Cognitio Juris
ISSN 2236-3009

OS LIMITES CONSTITUCIONAIS À QUEBRA DE SIGILO DE DADOS ESTÁTICOS: UMA ANÁLISE DO TEMA 1.148 DO STF À LUZ DA TEORIA ORWELLIANA

THE CONSTITUTIONAL LIMITS ON ACCESS TO STATIC DATA: ANALYSIS OF STF THEME 1,148 IN LIGHT OF ORWELLIAN THEORY

Artigo submetido em 21 de setembro de 2026
Artigo aprovado em 24 de setembro de 2026
Artigo publicado em 27 de setembro de 2026

Cognitio Juris
Volume 16 – Número 59 – 2026
ISSN 2236-3009

.

Autor:
Felipe Leoni Carteiro Leite Moreira[1]

.

RESUMO: A crescente digitalização das interações sociais impõe novos e complexos desafios ao Direito Penal e ao Processo Penal, notadamente no que se refere à compatibilização entre a eficácia da investigação criminal e a proteção dos direitos fundamentais dos cidadãos. Nesse contexto, o presente artigo examina criticamente a possibilidade de decretação

judicial da quebra de sigilo de dados estáticos de forma genérica, dirigida a pessoas indeterminadas, à luz do Tema 1.148, atualmente em julgamento perante o Supremo Tribunal Federal. Sustenta-se que tais ordens, ao carecerem de individualização e de fundamentos específicos, violam os princípios constitucionais da legalidade, da intimidade, da proteção de dados pessoais e, especialmente, da presunção de inocência. A análise articula a aplicação de dispositivos normativos, como, exemplificativamente, os incisos X, XII, LXXIX e LVII do artigo 5.º da Constituição Federal de 1988, com a jurisprudência do Supremo Tribunal Federal e do Superior Tribunal de Justiça, além de reflexões doutrinárias e filosóficas, notadamente aquelas inspiradas na obra 1984, de George Orwell, a qual oferece uma representação crítica dos riscos associados à vigilância estatal irrestrita. Conclui-se pela inconstitucionalidade de ordens judiciais genéricas de quebra de sigilo, defendendo a necessidade de estrita observância aos limites impostos pela Constituição ao poder investigativo do Estado na era digital.

Palavras-chave: Proteção de dados pessoais; Presunção de inocência; Processo penal digital; Tema 1.148/STF; Estado de vigilância; George Orwell.

ABSTRACT: The increasing digitalization of social interactions poses new and complex challenges to Criminal Law and Criminal Procedure, particularly with regard to reconciling the effectiveness of criminal investigations with the protection of citizens' fundamental rights. Against this backdrop, this article critically examines the possibility of courts issuing generic orders compelling the disclosure of static data concerning unidentified individuals, in light of Theme 1,148, currently under consideration by the Brazilian Federal Supreme Court (STF). It argues that such orders, insofar as they lack individualization and specific grounds, violate the constitutional principles of legality, privacy, personal data protection and, in particular, the presumption of innocence. The analysis combines the application of constitutional provisions, including, by way of example, items X, XII, LXXIX and LVII of Article 5 of the 1988 Federal Constitution, with the case law of the Brazilian Federal Supreme Court and the Superior Court of Justice (STJ), as well as doctrinal and philosophical reflections, particularly

those inspired by George Orwell's 1984, which provides a critical portrayal of the risks associated with unrestricted state surveillance. The article concludes that generic judicial orders compelling the disclosure of confidential data are unconstitutional and argues for strict adherence to the limits imposed by the Constitution on the State's investigative powers in the digital age.

Keywords: Personal data protection; Presumption of innocence; Digital criminal procedure; STF Theme 1,148; Surveillance state; George Orwell.

I INTRODUÇÃO

A intensificação da digitalização da vida cotidiana, sobretudo nos últimos anos, tem imposto desafios sem precedentes ao ordenamento jurídico, com especial incidência sobre o Direito Penal e o Processo Penal. Nesse novo contexto social, sobressai a tensão entre a busca por uma investigação criminal eficaz, cada vez mais alicerçada em fontes de prova digitais, e a necessária salvaguarda dos direitos fundamentais dos cidadãos, tal qual a proteção de dados pessoais e a privacidade.

Com efeito, o avanço das tecnologias de comunicação e de armazenamento de dados conferiu às informações telemáticas e estáticas um papel central na investigação de crimes complexos. Para além da crescente incidência de delitos cibernéticos, diversas infrações penais passaram a empregar recursos tecnológicos tanto em sua fase preparatória quanto executória, de tal sorte que dados de conexão, registros de acesso a aplicações de internet e demais informações digitais tornaram-se elementos importantíssimos à atividade investigativa, sendo, por isso, objeto frequente de requisições realizadas pela polícia judiciária no âmbito investigativo.

Contudo, a possibilidade de acesso a esta vastidão das informações levanta questionamentos profundos sobre os limites da atuação estatal na persecução penal. Emerge, com particular acuidade, a controvérsia acerca da constitucionalidade de ordens judiciais que determinam a

quebra genérica do sigilo de dados, telemáticos ou estáticos, atingindo um universo indeterminado de pessoas. Tais ordens, muitas vezes justificadas pela dificuldade inicial em identificar suspeitos de cometimento de atos ilícitos, colocam em xeque garantias constitucionais basilares, como a intimidade, a vida privada, a proteção de dados pessoais e, por fim, a própria sistemática da presunção de inocência.

Essa delicada ponderação entre eficácia da persecução penal e liberdades individuais encontra-se no cerne do Recurso Extraordinário 1.301.250/RJ, ao qual o Supremo Tribunal Federal reconheceu repercussão geral, identificando-o como Tema 1.148. Nesse *leading case*, ainda em julgamento, a Suprema Corte brasileira foi instada a definir os limites constitucionais para a decretação judicial da quebra de sigilo de dados telemáticos e estáticos no âmbito de investigações penais envolvendo pessoas indeterminadas.

Entendem-se por dados telemáticos o conteúdo das comunicações realizadas por meio de recursos tecnológicos, bem como à dinâmica da interação digital em tempo real. Incluem, por exemplo, o teor de mensagens trocadas em aplicativos, e-mails, conversas em redes sociais, transmissões de dados em chamadas de voz ou vídeo, e qualquer informação que revele o conteúdo comunicacional propriamente dito.

Em contraste, os dados estáticos são aqueles relacionados a informações pessoais e registros de conexão ou de acesso a servidores, navegadores ou aplicações de internet. Diferenciam-se dos dados telemáticos propriamente ditos, pois referem-se a elementos pré-existentes e armazenados, como logs de acesso, endereços IP, datas e horários de utilização.

A controvérsia perante o Supremo Tribunal Federal exige, nessa linha, a harmonização entre, de um lado, os direitos fundamentais, já mencionados, como a intimidade, a vida privada, a proteção de dados pessoais e a presunção da inocência – assegurados, respectivamente, pelos incisos X, XII, LXXIX e LVII do artigo 5.º da Constituição Federal de 1988 – e, de outro, os imperativos estatais de segurança pública e de efetividade da investigação criminal.

O presente artigo, portanto, tem como objetivo geral analisar criticamente os limites constitucionais impostos à decretação da quebra de sigilo de dados estáticos em relação a pessoas indeterminadas, tal qual requisitado no bojo do *leading case* analisado pelo Supremo Tribunal Federal, sustentando a inconstitucionalidade de ordens judiciais genéricas. Tais medidas, ao carecerem de especificidade e individualização de agentes, violam frontalmente direitos fundamentais e representam um risco significativo de instauração de um estado de vigilância generalizada, ecoando as preocupações distópicas levantadas por George Orwell em sua obra "1984".

A relevância desta análise reside não apenas na necessidade de oferecer segurança jurídica em um campo ainda nebuloso da investigação digital, mas também na urgência de proteger os cidadãos contra devassas indiscriminadas em suas vidas privadas, garantindo que a busca pela verdade processual não se converta em um instrumento de opressão ou controle social excessivo. A discussão transcende o âmbito estritamente jurídico, tocando em questões éticas e sociais fundamentais sobre o tipo de sociedade que se deseja construir na era da informação.

Para alcançar o objetivo proposto, adotar-se-á como metodologia a pesquisa bibliográfica e documental, com análise da Constituição Federal de 1988, da legislação infraconstitucional pertinente (com destaque para o Marco Civil da Internet – Lei 12.965/2014), da jurisprudência do Supremo Tribunal Federal, especialmente dos votos proferidos no Recurso Extraordinário 1.301.250/RJ, do Superior Tribunal de Justiça, da doutrina jurídica especializada em direito constitucional, processual penal e digital, bem como das reflexões de George Orwell sobre totalitarismo e vigilância.

Este trabalho está estruturado em três partes principais, além desta introdução. A primeira seção abordará a proteção constitucional conferida à intimidade, à vida privada e aos dados pessoais, cuja abrangência foi ampliada com a promulgação da Emenda Constitucional 115/2022. Nessa etapa, será enfatizada a exigência de ordem judicial fundamentada para

eventual relativização dessas garantias, bem como a necessidade de previsão legal expressa para a quebra do sigilo de dados estáticos.

A segunda seção será dedicada à análise do Tema 1.148 do Supremo Tribunal Federal, com a exposição da controvérsia jurídica, do caso concreto que lhe deu origem e dos votos já proferidos – ou menções realizadas – pelos ministros da Corte. Destaca-se, desde já, que o foco da discussão reside na requisição judicial de dados estáticos, tais como registros de conexão e de acesso a aplicações de internet, e não de dados telemáticos *stricto sensu*. Para tanto, far-se-á, em tópico apartado, a necessária diferenciação conceitual entre as categorias de dados estáticos e dados telemáticos, a fim de delimitar com precisão o objeto jurídico em análise.

Na terceira seção, será apresentada uma abordagem crítica com base na teoria orwelliana, examinando os riscos associados à quebra genérica de sigilo de dados como possível instrumento de vigilância estatal em larga escala e violação do princípio da presunção de inocência.

Por fim, a conclusão sintetizará os principais argumentos desenvolvidos ao longo do trabalho, reafirmando a tese defendida quanto à necessidade de limites constitucionais estritos à requisição indiscriminada de dados pessoais no contexto da persecução penal.

II A PROTEÇÃO CONSTITUCIONAL DA INTIMIDADE, DA VIDA PRIVADA E DO SIGILO DE DADOS E O PRINCÍPIO DA LEGALIDADE

A Constituição Federal de 1988, promulgada em um contexto de redemocratização e marcada por uma forte valorização dos direitos fundamentais, instituiu um sistema robusto de proteção aos direitos da personalidade como os direitos à intimidade, à vida privada e ao sigilo de dados e comunicações. No âmbito penal, com igual relevo, o texto constitucional consagrou os princípios do devido processo legal, do contraditório e da presunção de inocência, erigindo-os como garantias estruturantes de uma nova ordem democrática. Esses

pilares passaram a assegurar (ou buscar assegurar) não apenas a integridade do processo penal, mas também a proteção do indivíduo contra abusos estatais, funcionando como proteções indispensáveis em um Estado Democrático de Direito.

Com efeito, o inciso X do artigo 5º da Carta Magna estabelece de forma inequívoca que "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". Trata-se de uma cláusula geral de proteção à vida privada e à intimidade dos cidadãos, abrangendo um espectro amplo de situações da vida pessoal e informacional do indivíduo, com o objetivo de resguardá-lo contra ingerências arbitrárias, especialmente no tocante ao avanço de tecnologias que potencializam a vigilância e o controle estatal sobre os cidadãos.

Esse núcleo de direitos é complementado pelo inciso XII do mesmo dispositivo constitucional, que garante que o sigilo das comunicações telefônicas, de dados e de correspondência, somente poderá ser relativizado "por ordem judicial, nas hipóteses e na forma que a lei estabelecer, para fins de investigação criminal ou instrução processual penal". A redação expressa desse artigo evidencia que a violação dessas garantias não se dá de maneira discricionária, mas sim sob o crivo do princípio da legalidade estrita: apenas a lei pode autorizar, e de forma expressa, eventual restrição a esses direitos, mediante controle judicial e observância das finalidades legítimas constitucionalmente previstas.

Reforçando essa arquitetura de proteção aos direitos fundamentais, especialmente em um cenário contemporâneo marcado pela crescente digitalização da vida social, a Emenda Constitucional 115, de 2022, incluiu o inciso LXXIX ao artigo 5º, assegurando, "nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais". Essa inclusão elevou a proteção de dados pessoais ao status de direito fundamental autônomo, reconhecendo sua importância crescente e a necessidade de um regime jurídico específico para tutelá-lo, o que se reflete na Lei Geral de Proteção de Dados Pessoais (LGPD – Lei 13.709/2018), embora esta não se aplique diretamente à persecução penal (Art. 4º, III, 'd').

Assim, o que se observa no sistema constitucional brasileiro é a consagração de um modelo de proteção qualificada da privacidade e do sigilo, em que eventuais restrições somente são legítimas quando amparadas pela lei, autorizadas pelo Judiciário e estritamente vinculadas à finalidade de tutela do interesse público, especialmente no contexto da persecução penal. Trata-se, portanto, de um sistema que protege de forma ampla, mas que admite exceções rigorosamente condicionadas, sempre sob a égide do princípio da legalidade.

Conforme destacou a Ministra Rosa Weber em seu voto no Recurso Extraordinário 1.301.250/RJ,

[…] somente uma espécie de ato normativo específico, a lei, que se reveste, via de regra, de caráter geral e abstrato, produzido por um órgão de representação popular – no nosso caso, o Congresso Nacional – pode inovar na ordem jurídica.

O *direito de não se submeter senão às leis*, nas famosas palavras de Benjamin Constant, traduz concepção da lei como instrumento de salvaguarda dos direitos fundamentais individuais, pois se revela completamente oposto a qualquer modelo arbitrário e personalista.

Apesar das transformações decorrentes da ascensão do Estado Constitucional, ainda hoje prevalece compreensão de que não há poder acima ou à margem da Constituição e das leis, sendo tal compreensão notável mecanismo de proteção das liberdades públicas, além de base, de limite e de controle de todo poder estatal.[2]

Ainda segundo a Ministra do Supremo Tribunal Federal,

Desse modo, os direitos fundamentais individuais, por consubstanciarem matéria impassível de delegação legislativa (CF, art. 68, § 1º, II), estão abarcados pela reserva de lei formal. Em relação às questões processuais penais, há censura de edição de medidas provisórias (CF, art. 62, § 1º, I, b).

Destaco, por necessário, que, inequivocamente, o processo penal mantém vínculo de íntima conexão – quiçá de indissociabilidade – com os direitos fundamentais, não só pela existência de inúmeros princípios processuais de caráter fundamental que conformam todo ordenamento, como também pelo fato de que a restrição à liberdade de locomoção pressupõe o desenvolvimento de um devido processo disciplinado em lei.

Assim, dado o vínculo de íntima conexão acima exposto, é possível asseverar, sem qualquer dúvida razoável, que, não só pelo impedimento de delegação legislativa, as disposições normativas atinentes ao direito processual penal estão sujeitas à *reserva de parlamento (...).*[3]

Destarte, dadas as premissas constitucionais acima engendradas, o principal ponto de controvérsia em torno da possibilidade de quebra de sigilo de dados estáticos reside na interpretação segundo a qual o texto constitucional não lhes teria conferido o mesmo grau de proteção atribuído aos dados telemáticos. A partir da análise dos precedentes jurisprudenciais sobre a matéria — notadamente no julgamento do Recurso em Mandado de Segurança n.º 60.698/RJ, pelo Superior Tribunal de Justiça, verifica-se a consolidação do entendimento de que a requisição judicial de dados estáticos possui natureza jurídica distinta daquela relativa à interceptação de comunicações.

A determinação do Magistrado de primeiro grau, de quebra de dados informáticos estáticos, relativos a arquivos digitais de registros de conexão ou acesso a aplicações de internet e eventuais dados pessoais a eles vinculados, é absolutamente distinta daquela que ocorre com as interceptações das comunicações, as quais dão acesso ao fluxo de comunicações de dados, isto é, ao conhecimento do conteúdo da comunicação travada com o seu destinatário. Há uma distinção conceitual entre a quebra de sigilo de dados armazenados e a interceptação do fluxo de comunicações. Decerto que o art. 5º, X, da CF/88 garante a inviolabilidade da intimidade e da privacidade, inclusive quando os dados informáticos constarem de banco de dados ou de arquivos virtuais mais sensíveis. Entretanto, o acesso a

esses dados registrados ou arquivos virtuais não se confunde com a interceptação das comunicações e, por isso mesmo, a amplitude de proteção não pode ser a mesma.[4]

Conforme assentado no referido julgamento, a determinação judicial de acesso a dados informáticos estáticos não se equipararia à interceptação do fluxo de comunicações, que envolve o acesso ao conteúdo propriamente dito das mensagens trocadas entre interlocutores. Haveria, portanto, uma distinção conceitual clara entre a quebra de sigilo de dados armazenados e a interceptação em tempo real das comunicações, sendo esta última regida por requisitos mais rigorosos, em virtude da proteção reforçada assegurada pelo artigo 5º, inciso XII, da Constituição Federal.

Contudo, o entendimento segundo o qual existiria uma hierarquização constitucional entre dados estáticos e dados telemáticos, admitindo-se, por conseguinte, um grau de proteção inferior para a primeira categoria, não parece se harmonizar adequadamente com os princípios que estruturam o processo penal em um Estado Democrático de Direito. Isso porque, embora tal distinção encontre respaldo em parte da jurisprudência, ela colide com a existência de previsão legal expressa que assegura proteção aos dados de natureza estática, de tal sorte que qualquer interpretação que relativize essa proteção, no âmbito do processo penal, revela-se incompatível com os princípios da legalidade e da tipicidade.

Trata-se, nesse caso, do artigo 22 do Marco Civil da Internet (Lei Federal 12.965/14), cuja literalidade determina que é possível a requisição judicial de registros de conexão ou de acesso a aplicações de internet, desde que existam "fundados indícios da ocorrência do ilícito", "justificativa motivada da utilidade dos registros solicitados" e a especificação do "período ao qual se referem os registros". Importante destacar, outrossim, que o Decreto de regulamentação do Marco Civil da Internet (Decreto nº 8.771/2016) veda textualmente, em seu artigo 11, § 3º, determinações de quebra de sigilo genéricas, exigindo a indicação dos alvos afetados.

Art. 11. As autoridades administrativas a que se refere o art. 10, § 3º da Lei nº 12.965, de 2014 , indicarão o fundamento legal de competência expressa para o acesso e a motivação para o pedido de acesso aos dados cadastrais.

(…)

§ 3º Os pedidos de que trata o caput devem especificar os indivíduos cujos dados estão sendo requeridos e as informações desejadas, sendo vedados pedidos coletivos que sejam genéricos ou inespecíficos.[5]

Essa disposição normativa reforça a necessidade de individualização e especificidade nas ordens judiciais de quebra de sigilo, em consonância com os princípios constitucionais da privacidade e da fundamentação das decisões judiciais.

Assim, embora exista, de fato, uma distinção jurídica entre os dados telemáticos e os dados estáticos, sendo estes últimos o centro da controvérsia no Tema 1.148 do Supremo Tribunal Federal, tal diferenciação não autoriza um regime de proteção menos rigoroso que desconsidere os princípios constitucionais aplicáveis ao processo penal. Ainda que cada categoria de dado esteja submetida a premissas normativas próprias, a interpretação quanto à possibilidade de quebra do sigilo de dados estáticos deve ser realizada à luz dos princípios constitucionais gerais, especialmente aqueles que regem a atividade persecutória estatal, com destaque para o devido processo legal, a presunção de inocência e o princípio da legalidade.

III A NECESSÁRIA DISTINÇÃO CONCEITUAL ENTRE DADOS ESTÁTICOS E DADOS TELEMÁTICOS FRENTE AO TEMA 1.148/STF

Muito embora o Tema 1.148, atualmente em julgamento pela Suprema Corte brasileira, tenha sido formalmente intitulado como *“Limites para decretação judicial da quebra de sigilo de dados telemáticos, no âmbito de procedimentos penais, em relação a pessoas*

indeterminadas", observa-se que o caso concreto examinado envolve, na verdade, a requisição, por autoridade policial, dos chamados dados estáticos.

Dessa forma, a análise constitucional e procedimental da quebra de sigilo de dados estáticos referentes a pessoas indeterminadas exige, como premissa fundamental, uma compreensão técnica e jurídica acurada das distintas categorias de dados digitais e dos respectivos regimes de proteção que lhes são conferidos. Nesse contexto, revela-se essencial estabelecer uma distinção clara entre os chamados dados estáticos – oriundos de registros de conexão e de acesso a aplicações de internet – e os dados telemáticos propriamente ditos, que envolvem o conteúdo comunicacional.

Com efeito, o Marco Civil da Internet oferece definições normativas para a delimitação conceitual das diferentes categorias desses dados. Em seu artigo 5º, o legislador estabeleceu parâmetros técnicos que servem de base para essa delimitação, especialmente no que se refere à distinção entre dados de conexão, registros de acesso a aplicações de internet e o conteúdo das comunicações:

Art. 5º Para os efeitos desta Lei, considera-se:

(…)

VI – registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;

VII – aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet; e

VIII – registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.[6]

O inciso VI define “registro de conexão” como “o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados”. Trata-se, portanto, de dados estáticos, que não revelam o conteúdo das comunicações, mas apenas metadados sobre o estabelecimento da conexão.

Já o inciso VIII conceitua “registros de acesso a aplicações de internet” como “o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP”. Estes também são considerados dados estáticos, embora possam revelar padrões de comportamento do usuário.

Com base nas definições legais do Marco Civil da Internet, pode-se concluir que os dados estáticos correspondem a informações armazenadas que dizem respeito a aspectos técnicos da conexão e do uso de aplicações na internet, sem envolver o conteúdo das comunicações. Englobam, por exemplo, registros de data, hora, duração da conexão e endereços IP utilizados, bem como logs de acesso a sites e serviços digitais. Tais dados, por não revelarem diretamente o teor das interações do usuário, são considerados metadados, ainda que sua análise possa permitir a reconstrução de hábitos e comportamentos online. Sua coleta, embora menos intrusiva do que a interceptação de comunicações, continua sujeita à proteção constitucional, especialmente quando requerida de forma ampla ou indiscriminada, como no caso de pessoas indeterminadas.

A Lei de Interceptação Telefônica (Lei 9.296/1996), por seu turno, não apresenta uma definição expressa do termo “dados telemáticos” – vocábulo oriundo da junção entre “telecomunicações” e “informática” – mas deixa claro que se trata de informações obtidas por meio da “interceptação de comunicações telefônicas, de qualquer natureza”, bem como da “interceptação do fluxo de comunicações em sistemas de informática e telemática” (art. 1º).

Na prática jurídica e doutrinária, consolidou-se o entendimento de que os dados telemáticos abrangem um espectro mais amplo de informações digitais, que incluem, principalmente, o conteúdo das comunicações transmitidas por meios eletrônicos, como mensagens enviadas por e-mail, aplicativos de troca de mensagens, redes sociais e demais interações em tempo real no ambiente digital.

Conforme destaca BADARÓ (2012, p. 348),

"a tutela constitucional da liberdade das comunicações telefônicas (art. 5º, XII) não inclui os dados de registro das ligações telefônicas (p. ex: número da linha telefônica para a qual foi feita a ligação pelo telefone interceptado ou número da linha telefônica que efetuou ligação para linha interceptada, horário das ligações etc.) que ficam armazenados nas operadoras dos serviços de telefonia, e permanecem protegidos pela garantia geral da intimidade e da vida privada (CR, art. 5º, X)."[7]

Complementa essa distinção LIMA (2014, p. 239),

"por conteúdo de comunicações privadas deve-se entender a troca de mensagens por meio da Internet com qualquer restrição de acesso ao público amplo, podendo conter áudio, imagem, vídeo ou texto. Eventual obtenção do fluxo dessas comunicações, conforme exposto no § 2° do art. 10 do Marco Civil, deve seguir o disposto na Lei 9.296/1996, a qual regulamenta o inc. XII, parte final, do art. 5° da CF/1988."[8]

Ademais, conforme consignado pelo Superior Tribunal de Justiça no julgamento do Agravo Regimental no Recurso Ordinário em Mandado de Segurança 71.168/RJ, há uma distinção objetiva e material entre as categorias de dados:

"Não se pode entender como "registros de conexão" ou "registros de acesso a aplicações de internet", os conteúdos de e-mails, o conteúdo armazenado associados às contas Google, conteúdo de Gmail, conteúdo do Google Fotos (incluindo os respectivos metadados –

geomarcação), conteúdo o Google Drive, lista de contatos, histórico de localização, incluindo os trajetos pesquisados no google maps, waze ou outros que importem a função GPS, consultas (pesquisas) realizadas pelo usuário do dispositivo (histórico de navegação/ pesquisa), informações relacionadas às contas do Google Play, incluindo APPs baixados (downloads) ou comprados, lista de desejos, pessoas e informações relacionadas às contas referidas, etc., porque tudo isso representa a vida íntima dos usuários dos serviços de internet prestados pelas agravantes."[9]

A distinção entre dados estáticos e dados telemáticos, sob essa ótica, não se configura como mero desdobramento conceitual, mas sim como ponto relevante da controvérsia interpretativa acerca dos requisitos e da própria admissibilidade da quebra de sigilo dessas informações no âmbito da persecução penal.

De um lado, portanto, sustenta-se que os dados estáticos, por não envolverem o conteúdo das comunicações, estariam sujeitos a um regime jurídico menos restritivo, não sendo exigidas as mesmas cautelas aplicáveis às interceptações de dados telemáticos, mormente a necessidade de previsão legal expressa. De outro, há quem defenda que não se pode admitir qualquer forma de hierarquização normativa ou constitucional entre os dois institutos, uma vez que ambos se encontram abrangidos pela proteção conferida aos direitos fundamentais à intimidade, à vida privada e à proteção de dados, razão pela qual eventual acesso estatal a tais informações deve estar condicionado aos mesmos critérios de legalidade, necessidade, proporcionalidade e reserva de jurisdição daqueles impostos à quebra de sigilo de dados telemáticos.

IV O TEMA 1.148 DO STF: A CONTROVÉRSIA SOBRE A QUEBRA DE SIGILO GENÉRICA E A ANÁLISE DOS VOTOS

A tensão entre a necessidade de investigar crimes relevantes, assegurando a eficácia da persecução penal e a promoção da segurança pública, e a proteção dos direitos

fundamentais na era digital encontra-se em pleno julgamento no Supremo Tribunal Federal no âmbito do recurso extraordinário que culminou no Tema 1.148.

Neste julgamento, o Supremo Tribunal Federal busca definir se é constitucionalmente admissível a expedição de ordem judicial a um provedor de aplicação (art. 5º, VII, Marco Civil da Internet) para fornecimento de dados estáticos – mais especificamente dados e informações de usuários que realizaram buscas por termos específicos no Google – de um grupo não previamente determinado de usuários, sem a devida individualização dos investigados ou qualquer delimitação objetiva do universo de pessoas potencialmente vinculadas aos fatos.

Com efeito, o caso paradigmático que deu origem ao Tema 1.148 de repercussão geral no Supremo Tribunal Federal decorre da investigação do assassinato da vereadora Marielle Franco e de seu motorista Anderson Gomes, ocorrido em março de 2018, na cidade do Rio de Janeiro. Diante das dificuldades enfrentadas para a identificação dos autores do crime, a autoridade policial requereu ao juízo da 4ª Vara Criminal da Comarca do Rio de Janeiro uma ordem judicial dirigida à empresa Google Brasil Internet Ltda., com o objetivo de acessar informações capazes de auxiliar nas investigações. As informações requisitadas e autorizadas são:

"identificação dos IP's ou "DEVICE IDs" que tenham se utilizado do Google Busca (seja através do aplicativo ou sua versão WEB) no período compreendido entre o dia 10/03/2018 a 14/03/2018, para realizar consultas dos seguintes parâmetros de pesquisa: *"MARIELE FRANCO"*; *"VEREADORA MARIELE"*; *"AGENDA VEREADORA MARIELE"*; *"CASA DAS PRETAS"*; *"RUA DOS INVÁLIDOS, 122"* ou *"RUA DOS INVALIDOS""*[10]***[11]***

A autoridade policial visava, portanto, a identificação retroativa de potenciais suspeitos, partindo da premissa de que os autores do crime poderiam ter utilizado a ferramenta de busca para levantar informações relevantes sobre os hábitos da vereadora. A requisição, no

entanto, não individualizava previamente os investigados, tampouco estabelecia critérios objetivos de delimitação do universo de cidadãos potencialmente afetados.

A medida foi deferida pelo juízo da 4ª Vara Criminal da Comarca do Rio de Janeiro, sob o fundamento de que seria razoável e proporcional diante da gravidade do delito investigado e das dificuldades enfrentadas pelas autoridades na identificação dos seus autores. Considerou-se, como hipótese investigativa, que os responsáveis pelo atentado teriam utilizado serviços de busca na internet para planejar a ação criminosa, de modo que a análise de eventuais acessos a determinados termos pesquisados poderia contribuir para a elucidação dos fatos.

Contra a decisão judicial, o Google Brasil impetrou Mandado de Segurança, cuja segurança foi denegada pelo Tribunal de Justiça do Estado do Rio de Janeiro. Na sequência, interpôs Recurso Ordinário em Mandado de Segurança (RMS 71.168/RJ) perante o Superior Tribunal de Justiça, o qual manteve a decisão de origem, determinando o fornecimento dos chamados dados estáticos.

O ponto central dos recursos interpostos pelo Google, que culminaram no Recurso Extraordinária centrou-se, essencialmente, na alegação de que a ordem judicial apresentava caráter genérico e desproporcional, violando o direito fundamental à proteção de dados pessoais de diversos usuários certamente não vinculados à prática criminosa, configurando, segundo a argumentação da empresa, uma típica hipótese de *fishing expedition*. Sustentou-se, ainda, que a decisão carecia de fundamentação adequada e não encontrava respaldo legal expresso, especialmente no que tange ao artigo 22 do Marco Civil da Internet, o qual, segundo a interpretação do recorrente, não autorizaria medidas de requisição tão abrangentes.

A Ministra Rosa Weber, relatora original do caso (hoje aposentada), votou pelo provimento do Recurso Extraordinário n.º 1.301.250/RJ, destacando a centralidade do princípio da legalidade

no contexto dos meios de obtenção de prova no processo penal. Em seu entendimento, medidas como a quebra de sigilo de dados estáticos exigem autorização legal expressa, não sendo admissível, nessa seara, a adoção de "interpretações criativas, aditivas, muito menos contrárias à propria *mens legis*".

A Ministra salientou que, por se tratar de instrumentos que envolvem restrição a direitos fundamentais dos investigados, os meios de obtenção de prova devem observar, de forma estrita, os limites impostos pelo princípio da legalidade, atuando a norma legal como verdadeiro freio às investigações estatais.

"Vê-se, pois, que mesmo os Poderes Executivo e Legislativo compreendem indispensável a existência de lei autorizativa para o emprego dos meios de obtenção de prova, tendo em vista que acarretam graves restrições aos direitos fundamentais dos investigados, tanto assim que existem inúmeras disposições legais nesse sentido."[12]

Nessa perspectiva, cumpre observar o entendimento da Ministra de que os dados estáticos se enquadram no conceito de dados pessoais, conforme art. 5º, I, da Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD):

"Não se mostra relevante o fato de que o Device ID se vincula a um aparelho e não a uma pessoa, pois, mediante engenharia regular, é plenamente possível a identificação de seu proprietário ou usuário. No que diz com o endereço de IP atribuído a um terminal, de igual modo, viável a identificação do usuário, notadamente em razão do dever de fornecimento das portas lógicas."[13]

"Desse modo, tenho para mim, que, inequivocamente, tanto o Device ID quanto o endereço de IP possibilitam, sem qualquer empenho desmedido, a identificação de uma pessoa determinada, a evidenciar, pois, que, de fato, caracterizam dados pessoais. Por conseguinte, atraída para a hipótese a disciplina normativa concernente."[14]

Sendo assim, na visão da Ministra relatora, a quebra do sigilo de dados estáticos submete-se à disciplina jurídica aplicável aos dados pessoais, inclusive quanto à proteção conferida por sua natureza de direito fundamental.

Abrindo a divergência, o Ministro Alexandre de Moraes votou pela constitucionalidade da requisição, desde que observados certos requisitos mínimos de legalidade e proporcionalidade. Para o Ministro, a medida é admissível quando presentes: (i) fundados indícios da ocorrência do ilícito, (ii) justificativa motivada quanto à utilidade dos registros solicitados e (iii) delimitação precisa do período ao qual os dados se referem.

Em sua fundamentação, o Ministro Alexandre de Moraes argumentou que o Marco Civil da Internet admite expressamente exceções à privacidade mediante ordem judicial, com base em seu artigo 10, e que, por analogia, os princípios e limites estabelecidos pela Lei de Interceptação Telefônica podem ser utilizados para reforçar a legitimidade da medida.

O Ministro Cristiano Zanin acompanhou a divergência do Ministro Alexandre de Moraes, mas propôs adendos à tese, enfatizando a necessidade de que a ordem judicial seja adequada e proporcional, e que o acesso aos dados se baseie em "razões que fundamentam uma fundada suspeita", buscando maior alinhamento com os princípios constitucionais.

Por sua vez, o Ministro André Mendonça, em voto-vista, adotou uma posição mais restritiva, embora também divergindo da relatora. Defendeu que a quebra de sigilo não individualizada só seria admissível mediante critérios estritos e objetivos, a fim de evitar hipóiteses de pesca probatória. Propôs requisitos como a especificação do tipo de dado, análise da extensão temporal e espacial da medida, e demonstração da impossibilidade de obtenção da prova por outros meios menos invasivos.

A controvérsia central do Tema 1.148, como já exposto neste artigo, reside na tensão entre duas premissas fundamentais. De um lado, encontra-se a necessidade de assegurar instrumentos eficazes para a investigação de crimes graves e complexos, especialmente em

um cenário digital no qual evidências digitais frequentemente desempenham papel decisivo na formação da convicção das autoridades policiais e do Ministério Público para a construção da *opinio delicti*. De outro, impõe-se a preservação dos direitos fundamentais, com ênfase no direito à proteção de dados pessoais, os quais podem ser gravemente comprometidos quando ordens judiciais genéricas autorizam o acesso a dados de um número indeterminado de usuários, muitos dos quais, certamente, não possuem qualquer relação com o fato investigado. Nesses casos, há o evidente risco de que indivíduos não relacionados aos fatos investigados passem a ser submetidos, ainda que indiretamente, à devassa estatal e à imputação implícita de envolvimento em delitos de extrema gravidade.

V A AMEAÇA DO ESTADO DE VIGILÂNCIA: UMA PERSPECTIVA ORWELLIANA SOBRE A QUEBRA DE SIGILO GENÉRICA E A VIOLAÇÃO À PRESUNÇÃO DE INOCÊNCIA

A discussão sobre a constitucionalidade da quebra de sigilo de dados estáticos de forma genérica, com a possibilidade de atingimento de pessoas no máximo determináveis, transcende a mera análise técnica de dispositivos legais e constitucionais, inserindo-se, na opinião deste autor, em um plano mais amplo de reflexão sobre o modelo de sociedade que se pretende construir e sobre os contornos da relação entre Estado, tecnologia e liberdades individuais em um cenário de crescente digitalização das relações sociais.

Nesse contexto, a obra distópica 1984, de George Orwell, revela-se uma referência crítica de grande relevância para a construção de um juízo de valor social acerca dos riscos associados à concentração de poder informacional nas mãos do Estado. Ao projetar um futuro autoritário marcado pela vigilância irrestrita e pela supressão das liberdades individuais, Orwell fornece uma chave interpretativa para refletir sobre os limites ético-jurídicos do controle estatal no mundo contemporâneo.

Publicado em 1949, o romance descreve a realidade opressiva de Oceania, sociedade fictícia governada pelo onipresente “Grande Irmão” (*Big Brother*), em que o Partido controla todos

os aspectos da vida de seus cidadãos por meio da vigilância constante das “teletelas” e da temida “Polícia do Pensamento”, que punia até mesmo os “crimes de pensamento”. A privacidade é inexistente, a verdade é manipulada, e o objetivo é o controle absoluto.

Orwell, portanto, teve a aptidão de criar um cenário literário paradigmático, capaz de ilustrar, de forma simbólica e crítica, o conceito de Estado de Vigilância, compreendido como uma forma de organização política em que o controle social se realiza por meio da coleta sistemática e permanente de informações sobre os seus cidadãos, com vistas à conformação de comportamentos e à supressão de dissensos.

Nesse contexto, é forçoso reconhecer que a eventual declaração de constitucionalidade de decisões judiciais que autorizam a quebra genérica do sigilo de dados estáticos – como se discute no Tema 1.148 – representaria um avanço particularmente preocupante da sociedade brasileira rumo a um modelo de Estado de Vigilância orwelliano. Ao permitir que o Estado acesse dados pessoais de um número indeterminado de indivíduos, sem a exigência de individualização de suspeitos ou de apresentação de indícios concretos de envolvimento com o fato investigado, institucionaliza-se a prática da devassa estatal indiscriminada.

Tal medida subverte, em sua integralidade, a lógica estruturante das garantias fundamentais no processo penal, notadamente a presunção de inocência, transformando o exercício legítimo de liberdades civis, como a realização de pesquisas na internet sobre eventos de relevância pública, em comportamento potencialmente suspeito. A consequência prática é a erosão dos limites entre vigilância e investigação, e a consolidação de um paradigma em que a mera exposição a determinado conteúdo pode ensejar submissão à persecução penal, mesmo na ausência de qualquer vínculo objetivo com a infração penal apurada.

A prática, como dito, colide frontalmente com o princípio da presunção de inocência, insculpido no art. 5º, LVII, da Constituição Federal, que estabelece que “ninguém será considerado culpado até o trânsito em julgado de sentença penal condenatória”. A quebra de

sigilo genérica, ao submeter um grupo vasto e indeterminado de indivíduos à vigilância estatal e à análise de seus dados pessoais, trata todos, indistintamente, como potenciais suspeitos, a despeito de inexistir contra determinada pessoa qualquer indício de sua participação na atividade criminosa investigada. A investigação deixa de ser uma apuração de fatos direcionada a indivíduos sobre os quais recaem suspeitas fundamentadas, para se tornar uma varredura especulativa.

Em 1984, a lógica investigativa opera sob uma lógica similar. Em Oceania, os cidadãos vivem sob permanente incerteza quanto à vigilância estatal, o que inverte completamente a lógica da presunção de inocência e institui um estado de observação total. Nas palavras do autor:

"Claro que não havia como saber se alguém estava sendo observado em um dado momento. Saber a frequência, ou com qual sistema, a Polícia do Pensamento se conectava a uma determinada escuta era pura adivinhação. Era até possível conceber que eles observavam a todos o tempo todo. Mas, de qualquer forma, eles podiam se conectar à sua escuta sempre que quisessem. Você tinha que viver – e vivia, com um hábito que se tornou instinto – na suposição de que todo som que fazia era ouvido, e, exceto na escuridão, todo movimento era escrutinado."[15]

Em tal configuração, o governo se torna o árbitro soberano, e os direitos fundamentais são vistos como obstáculos à eficiência estatal, e não como sua condição de legitimidade. A quebra de sigilo genérica, dessa maneira, ao permitir que o aparato investigativo estatal vasculhe a vida digital de incontáveis cidadãos sem suspeitas individualizadas, reflete uma lógica policialesca: a suspeição é generalizada, o controle é preventivo e a privacidade é relativizada em nome de uma suposta segurança ou ordem pública. Isso se afasta radicalmente do Estado Democrático de Direito, que se funda na limitação do poder estatal pelos direitos fundamentais e na presunção de que os cidadãos são livres e inocentes até prova em contrário, formada sob o crivo do contraditório e da ampla defesa.

VI CONCLUSÃO

O presente artigo debruçou-se sobre a complexa questão dos limites constitucionais à decretação judicial da quebra de sigilo de dados estáticos em relação a pessoas indeterminadas, objeto do Tema 1.148, de Repercussão Geral, do Supremo Tribunal Federal. Buscou-se analisar criticamente a admissibilidade de ordens judiciais genéricas nesse contexto, confrontando a necessidade de investigação penal na era digital com a imperatividade da proteção aos direitos fundamentais à intimidade, à vida privada e à proteção de dados pessoais, sob a perspectiva adicional dos riscos de um Estado de Vigilância alertados pela teoria Orwelliana.

Conforme demonstrado, a Constituição Federal de 1988 estabelece uma proteção robusta a esses direitos, consagrando-os como cláusulas pétreas e pilares do Estado Democrático de Direito. A inviolabilidade prevista nos incisos X e XII do artigo 5º, reforçada pela recente inclusão da proteção de dados pessoais como direito fundamental autônomo (inciso LXXIX), impõe barreiras significativas à atuação estatal. A relativização dessas garantias, embora possível para fins de persecução penal, não é discricionária e exige, impreterivelmente, ordem judicial específica e concretamente fundamentada, nos termos do artigo 93, IX, da Carta Magna, além de lei válida e constitucional que possibilite o emprego deste meio de obtenção de prova de maneira tão genérica e abrangente.

A análise do Tema 1.148 e do Recurso Extraordinário 1.301.250/RJ revela a profunda controvérsia existente no próprio Supremo Tribunal Federal, com ministros apresentando teses divergentes sobre a possibilidade de ordens genéricas atingirem direitos fundamenyaos de pessoas indeterminadas. Enquanto a relatora original, Ministra Rosa Weber, e o Ministro André Mendonça (com ressalvas) apontaram para a incompatibilidade de tais ordens com o arcabouço constitucional e legal vigente (notadamente o Marco Civil da Internet), outros ministros, como Alexandre de Moraes e Cristiano Zanin, defenderam sua admissibilidade condicionada a determinados requisitos, priorizando a eficácia investigativa.

Contudo, argumentou-se que mesmo as teses que admitem a medida sob condições não afastam o vício de origem: a ausência de individualização e a violação massiva de direitos de terceiros não suspeitos.

A perspectiva Orwelliana, trazida à baila, reforça a gravidade dos riscos associados à quebra de sigilo genérica. A permissão para que o Estado realize varreduras amplas em dados estáticos que, ao fundo, se configuram em dados pessoais de cidadãos não individualizados, sob o pretexto de investigar delitos, assemelha-se perigosamente às práticas de vigilância onipresente descritas na obra fictícia "1984". Tal prática fomenta a pesca probatória, viola a presunção de inocência em larga escala e instaura um *chilling effect* sobre as liberdades individuais, minando a confiança nas instituições e pavimentando o caminho para um controle social excessivo e incompatível com a democracia.

Diante do exposto, conclui-se pela inconstitucionalidade das ordens judiciais genéricas de quebra de sigilo de dados estátivos que atinjam pessoas indeterminadas, ainda que determináveis. É imperativo que o Supremo Tribunal Federal, ao fixar a tese no Tema 1.148, reafirme os limites constitucionais intransponíveis à atuação estatal na era digital, vedando expressamente a quebra de sigilo genérica e resguardando os cidadãos contra a ameaça de um Estado de Vigilância.

REFERÊNCIAS

BIONI, Bruno Ricardo. Proteção De Dados Pessoais-a Função E Os Limites Do Consentimento. 2.a ed., Editora Forense, 2021.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF: Presidência da República, [2024]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 5 maio 2025.

BRASIL. Emenda Constitucional 115, de 10 de fevereiro de 2022. Altera a Constituição

Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais […]. Diário Oficial da União: seção 1, Brasília, DF, p. 2, 11 fev. 2022. Edição extra A. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm. Acesso em: 5 maio 2025.

BRASIL. Lei 9.296, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. Diário Oficial da União: seção 1, Brasília, DF, p. 13777, 25 jul. 1996. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 5 maio 2025.

BRASIL. Lei 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União: seção 1, Brasília, DF, p. 1, 24 abr. 2014. Edição extra. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 5 maio 2025.

BRASIL. Lei 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: seção 1, Brasília, DF, p. 59, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 5 maio 2025.

JR., Aury L. Direito Processual Penal – 22ª Edição 2025. 22. ed. Rio de Janeiro: SRV, 2025. E-book. p.399. ISBN 9788553625673. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788553625673/. Acesso em: 04 jun. 2025.

LEONARDI, Marcel. Fundamentos de direito digital. São Paulo: Thomson Reuters Brasil, 2019.

MASSO, Fabiano del, et al., editores. Marco civil da internet: lei 12,965/2014. Thomson Reuters Revista dos Tribunais, 2014.

NUCCI, Guilherme de S. Curso de Direito Processual Penal – 21ª Edição 2024. 21. ed. Rio de

Janeiro: Forense, 2024. E-book. p.I. ISBN 9786559649280. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786559649280/. Acesso em: 04 jun. 2025.

ORWELL, George. 1984. Tradução exclusiva da Gazeta do Povo. Curitiba: Gazeta do Povo, 2022. Disponível em: https://multimidia.gazetadopovo.com.br/media/info/2022/202209/1984/e-book-1984.pdf. Acesso em: 3 jun. 2025.

RODAS, Sérgio. STF retoma julgamento sobre quebra de sigilo telemático em investigações. Consultor Jurídico (ConJur), 23 abr. 2025. Disponível em: https://www.conjur.com.br/2025-abr-23/stf-retoma-julgamento-sobre-quebra-de-sigilo-telematico-em-investigacoes/. Acesso em: 5 maio 2025.

WIKIPEDIA. Nineteen Eighty-Four. Disponível em: https://en.wikipedia.org/wiki/Nineteen_Eighty-Four. Acesso em: 5 maio 2025.

---

[1] Mestrando em Direito Civil pela Pontífica Universidade Católica de São Paulo (PUC-SP). Pós-graduado em Direito Civil e bacharel em Direito pela Universidade Presbiteriana Mackenzie. Advogado atuante na área de Direito Digital com ênfase na intersecção entre Direito e Tecnologia e solução de conflitos. ORCID: https://orcid.org/0009-0007-9787-3703; Lattes: http://lattes.cnpq.br/9922344673278585

[2] BRASIL. Supremo Tribunal Federal. Voto da Ministra Rosa Weber. Recurso Extraordinário n°. 1.301.250/RJ, Relator: Ministra Rosa Weber, Brasília, 22 set. 2023. Disponível em: https://sistemas.stf.jus.br/repgeral/votacao?texto=5856376. Acesso em: 30 maio 2025.

[3] BRASIL. Supremo Tribunal Federal. Voto da Ministra Rosa Weber. Recurso Extraordinário n°. 1.301.250/RJ, Relator: Ministra Rosa Weber, Brasília, 22 set. 2023. Disponível em:

https://sistemas.stf.jus.br/repgeral/votacao?texto=5856376. Acesso em: 30 maio 2025.

[4] BRASIL. Superior Tribunal de Justiça. Recurso em Mandado de Segurança n. 60.698/RJ. Rel. Min. Rogerio Schietti Cruz. Terceira Seção. Julgado em 26 ago. 2020. Diário da Justiça Eletrônico, 4 set. 2020.

[5] BRASIL. Decreto nº 8.771, de 11 de maio de 2016. Regulamenta a Lei nº 12.965, de 23 de abril de 2014. Diário Oficial da União: seção 1, ed. extra, p. 7, 11 maio 2016. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm. Acesso em: 4 jun. 2025

[6] BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União: seção 1, p. 1, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 4 jun. 2025.

[7] BADARÓ, Gustavo Henrique Righi Ivahy. Processo penal. Rio de Janeiro: Campus; Elsevier, 2012. p. 348.

[8] LIMA, Caio César Carvalho in MASSO, Fabiano del, et al., editores. Marco civil da internet: lei 12,965/2014. Thomson Reuters Revista dos Tribunais, 2014.

[9] BRASIL. Superior Tribunal de Justiça. Agravo Regimental no Recurso Ordinário em Mandado de Segurança n. 71.168/RJ, Relatora: Ministra Laurita Vaz, Relator para o acórdão: Ministro Jesuíno Rissato (Desembargador Convocado do TJDFT), Sexta Turma, julgado em 8 ago. 2023, Diário da Justiça Eletrônico, 30 ago. 2023.

[10] BRASIL. Supremo Tribunal Federal. Voto da Ministra Rosa Weber. Recurso Extraordinário n°. 1.301.250/RJ, Relator: Ministra Rosa Weber, Brasília, 22 set. 2023. Disponível em: https://sistemas.stf.jus.br/repgeral/votacao?texto=5856376. Acesso em: 30 maio 2025.

[11] BRASIL. Supremo Tribunal Federal. Voto da Ministra Rosa Weber. Recurso Extraordinário n°. 1.301.250/RJ, Relator: Ministra Rosa Weber, Brasília, 22 set. 2023. Disponível em: https://sistemas.stf.jus.br/repgeral/votacao?texto=5856376. Acesso em: 30 maio 2025.

[12] BRASIL. Supremo Tribunal Federal. Voto da Ministra Rosa Weber. Recurso Extraordinário n°. 1.301.250/RJ, Relator: Ministra Rosa Weber, Brasília, 22 set. 2023. Disponível em: https://sistemas.stf.jus.br/repgeral/votacao?texto=5856376. Acesso em: 30 maio 2025.

[13] BRASIL. Supremo Tribunal Federal. Voto da Ministra Rosa Weber. Recurso Extraordinário n°. 1.301.250/RJ, Relator: Ministra Rosa Weber, Brasília, 22 set. 2023. Disponível em: https://sistemas.stf.jus.br/repgeral/votacao?texto=5856376. Acesso em: 30 maio 2025.

[14] BRASIL. Supremo Tribunal Federal. Voto da Ministra Rosa Weber. Recurso Extraordinário n°. 1.301.250/RJ, Relator: Ministra Rosa Weber, Brasília, 22 set. 2023. Disponível em: https://sistemas.stf.jus.br/repgeral/votacao?texto=5856376. Acesso em: 30 maio 2025.

[15] ORWELL, George. *1984*. Tradução exclusiva da Gazeta do Povo. Curitiba: Gazeta do Povo, 2022. Disponível em: https://multimidia.gazetadopovo.com.br/media/info/2022/202209/1984/e-book-1984.pdf. Acesso em: 3 jun. 2025. p. 10.