pilar fundamental da função essencial à administração da Justiça atribuída pela Constituição, dependerá da capacidade do profissional em equilibrar o zelo pela defesa técnica com o respeito aos direitos de personalidade. A ética, a cibersegurança e a proteção de dados não são obstáculos ao exercício da advocacia, sendo, na verdade, seus alicerces na era digital.

REFERÊNCIAS

ACADEMIA BRASILEIRA DE LETRAS. *Vocabulário Ortográfico da Língua Portuguesa*. 6. ed. Rio de Janeiro: ABL, 2021.

AMERICAN BAR ASSOCIATION. *Formal Opinion 477R: Securing Communication of Protected Client Information*. Chicago: ABA, 2017. Disponível em: <https://www.americanbar.org>. Acesso em: 10 fev. 2026.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR 6023: Informação e documentação – Referências – Elaboração*. Rio de Janeiro: ABNT, 2018.

BRASIL. [Constituição (1988)]. *Constituição da República Federativa do Brasil de 1988*. Brasília, DF: Presidência da República, [2016].

BRASIL. Conselho Federal da Ordem dos Advogados do Brasil. *Provimento n.º 188/2018*. Regulamenta o exercício da prerrogativa profissional do advogado de realização de diligências investigatórias para instrução em procedimentos administrativos e judiciais. Diário Eletrônico da OAB, Brasília, 11 dez. 2018.

BRASIL. *Lei nº 8.906, de 4 de julho de 1994*. Dispõe sobre o Estatuto da Advocacia e a Ordem dos Advogados do Brasil. Brasília, DF: Presidência da República, 1994.

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.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018.

BRASIL. *Lei nº 14.132, de 31 de março de 2021*. Acrescenta o art. 147-A ao Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para instituir o crime de perseguição. Diário Oficial da União, Brasília, 1 abr. 2021.

BRASIL. Tribunal de Justiça do Estado de São Paulo. *Agravo de Instrumento nº 2327501-45.2025.8.26.0000*. Agravo de instrumento. Ação de execução de título extrajudicial. Prescrição intercorrente. Nulidade de prova obtida. LGPD. Recurso não conhecido em parte e, na parte conhecida, não provido. Relator: Lavinio Donizetti Paschoalão. 38ª Câmara de Direito Privado. Julgado em: 16 out. 2025. Publicado em: 16 out. 2025.

BRASIL. Tribunal de Justiça do Estado de São Paulo. *Apelação Cível nº 1007804-48.2024.8.26.0038*. Apelação cível. Responsabilidade civil. Violação de sigilo profissional. LGPD. Atuação de advogado contra ex-cliente. Ausência de ilicitude. Recurso não provido. Relatora: Fátima Cristina Ruppert Mazzo. 4ª Câmara de Direito Privado. Julgado em: 30 set. 2025. Publicado em: 30 set. 2025.

BRASIL. Superior Tribunal de Justiça. *Recurso em Habeas Corpus nº 153988/SP*. Recurso em habeas corpus. Cumprimento de mandado de prisão preventiva. Realização de diligência de busca e apreensão sem prévia autorização judicial. Desvio de finalidade. *Fishing expedition*. Ilícitude das provas obtidas. Teoria dos frutos da árvore envenenada. Trancamento do inquérito policial. Recurso provido. Relator: Ministro Rogério Schietti Cruz. 6ª Turma. Julgado em: 11 abr. 2023. Publicado em: 19 abr. 2023. Diário da Justiça Eletrônico.

CONSELHO FEDERAL DA ORDEM DOS ADVOGADOS DO BRASIL. *Código de Ética e Disciplina da OAB*. Brasília, DF: CFOAB, 2016.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados*. 2. ed. São Paulo: Thomson Reuters Brasil, 2021.

ENCARNAÇÃO, Paulo Vitor Faria da. A responsabilidade civil pelo vazamento de dados pessoais: análise jurídico-hermenêutica da responsabilidade civil por vazamento de dados, com base na LGPD e precedentes do STF e STJ, entre 2023 e 2025. *Migalhas de Peso*, 25 ago. 2025. Disponível em: <https://www.migalhas.com.br/depeso>. Acesso em: 10 fev. 2026.

GRECO, Rogério. *Código Penal comentado*. 18. ed. Barueri: Atlas, 2024.

GUARIENTO, Maria; MARTINS, João. Advocacia e proteção de dados: o advogado como agente de tratamento na LGPD. *Revista de Direito Digital*, São Paulo, v. 7, n. 2, p. 115-134, 2021.

INFOPÉDIA. Cibersegurança. Porto: Porto Editora, 2021. Disponível em: <https://www.infopedia.pt/dicionarios/lingua-portuguesa/ciberseguranca>. Acesso em: 10 nov. 2025.

LOPES JR., Aury. *Direito Processual Penal*. 19. ed. São Paulo: Saraiva Educação, 2022.

MATTOS FILHO ADVOGADOS. *Proteção de dados e cybersecurity*. São Paulo: Mattos Filho, 2024. Disponível em: <https://www.mattosfilho.com.br>. Acesso em: 8 nov. 2025.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. *Big data: a revolution that will transform how we live, work, and think*. London: John Murray, 2013.

MAZZOCO DO NASCIMENTO, Joyce. Investigação defensiva: análise do provimento 188/18. *Migalhas de Peso*, 5 jul. 2022. Disponível em: <https://www.migalhas.com.br/depeso>. Acesso em: 15 out. 2025.

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

MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018): o novo paradigma da proteção de dados no Brasil. *Revista de Direito do Consumidor*, São Paulo, v. 120, p. 555-587, nov./dez. 2018.

NUCCI, Guilherme de Souza. *Código Penal comentado*. 24. ed. Rio de Janeiro: Forense, 2024.

OAB CAMPINAS. Comissão Especial de Privacidade e Proteção de Dados; Comissão de Direito Digital. *Guia da LGPD aplicada aos escritórios de advocacia*. Campinas: OAB Campinas, 2021.

OLIVEIRA, Cristina Godoy Bernardo de. *Direito ao esquecimento na internet: o Marco Civil da Internet e os novos desafios da proteção de dados*. São Paulo: Foco, 2022.

OLIVEIRA, Cristina Godoy Bernardo de; MINTO, Giovanna Aparecida Rossini. Segurança cibernética em escritórios de advocacia. *Migalhas – IA e Proteção de Dados*, 16 jul. 2021. Disponível em: <https://www.migalhas.com.br/ia-e-protecao-de-dados>. Acesso em: 20 out. 2025.

PRIBERAM. Cibersegurança. In: *Dicionário Priberam da Língua Portuguesa* [em linha]. Lisboa: Priberam, 2008-2026. Disponível em: <https://dicionario.priberam.org/ciberseguranca>. Acesso em: 10 nov. 2025.

ROSA, Alexandre Moraes da. *Guia do Processo Penal Estratégico: de acordo com a Teoria dos Jogos*. 5. ed. Florianópolis: Empório do Direito, 2020.

SUPERIOR TRIBUNAL DE JUSTIÇA. Tema 1.199/DF. Relator: Min. Gurgel de Faria. Julgado em 10 maio 2023. Disponível em: <https://www.stj.jus.br>. Acesso em: 10 fev. 2026.

VAN DIJCK, José. Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society*, v. 12, n. 2, p. 197–208, 2014.