O dever da devida diligência na investigação e persecução penal como direito da vítima de crime de homicídio e investigação contemporânea

Simone Sibilio do Nascimento*

Sumário

Resumo

Este artigo tem como objetivo a análise da compatibilidade de investigação penal tecnológica (ou digital) em crimes graves e em contexto de organização criminosa com os direitos e garantias fundamentais constitucionais, sob a perspectiva do direito da vítima a uma investigação diligente. O tema foi desenvolvido a partir do caso concreto submetido ao Supremo Tribunal Federal (Recurso Extraordinário 1.301.250) em que se discute a constitucionalidade de ordem judicial que determinou a quebra de sigilo telemático de número indeterminado de pessoas. O trabalho está dividido em duas partes. Na primeira parte, abordamos a compatibilidade entre o direito à privacidade e protocolos inéditos adotados em investigação de crime de homicídio, baseados em evidências digitais. Na segunda parte, analisamos a decisão do Superior Tribunal de Justiça sobre a constitucionalidade do art. 22 da Lei 12.965/2014 (MCI) e a interpretação da Ministra Rosa Weber que, no caso concreto, entendeu pela inconstitucionalidade devido à falta de especificidade e clareza da lei. O texto também aborda os possíveis problemas e consequências da decisão para investigações de crimes graves e a proteção dos direitos das vítimas, ressaltando os riscos de ineficiência no dever de proteção à vida e à segurança, que pode resultar em impunidade em um país com altos índices de homicídios.

Abstract

This article aims to analyze the compatibility of technological (or digital) criminal investigation in serious crimes and in the context of criminal organizations with fundamental constitutional rights and guarantees, from the perspective of the victim's right to a diligent

* Promotora de Justiça do Ministério Público do Rio de Janeiro (MPRJ). Mestranda em Teoria do Estado e o Direito Constitucional pela Pontifícia Universidade Católica do Rio de Janeiro (PUC-RJ). Bacharel em Direito pela Pontifícia Universidade Católica do Rio de Janeiro (PUC-RJ). E-mail: sibilo@mprj.mp.br

investigation. The topic was developed based on the specific case submitted to the Federal Supreme Court (Extraordinary Appeal 1.301.250) in which the constitutionality of a court order that ordered the breach of telematics confidentiality of an undetermined number of people was discussed. The work is divided into two parts. In the first part, we address the compatibility between the right to privacy and unprecedented protocols adopted in a homicide investigation based on digital evidence. In the second part, we analyze the decision of the Superior Court of Justice on the constitutionality of art. 22 of Law 12.965/2014 (MCI) and the interpretation of Justice Rosa Weber who, in the specific case, ruled that it was unconstitutional due to the law's lack of specificity and clarity. The text also addresses the possible problems and consequences of the decision for investigations into serious crimes and the protection of victims' rights, highlighting the risks of inefficiency in the duty to protect life and safety, which could result in impunity in a country with high homicide rates.

Palavras-chave: Quebra de sigilo telemático. Privacidade. Intimidade. Marco Civil da internet. Investigação diligente.

Keywords: *breach of telematics confidentiality. Privacy. Intimacy. Civil Framework for the Internet. Diligent investigation.*

1. Introdução

O presente trabalho tem como objetivo a análise da compatibilidade de investigação penal tecnológica (ou digital) em crimes graves e em contexto de organização criminosa com os direitos e garantias fundamentais constitucionais.

O tema será desenvolvido a partir do caso concreto submetido ao Supremo Tribunal Federal (STF) em sede de recurso extraordinário (RE 1.301.250) interposto pelas empresas Google Brasil Internet LTDA e Google LLC contra decisão do Superior Tribunal de Justiça (STJ) que manteve decisão do Tribunal de Justiça do Estado do Rio de Janeiro (TJRJ),[1] que determinou a quebra de sigilo telemático de número indeterminado de pessoas.

A decisão judicial ordenou que a Google fornecesse, com base no artigo 22 do Marco Civil da Internet - Lei 12.965/2014[2] (MCI), a identificação de todos os

[1] O caso concreto se refere à decisão judicial contestada pela empresa Google na investigação dos assassinatos ocorridos no Estado do Rio de Janeiro da vereadora Marielle e Anderson (e homicídio tentado da vítima sobrevivente Fernanda Chaves), em relação aos dois executores identificados, presos, processados e condenados pelo Tribunal do Juri, em outubro de 2024. Na referida investigação foram formulados pedidos inéditos quando ainda não havia suspeitos identificados, buscando identificar autoria através de provas digitais mediante afastamento de sigilo de dados telemáticos que contou com resistência das empresas de aplicação de internet, sobretudo, Google e Facebook. A empresa Google manejou vários mandados de segurança para ser desobrigada a fornecer os dados, sendo eles: STJ - RMS 60.698 (2019/0119654-6) Número Único 0072968-96.2018.8.19.0000, RMS 61.302 (2019/0199132-0) Número único 0016639-30.2019.8.19.0000 E RMS 62.143 (2019/0318252-3) Número único 0035023-41.2019.8.19.0000.

[2] BRASIL. Marco Civil da Internet. Lei 12.964/14. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 26 jun. 2024.

dispositivos que tivessem feito uso de sua ferramenta de busca no período de quatro dias que antecederam o crime de homicídio da vereadora Marielle Franco e de seu motorista Anderson Gomes, utilizando como parâmetros de busca palavras-chave referentes à vereadora para, a partir dos resultados, fazer a conexão com outros filtros investigativos, de modo a identificar os envolvidos no crime que teve repercussão nacional e internacional.

O STF reconheceu repercussão geral ao recurso extraordinário, definindo como tema a ser decidido: "Limites para decretação judicial da quebra de sigilo de dados telemáticos, no âmbito de procedimentos penais, em relação a pessoas indeterminadas" (tema n.º 1148). Até o momento, votaram apenas a Ministra Rosa Weber (relatora), dando provimento ao recurso, e os Ministros Alexandre de Moraes e Cristiano Zanin, ambos mantendo o entendimento das instâncias inferiores. Embora ainda não seja possível, a partir de três votos, apontar uma tendência da Corte nesse julgamento, é importante frisar que a decisão final resultará num precedente importante sobre um tema atual e complexo, com sérias consequências para investigações envolvendo letalidade violenta em contexto de organização criminosa, e outros crimes igualmente graves, o que justifica uma análise mais detida dos argumentos e da proposta de tese apresentados pela relatora – contrariando o entendimento adotado pelo STJ, pelo TJRJ e pelos demais ministros que votaram.

O trabalho está dividido em duas partes. Na primeira, há a abordagem de protocolos inéditos adotados em investigação de crime de homicídio, baseados em evidências digitais. Na segunda parte, analisa-se a decisão do Superior Tribunal de Justiça (STJ) sobre a constitucionalidade do art. 22 da Lei 12.965/2014 (MCI) e a interpretação da Ministra Rosa Weber que, no caso concreto, entendeu pela inconstitucionalidade devido à falta de especificidade e clareza. O texto também aborda os possíveis problemas e consequências da decisão para investigações de crimes graves e a proteção dos direitos das vítimas, ressaltando os riscos de ineficiência no dever de proteção à vida e à segurança, que pode resultar em impunidade em um país com altos índices de homicídios.

2. Investigação de crimes graves e a privacidade: até onde podem ir as decisões judiciais?

O tema referenciado joga luz no vetusto debate acadêmico e jurisprudencial acerca da ponderação, de um lado, dos direitos e garantias fundamentais, notadamente, o direito à privacidade e à intimidade, previstos no artigo 5º, inciso X, da Constituição Federal,[3] e artigo 21 do Código Civil[4] e, de outro bordo, do princípio da plenitude da tutela da vida humana e da segurança, bem como o direito da ampla defesa das

[3] Art. 5º, inciso X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

[4] Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

vítimas (diretas e indiretas)[5] da letalidade violenta e organizada. A importância do direito fundamental à privacidade e à intimidade no Brasil é amplamente reconhecida acadêmica e jurisprudencialmente, sobretudo a partir da aprovação da Lei Geral de Proteção de Dados (LGPD), em 2018, e da promulgação da Emenda Constitucional n. 115, em 2022, que assegura, "nos termos da lei o direito à proteção dos dados pessoais, inclusive nos meios digitais" (art. 5º, LXXIX, CF). O mesmo, contudo, não se pode dizer quanto ao direito das vítimas de crimes violentos. Há certa assimetria na abordagem dos direitos das vítimas e dos réus, seja na fase de investigação, seja em processos judiciais, sobretudo quanto ao direito à ampla defesa, geralmente associado aos réus e investigados. No entanto, como recordam Mazzuoli e Oliveira (2024: 254), "[o] art. 25(1) da Convenção Americana sobre Direitos Humanos, que é base convencional para obrigação positiva dos Estados de investigar, processar e punir violações criminosas a direitos humanos, trata expressamente da *proteção judicial* das vítimas", direito que "guarda perfeita simetria com o art. 5º, LV, da Constituição Federal que assegura a *ampla defesa judicial* das vítimas da criminalidade". De acordo com os autores (2024: 256):

> A leitura integral do conteúdo do princípio da ampla defesa, que confere embasamento à ampla fundamentação da pretensão acusatória e ao exercício da dimensão material daquele mesmo princípio, contempla a necessidade de sua aplicação mediante a admissão de meios de acesso das vítimas a instrumentos de proteção e restauração dos seus direitos humanos e fundamentais indevidamente violados.
>
> Quando a Constituição Federal assegura aos litigantes o exercício no plano judicial e no plano administrativo de todos os meios inerentes à ampla defesa, não se limita a referendar a utilização de ferramentas legais de resistência do titular de um direito em face do exercício do direito de ação de um terceiro. A extensão dos meios para a efetividade do princípio da ampla defesa compreende, ao revés, o emprego *ativo* de medidas judiciais e extrajudiciais adequadas à proteção do direito em questão, sob pena de defeituosa ineficácia do princípio fundamental.

Para uma ponderação adequada entre os direitos em conflito potencial no caso abordado neste trabalho, é importante destacar que a proteção pretendida pelo provedor de pesquisa não envolve, a rigor, o direito à privacidade dos usuários (que sequer são identificados), mas o interesse econômico da empresa, na medida em que, como uma das maiores *big datas* no mundo, ao dificultar acesso a dados

[5] A palavra vítima adotada neste ensaio abrange a vítima direta e vítima indireta, nos termos do conceito proposto pela vitimologia, assim como pela resolução 34/40 da ONU, segundo a qual o termo "vítima" inclui também os familiares próximos ou dependentes da vítima direta e as pessoas que tenham sofrido danos ao intervir para prestar assistência às vítimas em perigo ou para impedir a vitimização.

específicos, cria a percepção que está comprometida com a proteção de dados pessoais e, assim, fortalece a confiança da população na empresa. Esse mecanismo se reflete favoravelmente no mercado e valoriza suas ações. No entanto, não se pode olvidar que ao fazer a coleta dados e controlá-los, utiliza-os para aprimorar seus serviços e direcioná-los para incremento de suas atividades.

Em artigo que versa sobre capitalismo de vigilância e perspectiva para uma civilização de informação, Shoshana Zuboff, ao tratar da lógica emergente de acumulação hegemônica, ressalta justamente a postura da Google, considerada por muitos como a pioneira do *big data* e, em razão disso, a pioneira de acumulação mais ampla a praticar o que chama de capitalismo de vigilância (Zuboff 2018: 25), com práticas de coleta e utilização de dados pessoais.

Zuboff (2018: 31-32) evidencia como a Google coleta uma quantidade massiva de dados pessoais sem o conhecimento explícito do usuário, sem transparência nas práticas de coleta e uso de dados, e utiliza os dados coletados para fins lucrativos, muitas vezes sem o consentimento informado dos usuários:

> [...] a Google coloca a inovação a frente de tudo e resiste a pedir permissão. A empresa não pergunta se pode fotografar casas para os bancos de dados, ela simplesmente pega o que quer, então esgota seu adversário no tribunal ou eventualmente concorda em pagar multas que representa um investimento negligenciável para um retorno significativo [...] a *big data* é constituída pela captura de Small Data, das ações e discursos mediados por computador, de indivíduos no desenrolar da vida prática. Nada é trivial ou efêmero em excesso par essa colheita: as curtidas do Facebook, as buscas no Google, e-mails, textos, fotos, músicas e vídeos, localizações, redes, compras, movimentos, todos os cliques, palavras com erros ortográficos, visualizações de páginas e muitos mais. Esses dados são adquiridos, tornados abstratos, agregados, analisados, embalados, vendidos, analisados mais e mais e vendidos novamente.

A autora pontua que, para a Google, as subjetividades são convertidas em objetos que orientam o subjetivo para a mercantilização, trata as pessoas como fontes de extração de dados e alvos finais das ações que os dados produzem, mas que a indiferença formal se torna evidente, por exemplo, na agressividade com que a Google aplica no modelo *Street View*, incursionando em territórios legal e socialmente não protegidos, até que um dia possa encontrar resistência, normalmente através de denúncias (Zuboff, 2018 p. 34).

Assim, na visão da autora, essa forma de extrair dados se resume na:

> [...] ausência de reciprocidades estruturais entre a empresa e suas populações. Esse fato sozinho separa a Google, bem como empresas que participam dessa lógica de acumulação, da narrativa histórica das democracias de marcado ocidentais. [...] Essa independência estrutural das populações por parte da empresa é de importância excepcional à luz da relação histórica entre o capitalismo de mercado e a democracia. (Zuboff 2018: 36-38).

O capitalismo de vigilância, portanto, se qualifica como uma nova lógica de acumulação, como uma nova política e relações sociais que substituem os contratos, o Estado de direito e a confiança social pela soberania do *Big Other*, em que a população, ou não possui, ou possui de forma muito atenuada a gestão de sua privacidade porque o *capitalismo de vigilância prospera na ignorância do público* (Zuboff 2018: 49).

Dessa forma, num cenário em que se pretenda a responsabilização dos autores de crimes violentos, praticados em contexto de organização criminosa, em que a elucidação dependa de dados monopolizados por empresa de aplicação de internet, que opera na lógica do capitalismo de vigilância, o direito das vítimas diretas (e de toda sociedade desfalcada pela perda do defensor dos direitos humanos) deve prevalecer diante dos interesses econômicos da empesa de aplicação de internet, que costuma escamotear seus reais interesses sob o manto da privacidade e intimidade dos usuários dos seus produtos e serviços.

Neste sentido, a análise do tema n.º 1148 se mostra relevante na medida em que o Brasil é o país que mais mata no mundo, liderando o ranking mundial de homicídios em números absolutos, de acordo com dados do Estudo Global sobre Homicídios, divulgado pela ONU.[6] Brasil, Nigéria, México, Índia e Estados Unidos respondem por 33% dos homicídios mundiais. Entre as 35 cidades com maior taxa de homicídios, seis estão no Brasil, segundo dados divulgados pelo Observatório de Homicídios do Instituto Igarapé[7]. Em 2017, o Brasil alcançou a marca histórica de 31,6 mortes para cada 100 mil habitantes[8]. Já o índice de elucidação dos homicídios não guarda qualquer simetria com o alto índice de crimes, variando entre 5% e 8% de elucidação. Vale dizer, há um total descompasso entre o número de homicídios com o seu reflexo no Sistema de Justiça. Ademais, mesmo nos casos em que há conclusão das investigações, os quais se inserem na taxa de 5% a 8%, muitos processos não culminam em condenação.

Não se pode perder de vista que, se por um lado, no sistema de justiça brasileiro, os tribunais possuem legitimidade para impor suas orientações para gerações futuras

---

[6] DW. **Brasil lidera ranking de homicídios no mundo, mostra estudo da ONU**. Disponível em: <https://noticias.uol.com.br/ultimas-noticias/deutschewelle/2023/12/08/brasil-lidera-ranking-de-homicidios-no-mundo-mostra-estudo-da-onu.html>. Acesso em: 24 jun. 2024.

[7] Instituto Igarapé. **Observatório de Homicídios**. 2021. Disponível em: <https://igarape.org.br/temas/seguranca-publica/observatorio-de-homicidios/>. Acesso em: 10 mar. 2023.

[8] CERQUEIRA *et al*. Atlas da violência. São Paulo: FBSP, 2021

(criando os precedentes), e para afastar leis elaboradas pelo Poder Legislativo, por outro lado, a lei em vigor gera expectativa de seu cumprimento. Assim, na criação de um precedente judicial há que se observar o ônus da devida fundamentação e a realidade de um país com elevado índice de assassinato de pessoas e baixíssimo índice de elucidação da autoria.

A humanidade vivencia o momento da era das comunicações, dos meios digitais, da velocidade da informação inigualável, onde o uso da tecnologia, se melhora a qualidade de vida, também é utilizado para prática de crimes e desfazimento de provas.

É incontornável, diante da realidade criminal no Brasil, que haja uma reação eficiente por parte do sistema de justiça, através das interpretações e precedentes judiciais face à legislação aprovada pelo Poder Legislativo, com estabelecimento de métodos e estratégias consentâneos com a modernidade tecnológica, sob pena de se impor aos atores que fazem parte do sistema judicial métodos da era analógica enquanto o crime organizado caminha a passos largos pela era da conectividade, de modo que a elucidação de crimes não é mais compatível com os meios tradicionais e retrógrados de investigação penal.

3. A tese da Ministra Rosa Weber

O tema n.º 1148 do STF trata dos limites para decretação judicial da quebra de sigilo de dados telemáticos em relação a pessoas indeterminadas e, na origem, teve como fato gerador recurso contra decisão do Juízo de Direito da 4ª Vara Criminal da Comarca da Capital/RJ que determinara às duas empresas o fornecimento da identificação dos *IPs* ou "*DEVICE IDs*" que tenham se utilizado do Google Busca (seja através do aplicativo ou sua versão *WEB*) no período compreendido entre os dias 10/03/2018 e 14/03/2018, para realizar consultas dos seguintes parâmetros de pesquisa: "Marielle Franco", "Vereadora Marielle", "Agenda Vereadora Marielle", "Casa das Pretas", "Rua dos Inválidos, 122" e "Rua dos Inválidos".

Essa investigação refere-se aos homicídios ocorridos no dia 14 de março de 2018, na cidade do Rio de Janeiro, da vereadora Marielle Franco e de seu motorista, bem como de sua assessora, este na forma tentada, onde restou descortinado que a vítima principal desejada era a vereadora, ativista na defesa dos direitos humanos, crimes cometidos em razão da defesa das causas das minorias e das pessoas com vulnerabilidades, inclusive vulnerabilidades sobrepostas. Crimes com repercussão para além-fronteiras do Brasil.

No bojo da apuração, após esgotados todos os meios protocolares e tradicionais de investigação, dada a ausência de vestígios ululantes e sem identificação de suspeitos, foram manejadas, de forma inédita, medidas cautelares de quebra de sigilo telemático visando à identificação dos envolvidos.

Alguns pedidos formulados no processo utilizaram a técnica de rastreio de geoposicionamento de dispositivos, para que a empresa Google fornecesse a

identificação dos dispositivos (apenas dados registrais ou metadados)[9] que trafegaram em pontos específicos, em dias e horários delimitados e em coordenadas geográficas individualizadas no dia do crime (as coordenadas geográficas e todas as demais informações delimitadas do pedido foram fornecidas às empresas de aplicação de internet (Google, Appel, Microsoft).[10] Dito de outro modo, a partir de pontos específicos, com coordenadas delimitadas e horários determinados na decisão judicial, a empresa deveria fornecer as *Google accounts*, ou *devices*, ou *Apple accounts*, ou *iClouds accounts* que transitaram nas coordenadas geográficas e nos horários determinados, absolutamente restritos. Esses dados foram identificados por imagens de câmeras de segurança coletadas em que se identificou o veículo clonado com os executores se deslocando para a empreitada criminosa.

No que tange ao pedido que ensejou o tema de repercussão geral e que será analisado mais detidamente, a decisão judicial questionada pela Google Brasil Internet Ltda. e Google LLC, com já dito acima, determinou a quebra do sigilo de dados, com o objetivo de identificar *IPs* e *Device IPs* de um conjunto não identificado de pessoas que, em período determinado, fizeram buscas por palavras-chave.

As resultantes desse pedido não devolveriam conteúdo, tampouco dados sensíveis,[11] apenas um código referente ao dispositivo, que somente a empresa saberia a vinculação da propriedade ou posse, e, a partir de outros filtros, com novas autorizações judiciais, o pedido poderia ser ampliado, inclusive com dados de conteúdo.

Exatamente por isso, e com base na lei autorizativa do Marco Civil da Internet, os requerimentos foram devidamente fundamentados e regularmente deferidos nas três instâncias que julgaram o caso. Os argumentos jurídicos apontados pela Google em seus recursos foram basicamente os seguintes: 1) ausência de base constitucional e legal para quebra de sigilo genérica e aleatória, sem a individualização dos alvos e imputação de infração penal, a ensejar a violação do devido processo legal, do princípio

[9] **Metadados**, ou **Metainformação**, são dados sobre outros dados. Um item de um metadado pode dizer do que se trata aquele dado, geralmente uma informação inteligível por um computador. O World Wide Web Consortium – W3C define metadados como informação sobre objetos da Web compreensível por máquinas. A ênfase é no processamento automático, mas falta melhor especificação do tipo e finalidade das informações sobre os objetos da Web. Dempsey e Heery (1997, p. 5) conceituaram metadados como "dados associados com objetos que desoneram os usuários potenciais de ter conhecimento completo antecipado da existência e características desses objetos". Agora o foco concentra-se na finalidade: o metadado é, de certa forma, uma "economia" informacional. GillilandSwetland (2000, p. 1) adotou uma definição abrangente: metadado é "a soma total do que pode ser dito sobre algum objeto informacional em algum nível de agregação". Fonte: <https://brapci.inf.br/index.php/article/download/11673>, ***in*** METADADOS DIGITAIS: revisão bibliográfica da evolução e tendências por meio de categorias funcionais, por Luiz Fernando de Barros Campos

[10] Esses dois pedidos foram acolhidos integralmente tanto pelo Juízo de piso, Tribunal de Justiça do Rio de Janeiro e em razão disso a empresa Google impetrou mandado se segurança com respectivo recurso em mandado de segurança: **RMS 61.302 e RMS 62.143,** repita-se, ambos referentes a informações com base em coordenadas geográficas de dispositivos e apenas metadados a serem fornecidos.

[11] Os dados sensíveis, conforme definidos pela Lei Geral de Proteção de Dados (LGPD), são informações pessoais que revelam aspectos íntimos da vida de um indivíduo. Isso inclui dados sobre origem racial ou étnica, convicções religiosas, opiniões políticas, filiação a sindicatos, informações genéticas, dados biométricos, saúde ou vida sexual, artigo 5, inciso II da LGPD.

da presunção de inocência, da privacidade, do direito de acesso à informação e da liberdade de comunicação; 2) ausência de fundamentação adequada da decisão que determinou a quebra do sigilo; 3) inobservância do princípio da proporcionalidade.

A terceira seção do STJ, por maioria de votos (vencido o Ministro Sebastião Reis Júnior), negou provimento ao recurso das empresas e entendeu que o pedido encontra guarida no ordenamento jurídico para autorizar a quebra de sigilo com base em busca por palavras-chaves, e que a regra dos artigos 22 e 23 do Marco Civil da Internet prevê tal possibilidade, coadunando-se com as leis vigentes, sem que seja malferido o princípio do devido processo legal, da presunção de inocência, da privacidade e da liberdade de comunicação. Para o tribunal, basta a presença dos requisitos do artigo 22 do Marco Civil da Internet, que não exige a identificação de pessoas suspeitas a serem investigadas, sob pena de se esvaziar o propósito da lei.

Ao aportar a questão ao STF,[12] a Ministra Rosa Weber, de forma diversa do entendimento do STJ, entendeu que (item 46 do voto):

> Em suma: seja pela inexistência de lei própria, clara e precisa associada à ausência de normativo que atenda os princípios e as obrigações decorrentes do direito fundamental à proteção de dados pessoais (CF, art. 5º, LXXIX), seja pela inadmissibilidade de devassa indevida sobre o direito fundamental à privacidade (CF, art. 5º, X) de pessoas sobre as quais ausentes quaisquer suspeitas da prática de delitos previamente determinados, não se mostram viáveis ordens genéricas e não individualizadas de fornecimento dos números de *IP's* e *Devices ID's* de usuários que tenham realizado determinadas pesquisas em provedores de aplicação.

E, ao ver da magistrada, inexiste lei que autorize ordens de caráter mais abrangente a impor o fornecimento de endereços de *IPs* e *Devices IDs* de usuário que tenham pesquisado termos específicos em provedores de aplicação, tampouco inocorrente a possibilidade de invocação da disciplina normativa do Marco Civil da Internet para legitimar tais providências, ao mesmo tempo em que não se pode invocar o Marco Civil da Internet pois não contém regramento mínimo para salvaguarda do direito à proteção de dados pessoais. A Ministra propôs, então, a seguinte tese:

> À luz dos direitos fundamentais à privacidade, à proteção dos dados pessoais e ao devido processo legal, o art. 22 da Lei 12.965/2014 (Marco Civil da Internet) não ampara ordem judicial genérica e não

[12] Recurso Extraordinário n.º 1.301.250. Repercussão Geral, tema STF n.º 1148. Não houve julgamento final, em razão do pedido de vista do Ministro André Mendonça. Até a data de envio deste texto (10.01.2025), o feito foi retirado de pauta sem nova data designada. Os votos dos Ministros Alexandre de Moraes e Cristiano Zanin ainda não foram disponibilizados.

> individualizada de fornecimento dos registros de conexão e de acesso dos usuários que, em lapso temporal demarcado, tenham pesquisado vocábulos ou expressões específicas em provedores de aplicação.

A Ministra relatora entendeu que o artigo 22 do MCI, conquanto possa ser aplicado de modo válido e legítimo para a maior parte das situações (*not facially unconstitutional*), se mostra inconstitucional por vagueza quando aplicado à situação particular, em que não for indicado grupo de pessoas individualizado e se pede o fornecimento dos números de *IPs* e *Devices IDs* de usuários que tenham realizado determinada pesquisa em provedores de aplicação (*unconstitutional as applied*), pois não atende o comando constitucional de especificidade, clareza e precisão, vale dizer, embora o artigo 22 do MCI seja constitucional, a sua aplicação nesses casos apontados em concreto seria inconstitucional.[13]

Não se pode negar que a repercussão geral conferida pelo STF a esse tema não apenas resolve o caso concreto, com impacto amplo e relevante, como também permite contribuir para a construção de um sistema jurídico coerente e previsível, na medida em que há diversos casos similares a esse, nos quais se tornou comum empresas de tecnologia ou provedoras de serviços na internet se recusarem a fornecer os dados requeridos judicialmente sob o argumento de proteção à privacidade, à intimidade e ao devido processo legal de terceiras pessoas.

Ocorre que as decisões desafiadas pela Google no caso em referência não impõem qualquer violação da intimidade e da privacidade de número indeterminado de pessoas, pois dizem respeito a "metadados" (dados estáticos), sem qualquer identificação do usuário, preservando-se o caráter anônimo e sem identificação do conteúdo.

Além de não malferir direitos atinentes à intimidade ou à privacidade, o resultado da informação é recebido pela autoridade judicial, que irá determinar a inutilização dos dados (sem exposição do usuário), caso verifique que não guardam relação com a investigação, havendo perfeita compatibilidade com controle judicial e possibilidade de auditagem.

A medida era (no início da investigação) absolutamente necessária e pertinente porque, a partir da conjugação dos dados fornecidos, seria possível estabelecer uma interseção dos pontos por onde passaram os *devices*, e, com lastro nessas coincidências e convergências, tornaria plausível a análise dos dados consolidados, confrontando os dados cadastrais e o conteúdo armazenado nos sistemas operacionais respectivos e, dessa forma, num momento subsequente e com novas decisões judiciais, possibilitando a identificação dos suspeitos.

[13] Minuta de voto em plenário virtual de 22.09.2023 da Ministra Relatora Rosa Weber.

Ainda que assim não fosse, conforme constou da decisão do STJ, os direitos à privacidade e à intimidade , por não serem absolutos, admitem restrição quando em jogo proteção de outros direitos igualmente relevantes para a comunidade, sendo possível afastar a proteção diante de circunstâncias que denotem a existência de interesse público de significativa importância, invariavelmente por meio de decisão proferida por autoridade judicial competente, suficientemente fundamentada, na qual se justifique a necessidade da medida para fins de investigação criminal ou de instrução processual criminal.

A tese proposta pela relatora parece partir de uma interpretação equivocada ao exigir individualização de pessoas a serem alvo da medida, fazendo por vias transversas uma vinculação ao art. 2º da Lei n. 9.296/1996[14] (interceptação telefônica) que não se aplica ao caso, pois o que se quer são dados registrais com previsão no MCI (para o qual não se exigem indícios de autoria) e não na lei de interceptação, dados estes relacionados à identificação de aparelhos – não necessariamente de pessoas – utilizados por usuários.

Há, portanto, uma distinção conceitual entre a quebra de sigilo de dados armazenados e a interceptação do fluxo de comunicações. Segundo o entendimento do STF, *mutatis mutandis*, "não se pode interpretar a cláusula do artigo 5º, XII, da CF, no sentido de proteção aos dados enquanto registro, depósito registral. A proteção constitucional é da comunicação de dados e não dos dados" (HC n. 91.867/PA, Rel. Ministro Gilmar Mendes, DJe 20/9/2012).

Dessa forma, o procedimento de que trata o art. 2º da Lei n. 9.296/1996, cujas rotinas estão previstas na Resolução n. 59/2008 (com alterações ocorridas em 2016), do CNJ, as quais regulamentam o art. 5º, XII, da CF, não se aplica a procedimento que visa a obter dados estáticos armazenados em servidores e sistemas informatizados de um provedor de serviços de internet.

Não se mostra razoável, portanto, exigir requisitos de lei que não se aplica ao caso, pois é o MCI que rege a matéria e que não prevê, dentre os requisitos que estabelece para a quebra do sigilo, que a ordem judicial especifique previamente as pessoas objeto da investigação ou demonstre que a prova da infração (ou da autoria) possa ser realizada por outros meios.[15]

---

[14] BRASIL. Interceptação Telefônica. Lei 9.296/96. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l9296.htm>. Acesso em: 26 jun 2024.

[15] Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o **fornecimento de registros de conexão ou de registros de acesso a aplicações de internet**.
Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade:
I - Fundados indícios da ocorrência do ilícito;
II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e
III - período ao qual se referem os registros.
Art. 23. Cabe ao juiz tomar as providências necessárias à garantia do sigilo das informações recebidas e à preservação da intimidade, da vida privada, da honra e da imagem do usuário, podendo determinar segredo de justiça, inclusive quanto aos pedidos de guarda de registro.

Em complemento, o art. 10, parágrafo único, do MCI determina a observância da privacidade e da intimidade, cujo balizamento será feito pelo juiz,[16] sendo equivocado alegar (como constou do voto) larga margem de discricionariedade do juiz de primeiro grau para aferir esse balizamento, até porque, no ordenamento jurídico brasileiro, se o juiz pode declarar a inconstitucionalidade de uma lei e afastá-la na sua inteireza, com muito mais razão pode pontuar os balizamentos legais para determinar o afastamento do sigilo telemático.

Dessa forma, a tese proposta pela Relatora cria um precedente demasiado restritivo para o art. 22 da lei 12.965/14, ao exigir que a decisão de afastamento de sigilo informacional (sigilo de dados) tenha que, obrigatoriamente, indicar e identificar previamente os "alvos" ou pessoas da investigação suspeitas de cometer o ilícito investigado – contrariando a decisão do Congresso Nacional, que expressamente tratou do tema sem a referida exigência.

Sobre o cabimento do pedido e a perfeita compatibilidade do pedido com o ordenamento jurídico, vale citar Aras (2023), que defende que tanto o cerco digital (pesquisas com base em coordenadas geográficas) como as buscas digitais de autoria por pesquisas terminológicas (de que trata especificamente o tema 1148) não são regidos pela lei 9296/96, tampouco pela lei que versa sobre crime organizado (lei 12.850/2013), mas a conjugação desses dispositivos com os artigo 7º, 10, 22 e 23 do Marco Civil da Internet propicia a base jurídica adequada para viabilizar o deferimento dos pedidos:

> Uma técnica semelhante ao geofence, de busca de palavras-chave (*keyword search history warrants*) também tem sido usada pela Polícia e pelo Ministério Público em crimes graves. A identificação de seletores inseridos em buscadores digitais permite identificar indícios de envolvimento de um usuário de Internet em um crime informático ou em um crime comum. Pesquisas sobre venenos, armas e outros métodos de matar, assim como buscas sobre dados pessoais da vítima, seus hábitos, seus trajetos e laços, numa certa janela de tempo, nas proximidades da data da ocorrência do crime, podem ligar esse usuário de Internet ao fato sob investigação.

[16] Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, deve mater. à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º § 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º

> O acesso a esse registro de buscas em aplicativos como o Google deve se dar mediante ordem judicial, quando uma determinada conta (uma *Google account*, por exemplo) estiver logada durante a pesquisa, ou mediante acesso físico a dispositivos móveis (celulares, iPads etc.) ou a computadores pessoais do suspeito, ou ainda mediante a identificação do *IP* específico de conexão ao serviço.
>
> (...)
>
> A lógica é simples. Embora qualquer pessoa possa ter tido a curiosidade de pesquisar o nome ou a agenda da vereadora Marielle Franco em algum momento de sua vida parlamentar, a busca por esses termos – relacionados a outros que remetem ao lugar onde se iniciou a perseguição da vítima (Rua dos Inválidos, na Lapa) até a sua execução – tem grande importância para a identificação de autoria, quando eles estiverem referenciados no tempo. Isto é, a descoberta de que o usuário de um certo número *IP* ou de uma certa *Google Account* realizou pesquisas sucessivas sobre essas palavras entre os dias 10 e 14 de março de 2018, sendo este último a data dos homicídios, pode seguramente levar à descoberta da autoria do crime. Desta correlação entre conteúdo e coordenadas temporais se extraem a justa causa e a determinabilidade (*particularity*) da medida especial de investigação, sempre dependente de autorização judicial motivada e de cautelas de proteção de dados pessoais, nos termos do art. 2º, inciso II; do art. 3º, incisos II e III; e do art. 23 do MCI.[17]

O voto da relatora parece padecer de outro equívoco, ao deixar de analisar a ausência de legitimidade da Google para questionar a decisão do STJ, pois a empresa seria apenas a destinatária da ordem de quebra do sigilo informacional, desprovida de legitimidade para a defesa da privacidade de seus usuários,[18] sendo temerário que o interesse econômico de uma empresa possa servir como gatilho para um precedente que, se mantido, pode impactar na elucidação de investigações de graves crimes.

É importante frisar que a Corte Interamericana de Direitos Humanos (Corte IDH) tem reiteradamente enfatizado a importância de investigações criminais que sejam conduzidas de maneira eficiente e diligente. Em várias de suas decisões, a Corte IDH tem estabelecido parâmetros claros para garantir que os Estados cumpram suas

[17] ARAS, Vladimir. Cerco digital ("geofence") e varredura terminológica: balizas constitucionais e legais. In: SALGADO, Daniel de Resende; BECHARA, Fábio Ramazzini; DE GRANDIS, Rodrigo (Coord.). 10 anos da Lei das Organizações Criminosas: aspectos criminológicos, penais e processuais penais. São Paulo: Almedina, 2023. p. 655-656

[18] Vide idêntico questionamento no Tribunal de Apelações do Estado de Nova Iorque (nos EUA) decidiu que o Facebook não tinha legitimidade para contraditar uma ordem judicial que requisitava informações sobre as contas de 381 usuários. Por 5 votos a 1, a Corte decidiu que somente os alvos da investigação poderiam se insurgir contra a ordem. O caso foi catalogado como In re: 381 Search Warrants Directed to

obrigações de investigar violações de direitos humanos de forma adequada. E o Brasil se obrigou a cumprir suas decisões por meio do decreto n.º 4.463/2002, reconhecendo a jurisdição contenciosa da Corte.

Além disso, o artigo 68 da CADH estabelece que os Estados-parte devem cumprir as decisões da Corte em todos os casos em que forem partes, razão pela qual as decisões da Corte IDH devem ser utilizadas, inclusive pelo STF, como referência para fortalecer a proteção dos direitos humanos no Brasil.

À guisa de exemplo, citamos o caso Da Silva e outros vs. Brasil, em que a Corte IDH considerou o Brasil internacionalmente responsável pela falta de devida

---

Facebook Inc, New York State Court of Appeals, No. 16. Ver notícia publicada em 04.04.17 sobre o julgamento, acessível em: http://www.reuters.com/article/us-facebook-new-york-idUSKBN1762MY.

A respeito do tema, a título meramente exemplificativo, confira-se:

Facebook e Cambridge Analytica: sete fatos que você precisa saber. Disponível em: <https://www.techtudo.com.br/noticias/2018/03/facebook-e-cambridge-analytica-sete-fatos-que-voce-precisa-saber.ghtml>. Acesso em: 24 jun. 2024.

SUPER. **74% dos usuários do Facebook não sabem como seus dados são usados**. Disponível em: <https://super.abril.com.br/tecnologia/74-dos-usuarios-do-facebook-nao-sabem-como-seus-dados-sao-usados/>. Acesso em: 24 jun. 2024.

Vide relação apresentada na Manifestação final do MPRJ p.p. 26 até 31: **UNITED STATES V. WILSON (2015):** Nesse caso, as autoridades investigaram um site de pornografia infantil e solicitaram um mandado de busca para a google a fim de obter informações de identificação pessoal e endereços ip de usuários que acessavam o site. a google forneceu as informações solicitadas, que ajudaram as autoridades a identificar e prender um indivíduo que estava acessando o site.

PEOPLE V. LASSITER (2015): As autoridades investigaram um assassinato relacionado a gangues em chicago e solicitaram ao google informações sobre o endereço ip e o nome do assinante de um endereço de e-mail. A google forneceu as informações solicitadas, que ajudaram as autoridades a identificar e prender um indivíduo suspeito de estar envolvido no crime.

UNITED STATES V. ACKERMAN (2017): As autoridades investigaram um site de distribuição de drogas e solicitaram um mandado de busca para a google a fim de obter informações de identificação pessoal e endereços ip de usuários que acessavam o site. O google forneceu as informações solicitadas, que ajudaram as autoridades a identificar e prender um indivíduo suspeito de estar envolvido na distribuição de drogas.

STATE V. LIAO (2018): As autoridades estavam investigando a posse e distribuição de pornografia infantil e solicitaram ao google informações sobre os endereços e IPs dos usuários que acessavam um determinado site. O google forneceu as informações solicitadas, que ajudaram as autoridades a identificar e prender um indivíduo suspeito de estar envolvido na posse e distribuição de pornografia infantil.

"Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º."

"Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet.

Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade:

I – fundados indícios da ocorrência do ilícito;

II – justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e

III – período ao qual se referem os registros."

Vide decisão da ***Corte de Apelação U.S. vs Jones*** onde se analisou formas de vigilância de longo prazo e que poderiam proporcionar a violação de uma expectativa razoável de privacidade, totalmente inadequadas ao caso concreto.

diligência no processo penal iniciado em decorrência do homicídio de um brasileiro, trabalhador rural, em 1997, pois seria possível, no caso concreto, identificar vários fatos que refletiam a falta de devida diligência na investigação do caso:

> 70. A Corte recorda que a falta de diligência tem como consequência que, à medida do transcurso do tempo, diminuem as possibilidades de obter e apresentar provas pertinentes que permitam esclarecer os fatos e determinar as correspondentes responsabilidades, de modo que os operadores de justiça contribuem para a impunidade.90 Conforme se depreende do próprio reconhecimento de responsabilidade, foram as falhas cometidas pelo Estado no curso do processo penal que levaram à impunidade do caso em questão.
>
> 71. Diante do exposto, a Corte conclui que o Estado não cumpriu o seu dever de devida diligência no curso do processo penal iniciado em decorrência do homicídio de Manoel Luiz da Silva. Portanto, o Brasil é responsável pela violação dos direitos às garantias judiciais e à proteção judicial, contidos nos artigos 8.1 e 25.1 da Convenção Americana, em relação ao seu artigo 1.1, em detrimento de Josefa Maria da Conceição, Manoel Adelino de Lima e Edileuza Adelino de Lima.[19]

A vítima, seja direta, seja indireta,[20] possui direito à verdade, à memória, à justiça e à reparação, razão pela qual se mostra imperiosa uma investigação eficiente e diligente por parte do Estado Brasileiro, de modo a punir os culpados por crimes de homicídio, crime mais grave no ordenamento jurídico brasileiro, uma vez que a vida é a fonte de todos os direitos. E no âmbito do próprio STF, em sede de julgamento do *Habeas Corpus* 104410/RS, também se estabeleceu a necessidade da proteção eficiente do direito à vida, sendo indene de dúvida que, para uma proteção integral do direito à vida, há que se disponibilizar recursos e instrumentos para uma investigação eficaz.

4. Conclusão

Frederick Schauer, ao analisar a questão dos precedentes horizontais e verticais, alerta que os julgadores são obrigados a segui-los, não apenas quando os considera corretos, mas também quando discordam, na medida em que é a fonte ou *status* dos precedentes que lhe dá autoridade, não a higidez de seu fundamento, nem a crença da instância que decide de que o resultado é o mais correto.[21]

---

[19] Corte IDH. Caso Da Silva e outros Vs. Brasil. Exceção Preliminar, Mérito, Reparações e Custas. Sentença de 27 de novembro de 2024. Series C No. 552

[20] Assim entendidas todas aquelas que sofrem os efeitos de um crime, nos termos da Resolução 40/34 da ONU.

[21] SCHAUER, Frederick. Pensando como um advogado: uma nova introdução ao raciocínio jurídico. Trad. Rafael Pitta. Londrina: Troth, 2021.

Em investigações sobre letalidade violenta praticada em contexto de organização criminosa, a realidade demonstra que a elucidação se faz por provas eminentemente técnicas, e não testemunhais, pela óbvia conclusão de que as testemunhas silenciam com receio de sofrerem a mesma sorte das vítimas.

Nesse cenário, não se mostra adequado admitir um precedente tal como a tese da relatora proposta para o tema n.º 1148 do STF, na medida em que a orientação proposta está em descompasso com o modelo de produção probatória no viés vitimocêntrico, além de propiciar um terreno fértil para uma investigação não diligente que, além de elevar as estatísticas das violações dos direitos humanos no Brasil, também eleva o número de condenações do Brasil nos sistema interamericano de direitos humanos, como o caso citado, à guisa de ilustração, em linhas acima.

A tese proposta para a interpretação do art. 22 da Lei 12.965/2014, além de possibilitar obstáculos para investigação diligente e eficiente, com reflexos no âmbito da punição dos violadores de direitos humanos das vítimas de crime, não se presta a resolver a questão da generalidade e vagueza levantada pela Google. Ao utilizar termos como "ordem judicial genérica e não individualizada", a interpretação mantém a ambiguidade, permitindo questionamentos tanto sobre a abrangência de uma decisão específica quanto sobre a razoabilidade do período de tempo determinado pela decisão.

Dessa forma, a tese proposta para o precedente, além de não resolver o problema, continuará na dependência da apreciação e interpretação de cada julgador, com a agravante de que, se mantida for, cria exigências que o Legislador claramente não quis fazer.[22]

O avanço da tecnologia permite a melhoria da vida em sociedade e evolução de várias técnicas para o desenvolvimento de ações nos campos da política, economia, saúde e educação, mas, por outro lado, o crime organizado também se beneficia dessa evolução, de modo que a tecnologia precisa ser utilizada no âmbito da segurança pública, seja para prevenir, seja para coibir crimes, sobretudo os relacionados à letalidade violenta, com possibilidade de provas digitais e não apenas provas testemunhais, uma vez que a obtenção de dados telemáticos e provas eletrônicas repercute cada vez mais na investigação criminal e em toda forma de combate à criminalidade.

A sociedade experimenta um momento em que a velocidade da informação se mostra sem precedentes, e a prevalecer a tese esposada no tema n.º 1148, tal qual proposta pela relatora, pode se configurar a mais clara e ampla impunidade, na medida em que o crime organizado está cada vez mais sofisticado, e não se pode exigir que em um estado democrático de direito a investigação criminal (sempre observando limites legais, convencionais e constitucionais) permaneça na era analógica quando o crime organizado está na era digital.

[22] Pontue-se que na Lei de interceptação telefônica o legislador exigiu individualização de pessoas no artigo 2º, inciso I da Lei 9296/96, ao mencionar indícios de autoria, o que não o fez no MCI.

Se a tecnologia permite identificar suspeitos através de rastreio e coleta de dados telemáticos, não há razão para uma interpretação que restrinja o artigo 22 do MCI. Não se discute que o STF pode flexibilizar aplicação de leis aprovadas pelo legislativo, mas se revela preocupante que regras que envolvam tecnologia sejam encapsuladas em precedentes rígidos tal como proposto para o tema n.º 1148 do STF.

Convém pontuar que no caso concreto, após identificados os suspeitos e manejadas as medidas cautelares de modo individualizado, dentre outras provas, as evidências digitais comprovaram que, antes do crime, o executor[23] fez várias pesquisas relacionadas à vítima, o que reforça a tese de que, se a decisão judicial tivesse sido cumprida, poderia ter encurtado o lapso temporal na identificação dos executores e, por arrasto, dos demais envolvidos.

A Google (que carecia de legitimidade para interpor o recurso judicial), ao recalcitrar contra o cumprimento das decisões judiciais, parece desconsiderar sua prática de operar na lógica do capitalismo de vigilância. Se a empresa já está utilizando dados dos usuários, sem o seu consentimento, para ganho financeiro, também deve estar disposta a fornecer dados estáticos e anonimizados para fins de justiça e segurança pública, especialmente em crimes de letalidade violenta em contexto de organizações criminosas que violam direitos humanos.

Referências bibliográficas

ARAS, Vladimir. Cerco digital ("geofence") e varredura terminológica: balizas constitucionais e legais. In: SALGADO, Daniel de Resende; BECHARA, Fábio Ramazzini; DE GRANDIS, Rodrigo (Coord.). *10 anos da Lei das Organizações Criminosas: aspectos criminológicos, penais e processuais penais*. São Paulo: Almedina, 2023. p. 597-662.

BRASIL. Interceptação Telefônica. Lei 9.296/96. Disponível em:<https://www.planalto.gov.br/ccivil_03/leis/l9296.htm>. Acesso em: 26 jun 2024.

BRASIL. Marco Civil da Internet. Lei 12.964/14. Disponível em:<http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 26 jun 2024.

MAZZUOLI, Valério de Oliveira; OLIVEIRA, Kledson Dionysio de. Princípio constitucional da ampla defesa da vítima: exegese do art. 5º, LV, da Constituição Federal e incidência no processo penal brasileiro. *Revista do Ministério Público do Estado do Rio de Janeiro*, Rio de Janeiro, n. 93, jul./set. 2024. Disponível em:<https://www.mprj.mp.br/servicos/revista-do-mp/revista-93>. Acesso em: 02 dez. 2024.

[23] Réu confesso, conforme se verifica em fontes abertas:
1 - PODER 360. **Íntegra da delação do ex-policial militar Ronnie Lessa em 16 de fevereiro de 2024**. Disponível em: <https://www.youtube.com/watch?v=BWbujFg47l8>. Acesso em: 26 jun. 2024.
2 - UOL. **Moraes tira sigilo de delação de Ronnie Lessa sobre caso Marielle e autoriza sua ida para Tremembé**. Disponível em: <https://www.youtube.com/watch?v=Q4v6iVoW574>. Acesso em: 26 jun. 2024.

PEREIRA, Frederico Valdez; FISCHER, Douglas. *As Obrigações Processuais Penais Positivas Segundo as Cortes Europeia e Interamericana de Direitos Humanos*. 2019. 2ª ed. Porto Alegre/Livraria do Advogado.

PODER 360. *Íntegra da delação do ex-policial militar Ronnie Lessa em 16 de fevereiro de 2024*. Disponível em:<https://www.youtube.com/watch?v=BWbujFg47l8>. Acesso em: 26 jun.

SCHAUER, Frederick. *Pensando como um advogado: uma nova introdução ao raciocínio jurídico***.** Trad. Rafael Pitta. Londrina: Troth, 2021.

UOL. *Moraes tira sigilo de delação de Ronnie Lessa sobre caso Marielle e autoriza sua ida para Tremembé*. Disponível em:<https://www.youtube.com/watch?v=Q4v6iVoW574>. Acesso em: 26 jun. 2024.

ZUBOFF, Shoshana. Big Other: capitalismo de vigilância e perspectivas para uma civilização de informação. In: BRUNO, Fernanda; CARDOSO, Bruno; KANASHIRO, Marta; GUILHON, Luciana; MELGAÇO, Lucas (orgs.). *Tecnopolíticas da Vigilância: Perspectivas da Margem*. São Paulo: Boitempo, 2018. p. 19-68.