

RECURSO EXTRAORDINÁRIO 1.301.250 RIO DE JANEIRO

RELATORA : **MIN. ROSA WEBER**

RECTE.(S) : **GOOGLE BRASIL INTERNET LTDA.**

RECTE.(S) : **GOOGLE INC**

ADV.(A/S) : **EDUARDO BASTOS FURTADO DE MENDONÇA**

ADV.(A/S) : **PIERPAOLO CRUZ BOTTINI**

ADV.(A/S) : **ALDO ROMANI NETTO**

ADV.(A/S) : **BRUNO LESCHER FACCIOLLA**

RECDO.(A/S) : **ESTADO DO RIO DE JANEIRO**

PROC.(A/S)(ES) : **PROCURADOR-GERAL DO ESTADO DO RIO DE JANEIRO E OUTRO(A/S)**

RECDO.(A/S) : **MINISTÉRIO PÚBLICO DO ESTADO DO RIO DE JANEIRO**

PROC.(A/S)(ES) : **PROCURADOR-GERAL DE JUSTIÇA DO ESTADO DO RIO DE JANEIRO**

RECDO.(A/S) : **MINISTÉRIO PÚBLICO FEDERAL**

PROC.(A/S)(ES) : **PROCURADOR-GERAL DA REPÚBLICA**

INTDO.(A/S) : **MONICA TEREZA AZEREDO BENICIO**

ADV.(A/S) : **JOÃO CAPANEMA TANCREDO**

AM. CURIAE. : **EDUCAÇÃO E CIDADANIA DE AFRODESCENDENTES E CARENTES - EDUCAFRÓ**

ADV.(A/S) : **IRAPUA SANTANA DO NASCIMENTO DA SILVA**

AM. CURIAE. : **INSTITUTO BRASILEIRO DE CIÊNCIAS CRIMINAIS - IBCCRIM**

ADV.(A/S) : **MAIRA COSTA FERNANDES**

ADV.(A/S) : **RAQUEL LIMA SCALCON**

AM. CURIAE. : **INSTITUTO DE TECNOLOGIA E SOCIEDADE DO RIO DE JANEIRO - ITS RIO**

ADV.(A/S) : **CELINA BEATRIZ MENDES DE ALMEIDA BOTTINO**

ADV.(A/S) : **CHRISTIAN AUGUSTO SLOMP PERRONE DE OLIVEIRA**

ADV.(A/S) : **VANESSA VARGAS DOS SANTOS**

INTDO.(A/S) : **MINISTÉRIO PÚBLICO DO ESTADO DE MINAS GERAIS**

PROC.(A/S)(ES) : **PROCURADOR-GERAL DE JUSTIÇA DO ESTADO DE MINAS GERAIS**

AM. CURIAE. : **FACEBOOK SERVICOS ONLINE DO BRASIL LTDA**

ADV.(A/S) : **MARCELA TRIGO DE SOUZA**

RE 1301250 / RJ

ADV.(A/S)

: FELIPE ZALTMAN SALDANHA

VOTO VISTA

O SENHOR MINISTRO GILMAR MENDES: Trata-se de recurso extraordinário interposto por GOOGLE BRASIL INTERNET LTDA. e GOOGLE INC. contra acórdão do Superior Tribunal de Justiça que negou provimento a recurso em mandado de segurança, nos termos da seguinte ementa (eDOC 10 - p. 95-98):

RECURSO EM MANDADO DE SEGURANÇA. DIREITO À PRIVACIDADE E À INTIMIDADE. DETERMINAÇÃO DE QUEBRA DO SIGILO DO REGISTRO DE ACESSO À INTERNET. FORNECIMENTO DE IPS. DETERMINAÇÃO QUE NÃO INDICA PESSOA INDIVIDUALIZADA. AUSÊNCIA DE ILEGALIDADE OU DE VIOLAÇÃO DOS PRINCÍPIOS E GARANTIAS CONSTITUCIONAIS. FUNDAMENTAÇÃO DA MEDIDA. OCORRÊNCIA. PROPORCIONALIDADE. RECURSO EM MANDADO DE SEGURANÇA NÃO PROVIDO.

Nas razões do recurso extraordinário (eDOC 10 - p. 135-187), as recorrentes apontaram a violação do art. 5º, incisos X e XII, e do art. 93, inciso IX, da Constituição Federal. Sustentaram que são incompatíveis com a Constituição ordens exploratórias que afetam quantidade indeterminada de inocentes. Arguiram a fundamentação insuficiente e genérica da decisão que autorizou a quebra do sigilo. Alegaram que o ato impugnado consistiu em ingerência desproporcional no direito à privacidade.

O Plenário do Supremo Tribunal Federal reconheceu a repercussão geral da questão constitucional controvertida (eDOC 17).

Iniciado o julgamento em Sessão Virtual, a eminente Ministra Relatora, Rosa Weber, encaminhou voto pelo provimento do recurso

extraordinário, “para conceder a ordem mandamental e, em consequência, cassar o item 5 da decisão proferida, em 27.8.2018, pelo Juízo de Direito da 4ª Vara Criminal da Comarca da Capital/RJ, facultando que outra seja proferida, desde que observados os limites formais e materiais dos direitos fundamentais à privacidade, à proteção de dados pessoais e ao devido processo legal”.

Propôs ainda a seguinte tese de repercussão geral: “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 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”.

O julgamento foi interrompido por pedido de vista formulado pelo Min. Alexandre de Moraes. Na retomada do julgamento, o Min. Alexandre de Moraes inaugurou a divergência para declarar a constitucionalidade do compartilhamento coletivo de dados pessoais, com a fixação de tese em sede de repercussão geral, no que foi acompanhado pelo Min. Cristiano Zanin.

Pedido de vista formulado pelo Min. André Mendonça interrompeu novamente o julgamento, o qual foi retomado com o voto apresentado pelo eminente Ministro Vitor, que propôs uma segunda tese a ser apreciada por este Plenário.

Em 24 de abril de 2025, pedi vista antecipada dos autos para melhor exame do caso. Antes do encerramento da sessão, o Ministro Alexandre de Moraes aditou seu voto para incorporar as sugestões apresentadas pelos demais Ministros à tese a ser fixada em sede de repercussão geral.

Após essa breve síntese da tramitação do processo e das discussões que se encontram subjacentes, passo a apresentar meu voto vista a partir da indicação de uma primeira questão, a qual se refere à definição das funções constitucionais do STF no contexto do alegado ativismo judicial e da necessidade da adoção de posturas minimalistas, auto-restritivas ou

deferentes em casos complexos e não maduros como o que se ora analisa.

I - Do ativismo judicial, das funções constitucionais do STF e do exercício do minimalismo ou da auto-restrição em causas complexas e não maduras

O caso em análise trata de questões complexas e interdisciplinares que já foram reveladas a partir dos intensos debates que surgiram nas sessões anteriores, os quais correlacionam temas difíceis que envolvem os limites da jurisdição constitucional e do sistema de proteção dos direitos à privacidade, à inviolabilidade e à proteção de dados frente a emergência de novos fenômenos, como o constitucionalismo digital, o direito coletivo à segurança pública e o uso de novas tecnologias por parte dos órgãos e agentes de investigação.

Além do debate relativo a estas complexas questões que deverão ser enfrentadas por esta Corte para o estabelecimento de uma interpretação constitucional, há ainda o caso concreto, em que se busca esclarecer de forma ampla e irrestrita o assassinato da Vereadora Marielle Franco e de seu motorista Anderson, um dos mais relevantes ocorridos no país nos últimos anos, tendo em vista a gravidade dos fatos que envolvem a morte de uma agente política por parte de uma organização criminosa em virtude do exercício de suas funções parlamentares.

Ressalte-se que a assimilação da complexidade do caso em sua dupla dimensão, em uma perspectiva objetiva, da decisão da matéria em sede de repercussão geral, e subjetiva, no que se refere à solução para o caso concreto, expõe de forma clara algumas questões conceituais e limitações da atuação deste Supremo Tribunal Federal.

Muito tem se falado, nos últimos anos, sobre um suposto ativismo judicial do STF na decisão de temas que se encontram pendentes de debate ou deliberação no âmbito dos demais poderes, ou que envolvem atribuições do Poder Legislativo e do Poder Executivo.

Essa questão, aliás, voltou ao centro do debate nacional em virtude

dos últimos acontecimentos políticos e constitui um tema caro e necessário, o qual deve ser objeto de consideração séria e detida por parte desta Corte.

Nesse sentido, a definição do caráter ativista, auto-contido ou deferente de determinada decisão pressupõe uma delimitação clara sobre o papel constitucional do STF e suas eventuais limitações jurídicas, políticas e institucionais. Requer-se, ainda, a consideração da aplicação de regras procedimentais e de técnicas decisórias adequadas.

No que se refere à definição da função político-constitucional do Supremo Tribunal Federal, é importante pontuar que inúmeras decisões envolvendo competências distintas e relevantes desta Corte são transferidas para a vala comum do ativismo, como se o Supremo jamais pudesse decidir, independentemente do contexto ou das circunstâncias, sobre qualquer tema que possa refletir ou impactar nas atribuições concorrentes dos demais poderes.

É certo que o Tribunal possui um largo rol de competências, tal como se observa do art. 102 da CF/88, que estabelece ser atribuição do STF o julgamento de ADIs por ação ou omissão, de ADCs, ADPFs, mandados de segurança e julgamentos penais originários contra autoridades públicas e os chefes dos demais poderes, além de prever uma ampla competência recursal, inclusive na esfera penal.

É possível afirmar, ainda, que tais competências, por vezes, se sobrepõem ou entram em choque com as funções atribuídas ao Congresso Nacional ou ao Poder Executivo e que não há o monopólio absoluto, isento a qualquer mecanismo de controle, freio ou contrapeso, no exercício das mais variadas funções legislativas, administrativas ou jurisdicionais previstas pela Constituição Federal.

Portanto, é dentro dessa moldura mais ampla e dinâmica, estabelecida pela Constituição Federal de 1988, que o Supremo Tribunal Federal tem exercido, simultaneamente, funções que podem ser associadas a um papel constitucional de órgão implementador ou legitimador de políticas públicas, de árbitro de conflitos políticos ou de

guardião dos direitos e garantias fundamentais.

A título de exemplo, esta Corte atua como órgão de implementação ou legitimação de políticas públicas quando chancela e valida programas oficiais de desestatização da máquina pública ou quando declara a constitucionalidade das medidas provisórias que estabeleceram a política oficial de racionamento, durante a crise do apagão ocorrida nos anos 2000, tal como se observa do precedente fixado no julgamento da Ação Declaratória de Constitucionalidade nº 9 (KAPISZEWSKI, Diana. *Power broker, policy maker, or rights protector? The Brazilian Supremo Tribunal Federal in transition. Courts in Latin America*. New York: Cambridge University Press, 2011, p. 159; TAYLOR, MATTHEW M. *Judging Policy: courts and policy reform in democratic Brazil*. Stanford: Stanford University Press, 2008 2008, p. 66-68).

Em tempos mais recentes, a atuação do Tribunal na fixação da competência federativa concorrente e no estabelecimento de diretrizes para a atuação do Estado brasileiro no combate à pandemia da Covid-19 e na proteção de grupos vulneráveis, como nos casos de povos indígenas e das comunidades quilombolas (ADIs 6341, 6343, ADPF 709 e ADPF 742), também podem ser considerados como exemplos relevantes dessa atuação como *policy-maker*, nos termos da feliz e precisa definição estabelecida pelo cientista político norte-americano Robert Dahl (DAHL, Robert A. *Decision Making in a Democracy: the Supreme Court as a National Policy Maker* *Journal of Public Law* , 1957).

Por sua vez, o STF atua na condição de árbitro de conflitos políticos quando decide demandas que envolvem a contestação de atos oficiais do governo em ações ajuizadas pelos partidos de oposição, bem como nas causas em que aprecia impasses ou embates instaurados entre os poderes constituídos ou entre estes e as representações dos partidos políticos e de segmentos específicos da sociedade civil (KAPISZEWSKI, Diana. *Power broker, policy maker, or rights protector? The Brazilian supremo tribunal federal in transition. Courts in Latin America*. New York: Cambridge University Press, 2011. p. 169. No mesmo sentido: NUNES,

Rodrigo M. **Politics without insurance: democratic competition and judicial reform in Brazil.** *Comparative Politics*, vol. 42, no. 3, 2010. p. 313 e ss).

Podem ser reconduzidas a essa segunda hipótese de atuação as decisões proferidas pelo STF nas ações que contém alegações de sub-representação de determinados entes federativos nas Câmara dos Deputados (MI 219, ADI 4947, ADO 38), ou as que tratam da constitucionalidade das cláusulas de desempenho eleitoral (ADIs 1354, 1351 e 5.920), os precedentes relativos à fidelidade partidária como causa de perda do mandato parlamentar (MS 26.602 e ADI 3.999), além dos julgados em que se delimitaram os poderes de atuação das CPIs e os direitos das minorias parlamentares (MS 26.441), ou os processos em que foram assentados a extensão e os limites das atribuições do Presidente da República de editar medidas provisórias (ADI 1.612, RE 231.630, RE 592.315, Súmula Vinculante 54 e ADI 4048-MC), dentre outras hipóteses (VIEIRA, Oscar Vilhena. **Supremocracia.** *Revista Direito GV*, vol. 4, no. 2, 2008, p. 451).

Por fim, a Corte atua na condição de guardião dos direitos fundamentais quando decide ações ou recursos que envolvem as garantias básicas e fundamentais de todos os cidadãos brasileiros. No exercício de tal função, entende-se que seria função do STF estabelecer um sistema rígido e forte de proteção a tais direitos, ainda que sem qualquer pretensão de atuação exclusiva na matéria, ou seja, com o resguardo da atribuição dos demais poderes de também deliberar sobre essas questões.

Ressalte-se que embora existam evidências históricas e científicas que apontem que a criação do controle de constitucionalidade esteve mais associada a controvérsias relativas ao modelo de separação dos poderes e funções, há uma forte e evidente consolidação do papel das Supremas Cortes ou dos Tribunais Constitucionais como fóruns ou órgãos destinados à proteção dos direitos e garantias fundamentais (SHAPIRO, Martin; SWEET, Alec Stone. **On Law, Politics &**

Judicialization. New York: Oxford University Press, 2002. p. 155).

Nesse sentido, é possível dizer que a função de proteção objetiva e subjetiva de direitos e garantias fundamentais deve aplicada de forma transversal a todas as hipóteses de atuação desta Corte, tal como inclusive já tive a oportunidade de defender ao tratar da condição de *policy-maker* e de guardião dos direitos e garantias fundamentais do Supremo Tribunal Federal (MENDES, Gilmar Ferreira. **As Cortes Constitucionais e a sua condição de policy-maker: análise jurisprudencial da atuação do Supremo Tribunal Federal**).

Faço esse breve introito apenas para dizer que esta Corte possui maior legitimidade decisória quando atua na decisão de relevantes questões de direitos e garantias fundamentais, em favor do sistema de reforço ou proteção a tais direitos.

Por outro lado, entendo que cabe ao Tribunal adotar posição mais deferente, auto-contida, restrita ou minimalista, nas hipóteses em que somos chamados a estabelecer, de forma inicial e como ponto de partida, políticas públicas que são normalmente atribuídas à esfera de atuação dos demais poderes, como em casos de medidas de segurança pública e novas diligências investigativas, tal como ocorre no presente caso.

Em reforço ao primeiro argumento teórico ou conceitual deduzido neste tópico, o qual se dirige não contra a solução do caso concreto, mas sim como regra de prudência em relação à expansão ou à delimitação da tese a ser adotada em sede de repercussão geral, entendo ser relevante pontuar sobre as inerentes dificuldades práticas que esta Corte possui em fixar regras gerais em um assunto tão novo, com tantas especificidades tecnológicas e com imenso potencial de reverberação.

Em relação a esse segundo ponto, é imperioso mencionar a sempre pertinente crítica sobre as eventuais limitações em termos de **capacidades institucionais** deste Supremo Tribunal Federal para a resolução de questões complexas com possíveis efeitos sistêmicos não previstos ou indesejados.

No âmbito da doutrina, há o seminal trabalho elaborado por Cass

Sunstein e por Adrian Vermule, intitulado “Interpretation and Institutions”, no qual os autores problematizam a forma como instituições com distintas habilidades e limitações devem interpretar e resolver, diante da realidade prática, textos legais e questões complexas (SUNSTEIN, Cass R; VERMULE, Adrian. **Interpretation and Institutions**. John M. Olin Program in Law and Economics Working Paper, Chicago, n. 156, 2002, p. 2).

Sob essa perspectiva, os autores apresentam uma visão mais realista para a atuação dos Juízes e das Cortes que se distancia da mítica figura do Juiz Hércules, de Dworkin, capaz de sempre enxergar a solução correta diante do substrato fático e legal, para considerar a existência de limitações em termos de tempo e de assimetria de informações que devem ser consideradas pelos magistrados na elaboração de decisões mais modestas ou minimalistas, sob pena inclusive de se produzirem efeitos sistêmicos e dinâmicos não previstos ou indesejados (SUNSTEIN, Cass R; VERMULE, Adrian. **Interpretation and Institutions**. John M. Olin Program in Law and Economics Working Paper, Chicago, n. 156, 2002, p. 35).

Nos casos em que verificadas tais limitações, Sunstein e Vermule sugerem a adoção de técnicas e de posturas decisórias cautelosas, minimalistas, gradualistas ou deferentes e desaconselham a prolação de amplas decisões maximalistas que possam incorrer nos riscos acima mencionados (SUNSTEIN, Cass R; VERMULE, Adrian. **Interpretation and Institutions**. John M. Olin Program in Law and Economics Working Paper, Chicago, n. 156, 2002, p. 24-27).

Em outra publicação sobre o tema, Cass Sunstein apresenta um título sobre a sua teoria do minimalismo judicial que soa quase como um mantra: *One case at a time*, que pode ser livremente traduzido ou interpretado como a importância de se julgar cada caso no seu devido tempo, dentro de seus estreitos limites (SUNSTEIN, Cass. **One case at a time: Judicial Minimalism on The Supreme Court**. Harvard University Press. 2001).

Ao se aplicar o referido argumento ao caso em análise, a conclusão a que se chega é que uma decisão ampliativa ou maximalista em termos de admissão da quebra coletiva de dados pessoais possui consequências jurídicas, políticas e tecnológicas que não são ou não foram inteiramente apreendidas ou consideradas por esta Corte, tendo em vista inclusive a ausência de utilização dos instrumentos previstos para a superação dessa situação, como a realização de audiências ou consultas públicas com técnicos ou especialistas no assunto.

Nesses termos, seria importante, por exemplo, que esta Corte pudesse abrir o processo à participação de agentes de segurança pública, representantes da sociedade civil e de empresas de tecnologia que sejam capazes de contribuir para a melhor decisão da causa, ou que o STF pudesse esperar a aprovação de eventual LGPD Penal, que já está em tramitação no Congresso, ou ainda, que apreciasse uma concreta política pública do Poder Executivo do uso de tais tecnologias para investigações penais.

Acresça-se que o nível de comprometimento da privacidade dos usuários de serviços digitais e o aumento exponencial do riscos de vigilância e de abusos na persecução penal também não foram, a meu ver, devidamente tematizados.

Em complemento aos argumentos teórico-conceituais e institucionais anteriormente descritos, há ainda elementos jurídico-formais e de estratégia decisória que se conectam ao raciocínio desenvolvido no presente tópico e que também recomendam uma decisão restrita ao caso concreto. Cito, por exemplo, a experiência da Suprema Corte dos Estados Unidos, que se utiliza da noção de *ripeness* ou de maturação para evitar uma intervenção judicial mais incisiva em casos nos quais a causa não esteja madura o suficiente para ser objeto de apreciação judicial (FACCHINI NETO, Eugênio. **Filtros e Barreiras no Acesso à Justiça Norte-americana: as doctrines of justiciability**. *Quaestio Iuris*. V. 9. N. 1. Rio de Janeiro, 2016. p. 496).

No Brasil, embora ainda não seja possível a utilização de

argumentos discricionários de maturidade da causa enquanto óbice ao conhecimento de determinadas causas ou recursos, já há a possibilidade admitida pela jurisprudência de cancelamento da repercussão geral ou de não fixação de teses constitucionais com eficácia *erga omnes* ou expandida, tal como ocorreu, por exemplo, no tema 206, que tratava da compensação de registradores civis pela prática de atos gratuitos previstos em lei (RE 597.673, Rel. Min. Dias Toffoli, Tribunal Pleno, j. 29.5.2023), ou no caso relativo ao uso de banheiros compatíveis com o gênero por parte de pessoas trans (RE 845.779. Red. p/ o acórdão Min. Luiz Fux, Tribunal Pleno, j. 6.6.2024).

Trago essa questão ao Pleno por considerar que a decisão da tese, nesse exato momento, não me parece suficientemente madura, razão pela qual inclusive sinalizei com a possibilidade de apresentação da proposta de cancelamento da repercussão geral na assentada anterior.

As inúmeras dúvidas e divergências contidas nos votos até então apresentados, e as mais variadas redações já propostas para a tese a ser fixada em sede de repercussão geral, exemplificam bem esse argumento e apontam para a necessidade de uma maior reflexão do tema por parte do STF, sob pena de termos de revisitá-lo por incongruências e dificuldades práticas em um futuro próximo.

Penso que até mesmo a seleção de um caso menos polêmico ou trágico poderia ser melhor para decidirmos sobre questões de direitos fundamentais com um maior nível de distanciamento e objetividade.

Por tais motivos, gostaria de apresentar ao Tribunal, a título introdutório, a sugestão de cancelamento da repercussão geral e de limitação do julgamento às peculiaridades do caso concreto. Caso vencido em relação a essa questão preliminar, em um cenário que se parece ser o mais provável, diante dos debates até aqui realizados, entendo ser o caso de se estabelecer critérios e parâmetros seguros, com base na Constituição Federal, na jurisprudência desta Corte e na legislação até aqui vigente, para se equacionar essa difícil questão de nova política ou medida de segurança pública e investigação criminal da quebra coletiva de dados

personais com as garantias da privacidade e da proteção de dados pessoais (art. 5º, X e LXXIX, da CF/88).

II – Da análise da questão controvertida

A questão controvertida nestes autos, delimitada pela Ministra Relatora por ocasião do reconhecimento da repercussão geral, consiste em definir “a **possibilidade da decretação judicial da quebra de sigilo de dados telemáticos, no âmbito de procedimentos penais, em relação a pessoas indeterminadas**” (eDOC 17 - p. 11).

Penso que é relevante começar a partir de considerações sobre o direito fundamental à proteção de dados pessoais e sua relação com o direito à privacidade.

II.a. Da autonomia do direito fundamental à proteção de dados pessoais

No julgamento da ADI 6387 MC-Ref, de relatoria da Min. Rosa Weber (DJe de 12.11.2020), consignei que, dentro da teoria jurídica moderna, a compreensão histórica do direito à privacidade é comumente vinculada – com todas as possíveis e necessárias ressalvas – à publicação do seminal artigo “The Right to Privacy”, escrito por Samuel Warren e Louis Brandeis ainda no final do Século XIX (Warren, S., & Brandeis, L. (1890). The Right to Privacy. Harvard Law Review, 4(5), p. 193–220). Esse texto revelou-se paradigmático por ter possibilitado, a partir de precedentes da tradição do *common law*, a identificação de um direito de privacidade de natureza pessoal independente da estrutura da tutela da propriedade.

Nessa concepção tradicional, o direito à privacidade pressupunha uma dicotomia entre as esferas pública e privada, colmatando-se o núcleo da proteção jurídica como o direito de ser deixado só (“*the right to be left alone*”). Em sentido individualista, a proteção atribuída ao direito à

privacidade importaria, portanto, uma postura absenteísta do Estado: o direito do titular de retrain aspectos de sua vida do domínio público (BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. São Paulo: Editora Gen, 2019, p. 95).

Na doutrina pátria, os estudos voltados à identificação da autonomia do direito à privacidade parecem ter se vinculado inicialmente a essa abordagem formal de um direito negativo de não intervenção. Tal abordagem foi reproduzida em artigo clássico do Professor Tércio Sampaio Ferraz Júnior (**Sigilo de dados: o direito à privacidade e os limites da função fiscalizadora do estado**. Revista da Faculdade de Direito da Universidade de São Paulo, v. 88, p. 430-459, 1993).

O corolário imediato dessa subsunção do direito à privacidade à função negativa de um direito fundamental personalíssimo limitou o reconhecimento da proteção constitucional do sigilo (art. 5º, inciso XII) ao conteúdo dinâmico das comunicações. Tal abordagem formalista influenciou, na década passada, o entendimento do Supremo Tribunal Federal, sobretudo no julgamento do Mandado de Segurança 21.729/DF e no julgamento do RE 418.416-8/SC.

No recurso extraordinário, o Tribunal negou que as informações contidas em registros de comunicações estariam acobertadas pelo direito à privacidade, reproduzindo, mais uma vez, a fórmula do Professor Ferraz Júnior. Na visão do saudoso Ministro Sepúlveda Pertence, Relator do caso, não teria havido violação do art. 5º, inciso XII, da Constituição, uma vez que não houve interceptação de *comunicações*, e sim a apreensão da *base física* dos dados (RE 418.416, Rel. Min. SEPÚLVEDA PERTENCE, Plenário, DJ 19.12.2006).

Todavia, essa concepção do direito à privacidade como uma garantia individual de abstenção do Estado na esfera privada individual passou por profundas transformações no decorrer do século XX. Devido ao próprio avanço das tecnologias da informação, assistiu-se a uma verdadeira mutação jurídica do sentido e do alcance do direito à privacidade. Nas palavras de Stefano Rodotà, nas últimas décadas,

vivenciamos verdadeiro “processo de inexorável reinvenção da privacidade” (RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008, p. 15).

Esse processo de reinvenção do direito à privacidade é analisado na monografia do Professor Danilo Doneda (DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Renovar: Rio de Janeiro, 2006). Ao examinar as sucessões geracionais das leis de proteção de dados a partir da década de 1970, bem como o espraiamento da proteção jurídica da privacidade em tratados internacionais ao longo do século XX, o autor assevera que:

“A trajetória percorrida pelo direito à privacidade reflete tanto uma mudança de perspectiva para a tutela da pessoa quanto sua adequação às novas tecnologias da informação. Não basta pensar a privacidade nos moldes de um direito subjetivo, a ser tutelado conforme as conveniências individuais, nem da privacidade como uma ‘predileção’ individual, associada basicamente ao conforto e comodidade. (...)”

A privacidade assume, portanto, posição de destaque na proteção da pessoa humana, não somente tomada como escudo contra o exterior – na lógica da exclusão – mas como elemento positivo, indutor da cidadania, da própria atividade política em sentido amplo e dos direitos de liberdade de uma forma geral. Neste papel, a vemos como pressuposto de uma sociedade democrática moderna, da qual o dissenso e o anticonformismo são componentes orgânicos” (DONEDA, op. cit., pp. 141-142).

A releitura do direito à privacidade coincide com o desenvolvimento jurisprudencial do conceito de autodeterminação informacional (*die informationelle Selbstbestimmung*) pelo Tribunal Constitucional Alemão.

Como destaca Claudio Franzius, a característica especial do direito à autodeterminação informativa não é resultante de invencionismo, mas sim de “*várias linhas de argumentação da jurisprudência do Tribunal, que já na*

decisão do microcenso, com recurso à sua jurisprudência sobre a dignidade humana, atribuiu ao cidadão individual uma esfera inviolável da vida privada, da qual se supõe que a influência da autoridade pública deve ser removida” (FRANZIUS, Claudio. **Das Rechtaufinformationelle Selbstbestimmung**. Zeitschrift für das juristische Studium. Gießen, 2015, p. 262).

No paradigmático caso Volkszählungsurteil (BVerfGE 65, 1), de 1983, o Tribunal declarou a inconstitucionalidade da chamada Lei do Censo alemã (Volkszählungsgesetz), que possibilitava que o Estado realizasse o cruzamento de informações sobre os cidadãos para mensuração estatística da distribuição especial e geográfica da população. Nesse julgado, a Corte Constitucional redefiniu os contornos do direito de proteção de dados pessoais, situando-o como verdadeira projeção de um direito geral de personalidade, para além da mera proteção constitucional ao sigilo.

A partir da leitura ampliativa do artigo 2.1, em conjunto com o artigo 1.1. da Grundgesetz, o Tribunal Constitucional reconheceu a existência de um direito constitucional de personalidade que teria como objeto de proteção o poder do indivíduo de “decidir sobre a divulgação e o uso dos seus dados pessoais” (*„selbst über die Preisgabe und Verwendung seinerpersönlichen Daten zu bestimmen“*), de “decidir sobre quando e dentro de quais limites os fatos da sua vida pessoal podem ser revelados” (*„zuentscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden“*) e ainda “de ter conhecimento sobre quem sabe e o que sabe sobre si, quando e em que ocasião” (*„wissen können, wer was wann und bei welcher Gelegenheit über sie weiß“*). (FRANZIUS, op. cit., p. 259).

Seguindo esse raciocínio, o Tribunal entendeu que o processamento automatizado dos dados possibilitado pela Lei do Censo de 1983 colocaria em risco o poder do indivíduo de decidir por si mesmo sobre se e como ele desejaria fornecer a terceiros seus dados pessoais. O risco identificado pelo Tribunal referia-se à possibilidade de, por meio de sistemas automatizados, o Estado formar um “perfil completo da

personalidade” dos cidadãos.

Essa nova abordagem revelou-se paradigmática por ter permitido que o direito à privacidade não mais ficasse estaticamente restrito à frágil dicotomia entre as esferas pública e privada, mas, sim, se desenvolvesse como uma proteção dinâmica e permanentemente aberta às referências sociais e aos múltiplos contextos de uso. Como destacou a decisão, a identificação de um constante avanço tecnológico demanda a afirmação de um direito de personalidade que integre o contexto das “condições atuais e futuras circunstâncias do processamento automático de dados” (*“heutigen und künftigen Bedingungen der automatischen Datenverarbeitung“*).

Essa releitura possibilita a afirmação do direito à autodeterminação informacional como um contraponto a qualquer contexto concreto de coleta, processamento ou transmissão de dados passível de configurar situação de perigo.

Nas palavras de Stefano Rodotà, **a privacidade também passa ser definida como "o direito de manter o controle sobre suas próprias informações e de determinar como a privacidade é alcançada e, em última instância, como o direito de escolher livremente o seu modo de vida"** (tradução livre) (RODOTÀ, Stefano. *In diritto di avere*. Roma: Laterza, 2012, p. 321).

A maior abrangência da proteção atribuída ao direito de autodeterminação repercute no âmbito de proteção do direito à proteção de dados pessoais, que não recai sobre a dimensão privada ou não do dado, mas sim sobre os riscos decorrentes de seu processamento.

Destaque-se que a afirmação da autonomia do direito fundamental à proteção de dados pessoais não se faz tributária de mero encantamento teórico, e sim da necessidade de afirmação de direitos fundamentais nas sociedades contemporâneas.

Com efeito, ao consideramos que os espaços digitais são controlados por agentes econômicos dotados de alta capacidade de coleta, armazenamento e processamento de dados pessoais, a intensificação do fluxo comunicacional na internet aumenta as possibilidades de violação

de direitos de personalidade e de privacidade. Todas essas transformações tecnológicas ensejam aquilo que Bruno Bioni enxerga como um cenário de hipervulnerabilidade no regime de proteção de dados pessoais, que se desdobra em traços vulnerantes peculiares sob as perspectivas informacional, técnica e econômica (BIONI, op. cit., p. 164).

Desse modo, a força normativa do direito fundamental à proteção de dados pessoais decorre da necessidade de proteção da dignidade da pessoa humana, vis-à-vis a contínua exposição dos indivíduos ao risco de comprometimento da autodeterminação informacional. Como explica a professora Laura Schertel Mendes o reconhecimento desse direito fundamental é necessário *“para tornar efetivos os fundamentos e princípios do Estado democrático de direito, na sociedade contemporânea da informação, conforme determina a Constituição Federal”* (MENDES, Laura Schertel Ferreira. **Habeas data e autodeterminação informativa: os dois lados da mesma moeda.** Direitos Fundamentais & Justiça, Belo Horizonte, ano 12, n. 39, p. 185-216, 2018).

Essa evolução não passou despercebida por este Tribunal. Se, como visto, em uma perspectiva mais tradicional da compreensão do direito à privacidade, a doutrina e a jurisprudência entendiam que a proteção constitucional expressa no art. 5º, inciso XII, não abrangia o conteúdo dos dados pessoais e dizia respeito tão somente ao fluxo de informações em meios comunicacionais (RE 418.416, Rel. Min. Sepúlveda Pertence, Tribunal Pleno, DJ de 19.12.2006), não há dúvidas de que esse entendimento foi superado a partir de decisões do Supremo Tribunal Federal que alargaram o âmbito de proteção do art. 5º, incisos X e XII, para afirmar a autonomia do direito fundamental à proteção de dados (RE 673.707, Rel. Min. Luiz Fux, Tribunal Pleno, julgado em 17.6.2015, DJe 30.9.2015).

Por força do direito fundamental à proteção dos dados pessoais, todas essas informações estão albergadas pela tutela constitucional. Nesse sentido, não restam dúvidas que a posição tradicional desta Corte no sentido da diferenciação entre dados estáticos e em fluxo para

aferição de proteção consitucional foi superada.

Em outras palavras, a distinção entre dados estáticos e dinâmicos diz pouco sobre os limites para ingerência estatal nos dados pessoais. É necessário avançar no tema para melhor delimitar as formas de coleta e tratamento dos dados pessoais, bem assim os espaços abrangidos pela reserva de jurisdição.

A consideração desses aportes teóricos e jurisprudenciais para o exame da questão controvertida neste tema de repercussão geral é imprescindível, na medida em que se discute a legitimidade de decisão judicial proferida em investigação criminal que implica a obtenção de dados pessoais - endereços de IP e parâmetros de busca na internet - de número indeterminado de usuários, independente de qualquer vínculo indiciário ou suspeita de cometimento do ato ilícito.

II.b. O impacto da digitalização para as práticas de persecução penal

A evolução tecnológica traz à baila uma série de questões acerca dos limites da atividade estatal nas atividades de persecução penal. Com a disseminação de dispositivos conectados à internet e o fenômeno de datificação, observa-se coleta de informações sem precedentes. Tecnologias como câmeras de vigilância ubíquas, reconhecimento facial, celulares e GPS permitem a coleta e análise massiva dados a partir do rastreamento detalhado de movimentos e comunicações.

Sabemos, hoje, que grande parte das atividades cibernéticas que o ordenamento jurídico procura proteger já não se encontra mais em bases físicas, mas em bancos de dados espalhados pelo mundo, verdadeiras gavetas virtuais nas quais são guardados substanciais aspectos da nossa vida privada.

Essa ampliação dos registros das atividades humanas tem um impacto substancial para a capacidade de investigação penal estatal. A cada ano, observamos a emergência de novos meios de produção de

provas - como a busca reversa, que ora discutimos, o uso de ferramentas de intrusão remota (*spywares*), câmeras com reconhecimento facial, entre outras.

A ampliação das medidas investigativas à disposição da persecução penal impõe criteriosa reflexão acerca dos limites fixados pelos direitos fundamentais — em especial as garantias já mencionadas de respeito à vida privada e de proteção dos dados pessoais. Nesse ponto, penso que é importante recuperar como Cortes Constitucionais alhures vêm lidando com a temática.

A decisão da Corte Constitucional alemã no caso *Online-Durchsuchungen*, ao conferir novos contornos à garantia de proteção ao direito de personalidade por meio de interpretação no sentido de que a confidencialidade e a integralidade dos sistemas de tecnologia da informação configuram direito fundamental comparável à inviolabilidade do domicílio, compreendeu, de forma inovadora, o alcance dessa garantia.

Nesse precedente, recursos constitucionais foram apresentados contra determinados dispositivos da lei de defesa da Constituição do Estado de Nordrhein-Westfalen, que permitiam às autoridades capturar, inclusive por meio de acesso remoto, dados de computadores e redes de informática.

Quais tecnologias, em que circunstâncias os agentes do Estado estão autorizados a utilizá-las na captação remota de dados armazenados em computadores e quais atividades cibernéticas estão cobertas pelo termo “comunicação de dados”, foram perguntas enfrentadas pela Corte no julgamento do referido caso.

A Corte Constitucional considerou os dispositivos questionados incompatíveis com o que denominou de direito à garantia de confidencialidade e de integralidade de sistemas de tecnologia da informação. Passou-se a garantir, por esse direito, a proteção contra interferências em sistemas de tecnologia da informação não assegurados por outros direitos fundamentais, como a privacidade de

correspondência, correios e telecomunicações, ou a inviolabilidade do domicílio (Lei Fundamental, arts. 10 e 13).

Especificamente em relação ao sigilo das telecomunicações, predominava no direito alemão, no mesmo sentido da antiga jurisprudência do STF, há pouco examinada, o entendimento de que seu objeto é o conteúdo da comunicação no momento em que ela se realiza e não os dados armazenados após a sua transmissão. A razão de ser dessa distinção é que as informações armazenadas em qualquer dispositivo, após a sua transmissão, já não estariam mais expostas aos perigos que normalmente resultam da vulnerabilidade dos dados durante o processo interativo e dinâmico de comunicação.

No caso *Online-Durchsuchungen*, contudo, foi ressaltado que os computadores estão presentes em todas as áreas da vida moderna e são cada vez mais essenciais ao desenvolvimento da personalidade. Todavia, ao tempo que criam novas oportunidades, também colocam em risco os seus usuários. Dessa forma, tendo em conta a possibilidade de busca e apreensão remota de dados já armazenados, sem a necessidade, portanto, da apreensão do computador, a proteção com base na distinção entre transmissão e armazenamento passou a se mostrar insuficiente.

Diante dessa nova realidade, adotou o Tribunal o conceito de sistema de tecnologia da informação como um sistema com capacidade de conter dados técnicos a um ponto que fosse possível ter conhecimento de uma substancial parcela da vida de um indivíduo e noção significativa de sua personalidade. Com base nesse conceito, assentou a Corte que a confidencialidade e a integralidade dos sistemas de tecnologia da informação configuram direito fundamental comparável à inviolabilidade do domicílio.

Sem essa concepção do direito à privacidade, observou a Corte que não haveria, por exemplo, nenhum óbice legal à captação de conteúdos gráficos da tela do computador de pessoas sujeitas a investigações criminais, ante a inexistência de qualquer forma de comunicação no instante em que alguém está lendo um texto nestes dispositivos.

Considerou a Corte que casos dessa espécie confeririam um poder excessivo ao Estado para espionar os cidadãos.

Quanto à infiltração clandestina (*heimliche Infiltration*) por meio de softwares espões como Trojan Horse, observou a Corte que esse tipo de investigação criminal **somente seria possível em raríssimos casos de investigações de crimes graves em um rol pré-estabelecidos**, quando se verificasse, por exemplo, ameaça concreta e iminente a um bem jurídico importante, como a vida ou a liberdade de uma pessoa ou a existência e segurança do próprio Estado.

Ressaltou a Corte, todavia, que a “busca on-line” de informações poderia ser justificada com a finalidade de investigar e prevenir práticas criminosas, mediante autorização judicial e desde que observados os requisitos constitucionais de clareza e determinação jurídica.

Essa nova concepção do direito à privacidade, sem precedente no direito alemão, serviu como forma de preencher uma lacuna até então existente e passou a ser um marco não apenas na Alemanha, mas em toda a Europa.

Mais recentemente, no caso 1 BvR 142/15, o Tribunal Constitucional Alemão examinou a constitucionalidade do uso de sistemas automáticos de reconhecimento de placas de veículos, previstos na lei estadual da Baviera, como parte de investigações criminais. De acordo com a legislação, as placas dos veículos em trânsito seriam registradas de forma automática, sendo armazenados temporariamente em conjunto com informações relativas ao local, data, hora e direção do deslocamento, sendo cruzadas com as bases de dados da polícia.

A Corte avaliou que a lei envolveria essencialmente duas atividades de tratamento de dados pessoais - a coleta e a verificação cruzada com os bancos de dados da polícia. Nesse sentido, representaria restrição ao direito à autodeterminação informativa. A partir da análise do princípio da proporcionalidade, **a Corte concluiu que o emprego do reconhecimento automático de placas de veículos somente se mostraria constitucionalmente admissível quando amparado em fundamentos de**

significativa relevância. A norma impugnada, entretanto, não atenderia esta exigência, à medida que não era limitada à circunstâncias de crimes graves ou locais perigosos.

Nessa mesma linha, podemos mencionar, ainda, a solução adotada pela Suprema Corte dos Estados Unidos no caso *US v. Jones*, ao equiparar o conceito de busca e apreensão, previsto na Quarta Emenda Constitucional, à instalação de equipamento GPS no automóvel de um suspeito para o contínuo monitoramento de sua localização. No caso, a *Justice* Sonia Sotomayor apresentou opinião concordante, na qual traçou considerações quanto aos efeitos do monitoramento a partir de tecnologia de GPS sob a perspectiva de vigilância estatal:

“(...) por ser o monitoramento via GPS mais acessível economicamente em comparação com técnicas convencionais de vigilância e, por sua própria natureza, ocorrer de forma furtiva, ele escapa aos controles ordinários que limitam práticas abusivas de persecução penal — como os recursos policiais limitados e a resistência da comunidade (*Illinois v. Lidster*, 540 U.S. 419, 426, 2004). A consciência de que o Estado pode estar observando exerce efeito inibidor sobre as liberdades de associação e de expressão. O poder descontrolado do Estado de coletar dados que revelam aspectos privados da identidade é, por sua vez, suscetível a abusos. Como resultado, o monitoramento por GPS — ao disponibilizar, a custo relativamente baixo, uma quantidade substancial de informações íntimas sobre qualquer pessoa que o Estado, a seu critério irrestrito, decida rastrear — pode ‘alterar a relação entre cidadão e governo de forma incompatível com uma sociedade democrática’ (*United States v. Cuevas-Perez*, 640 F.3d 272, 285, 7ª Cir., 2011, voto concordante de Flaum, J., tradução livre).”

Mais recentemente, no caso *Carpenter v. United States*, a Corte avaliou em que medida obtenção de registros históricos de localização de

celulares representaria uma “busca” protegido pela Quarta Emenda à Constituição. Na oportunidade, a Corte afastou a aplicação da chamada “third-party doctrine”, estabelecida nos precedentes *US v. Miller* (1976) e *Smith v. Maryland* (1979), segundo a qual informações compartilhadas com terceiros perderiam a “expectativa razoável de privacidade”, deixando de estar protegidas pela Quarta Emenda.

No caso em exame, tratava-se de dados gerados por usuários na utilização de telefones celulares, compartilhados com operadoras de serviços de telefonia, de modo que a Corte concluiu que representaria uma *“crônica exaustiva de informações de localização coletadas de forma casual pelas operadoras de telefonia sem fio”*. **Penso que o caso é interessante à medida que ilustra que o fato de informações estarem disponíveis para terceiros - empresas de telefonia, no caso - não representa uma renúncia aos direitos fundamentais à vida privada.**

Esta breve incursão em casos internacionais ilustra os esforços de Cortes Constitucionais em atualizar as garantias penais ao cenário de evolução tecnológica. Conforme já tive a oportunidade de discutir em outros julgamentos e em artigos acadêmicos, o constitucionalismo digital destaca o papel da jurisdição constitucional em assegurar um nível de proteção adequado aos direitos fundamentais em face do desenvolvimento tecnológico (MENDES, Gilmar Ferreira; FERNANDES, Victor Oliveira. **Constitucionalismo digital e jurisdição constitucional: uma agenda de pesquisa para o caso brasileiro.** Revista Brasileira de Direito, Passo Fundo, v. 16, n. 1, p. 1-33, jan./abr. 2020).

Não é porque eventual inovação no campo tecnológico não esteja suficientemente contemplada na legislação em vigor que a garantia constitucional ameaçada fica sem proteção, cabendo ao intérprete, ao lidar com essa realidade, assegurar que o direito fundamental em si, com as garantias a ele inerentes, não seja menosprezado a ponto de negar-lhe efetividade.

Nesse sentido, a observância de normas de organização e procedimento pela autoridade pública revela-se essencial para assegurar

a proteção dos dados pessoais, evitando que a coleta e tratamento dessas informações ocorra à revelia de firmes balizas constitucionais.

Em que pese essa constatação, diretamente decorrente das reflexões acima realizadas a respeito do direito fundamental à proteção de dados pessoais, convém salientar que a controvérsia não se exaure em mero exame de legalidade. Em outras palavras, malgrado a legislação desenvolva papel importante na estruturação de normas de organização e procedimento, é possível vislumbrar situações nas quais determinadas técnicas modernas de investigação sejam legítimas, ainda que não contempladas expressamente na legislação vigente.

Tive a oportunidade de ponderar, em sede doutrinária (Curso de Direito Constitucional. p. 659-661), que os avanços tecnológicos, no que diz respeito à privacidade, alcançaram uma dimensão tão distante da moldura jurídica com a qual trabalhamos que, em certa medida, talvez já nem seja mais correto falar-se em insuficiência da legislação, no sentido de seu descompasso com as tecnologias invasivas com as quais convivemos.

Com essas considerações, **poderíamos avançar em relação ao tema não mais nos preocupando tanto em contemplar, em textos legais, de modo específico, cada nova tecnologia que surge, mas, sim, na reformulação do modelo de regulação, de forma a estabelecer requisitos mínimos como, por exemplo, crimes passíveis de investigação por tecnologias invasivas, imprescindibilidade de autorização judicial, duração da investigação, forma de registro dos dados obtidos, restrições na divulgação dos dados capturados e sistema de acompanhamento do efetivo cumprimento dos requisitos estabelecidos.**

Nesse ponto, rememoro que o Congresso Nacional não avançou para a necessária edição de uma Lei Geral de Proteção de Dados para Fins Penais (LGPD Penal), cujo anteprojeto já se encontra em tramitação na Câmara dos Deputados (VERONESE, Alexandre; CALABRICH, Bruno. **Crimes na internet e o Brasil no cenário da cooperação jurídica internacional**. Portal Jota. 24.4.2021). Com efeito, o anteprojeto estabelece

uma série de limites para a coleta e tratamento de dados pessoais nos procedimentos investigatórios, a exemplo de seus artigos 15 e 16. Nesse sentido, vale recuperar as considerações de Laura Schertel Mendes e Jacqueline de Souza Abreu:

“O recorte existente na LGPD e o espaço para a aprovação de uma LGPD penal não significam que a noção de proteção de dados como a conhecemos hoje não seria aplicável no processo penal e na segurança pública. Dois pontos demonstram o contrário: primeiro, o reconhecimento da proteção de dados pessoais como direito fundamental autônomo pelo STF e a sua aplicação em contextos envolvendo inteligência nacional e segurança pública; segundo, a observância dos princípios e direitos da proporcionalidade e devido processo legal, conforme determinado pela própria LGPD. (...) Nesse sentido, a importância de se aprovar uma lei específica de proteção de dados para investigação criminal e segurança pública no Brasil consiste em: criar parâmetros procedimentais para que existam balizas legais concretas no tratamento de dados pelos órgãos de investigação; ampliar a transparência sobre como dados são tratados para permitir a responsabilização e desencorajar usos secundários inadvertidos; e minimizar riscos de tratamentos abusivos, ilegais e de incidentes de segurança, dentre outros.” (Schertel Mendes, Laura; Abreu, Jacqueline. *Carta das Editoras - Dossiê Temático "Privacidade e Proteção de Dados Pessoais na Segurança Pública e no Processo Penal"*. *Direito Público*, 18(100). <https://doi.org/10.11117/rdp.v18i100.6214>. 2022)

Não é demais lembrar: o direito à proteção de dados pessoais é também uma garantia oponível ao Estado no âmbito de investigações criminais - como a jurisprudência da Corte Constitucional alemã bem ilustra.

Seja qual for o cenário tecnológico que nos cerca, não se pode perder de vista que é a boa aplicação dos direitos fundamentais de caráter processual, principalmente da proteção judicial efetiva, que nos permite distinguir o Estado de Direito do Estado Policial. O prestígio desses direitos configura também elemento essencial de realização do princípio da dignidade humana na ordem jurídica, impedindo, dessa forma, que o homem seja convertido em mero objeto do processo.

II.c. Apontamentos sobre a tese de repercussão geral

Como já pude observar no início de meu voto, acredito que seria necessário avaliarmos enquanto colegiado a pertinência de desafetarmos a fixação de tese de repercussão geral do presente caso concreto. Como busquei demonstrar, o tema de acesso a informações no âmbito de investigações criminais é complexo e meritório de debate aprofundado. Em face do acelerado desenvolvimento tecnológico, é igualmente rápida a evolução de novas técnicas de investigação.

Contudo, como penso ser vencido em relação à desafetação, tendo em vista o extenso debate ocorrido até o presente momento, passo, subsidiariamente, a propor alguns elementos que considero essenciais para a fixação de eventual tese de repercussão geral que represente balanceamento adequado entre os direitos à proteção de dados pessoais e a efetividade das persecuções criminais, ambos valores centrais para o Estado Democrático de Direito.

Com efeito, a primeira questão que antevejo em relação a uma possível omissão inconstitucional na regulação deste tema de segurança pública, o qual exige e requer a prolação de decisão aditiva com base em parâmetros legais já existentes, é com relação a quais crimes justificariam a presente restrição aos direitos de privacidade e de proteção de dados de pessoas indetermináveis, a partir do princípio da proporcionalidade.

Esse ponto foi tratado na decisão da Corte Federal Alemã sobre leitura automática de placas, que entendeu que a norma seria

parcialmente inconstitucional por conter autorização ampla de utilização das informações:

“Em conformidade com o princípio da proporcionalidade, o uso do reconhecimento automático de placas de veículos é, em princípio, admissível apenas quando fundado em razões de suficiente peso. As disposições impugnadas não atendem a tal exigência na medida em que as medidas autorizadas não se limitam à proteção de bens jurídicos de relevância ao menos considerável. (...) As disposições que regulam o cruzamento das placas veiculares registradas com os bancos de dados de veículos de interesse (*Fahndungsbestände*) devem ser interpretadas de forma restritiva e em conformidade com a Constituição, de modo que as placas somente possam ser confrontadas com dados efetivamente aptos a proteger contra o perigo específico que motivou a determinação do reconhecimento automático no caso concreto. Por fim, o marco legal não estabelece a obrigação das autoridades de documentar os fundamentos que justificaram a decisão de empregar o reconhecimento automático de placas.” (Ordem de 18 de dezembro 2018 - 1 BvR 142/15, tradução livre).

Nesse sentido, acredito que é central restringirmos o uso da medida da quebra coletiva ou indeterminada de dados pessoais no caso de busca reversa de palavras chaves pesquisadas em buscadores de Internet às investigações relacionadas a crimes hediondos, previstos pela Lei 8.072/90, em que a relevância da persecução penal, dos bens jurídicos protegidos e da gravidade em concreto dos delitos se coadunam com uma análise de proporcionalidade e adequação da restrição aos direitos fundamentais envolvidos.

Nesse sentido, observo que os requerentes apresentaram, em memoriais, decisões judiciais de primeiras instâncias com pedidos de busca reversa em crimes de baixo potencial lesivo - inclusive um caso de

furto de igreja, cometido sem qualquer elemento de violência ou grave ameaça.

Penso que a tese de repercussão geral deve coibir a utilização indiscriminada dessa gravosa medida investigativa para qualquer espécie de delito, inclusive pelos riscos de seletividade penal e do direcionamento aleatório de inquéritos para pessoas identificadas com base apenas nessa medida investigativa.

Um **segundo ponto** que acredito que é essencial e que decorre da defesa do minimalismo e da auto-restrição apontada nos tópicos anteriores do meu voto, é a **delimitação da tese de repercussão geral para o meio de obtenção de prova e as categorias de dados que estão sendo discutidas no âmbito desse processo** - qual seja, a busca reversa de indivíduos a partir de palavras chaves pesquisadas em buscadores de internet. Passo a explicar o por que dessa restrição.

A proteção de dados pessoais e o impacto de cada atividade de coleta e tratamento para os direitos fundamentais de um indivíduo depende, invariavelmente, das categorias de dados pessoais discutidas e do contexto. Como explica Helen Nissenbaum, em seu influente livro "Privacy in context : technology, policy, and the integrity of social life", as expectativas dos indivíduos com relação a seus dados pessoais importam, de modo que as categorias de dados e contextos de tratamento têm um papel inegável em delimitar o nível de proteção que se espera para cada situação.

Com efeito, essa lógica foi expressamente adotada no já mencionado *Carpenter v. United States*, no qual a Suprema Corte norte-americana reconheceu que o acesso a informações no âmbito de investigações criminais tem quem levar em conta a categoria de dados pessoais a que se refere, a partir de considerações sobre o impacto do uso de informações de geolocalização no âmbito de investigações.

Nesse sentido, penso que é temerário o estabelecimento de uma tese de repercussão geral aplicável a todas as hipóteses de tecnologias de acesso a dados e a informações armazenadas digitalmente. A

necessária atualização das balizas processuais criminais das novas medidas de investigação deve levar em consideração o impacto daquela atividade para os direitos fundamentais. O impacto de determinada atividade para o direito à privacidade e proteção de dados, por sua vez, está relacionado ao contexto e também ao tipo de dado que se busca.

Por exemplo, já mencionamos o caso de acesso a informações de geolocalização - que a meu ver é distinto e mais grave para a esfera privada do indivíduo do que as informações de busca que ora discutimos. Nesses casos, o monitoramento de localização de indivíduos pode gerar informações sobre os mais diversos elementos que integram a sua vida privada ou a sua intimidade, de modo a gerar um risco potencial de vigilância estatal excessiva ou desmedida.

Não ignoro que dados de pesquisas podem conter informações pessoais consideradas sensíveis, conforme definido na legislação pátria. Seria o caso, por exemplo, de um número grande de buscas sobre determinada doença.

Em um caso como esse, é possível que a quebra coletiva de dados relativos a pesquisas em buscadores possa ter um impacto tão ou até mesmo mais grave que a geolocalização, já que essas informações podem ser utilizadas para fins discriminatórios e gerar uma série de potenciais danos para seus titulares.

A tese aqui discutida, entretanto, tem um impacto menor. Trata-se de busca intrinsecamente relacionada ao crime - busca nominal e de endereços que remetem às vítimas e ao local do delito.

Pelas razões acima expostas, creio que o mais correto é nos limitarmos a essa hipótese específica de quebra coletiva de dados, dentro desse contexto mais restrito.

Um **terceiro ponto** conectado ao argumento anterior é a necessária limitação da medida investigativa. A busca reversa deve ser limitada e precisamente definida - tanto quanto aos termos buscados quanto com relação à sua limitação temporal.

Nesse ponto, observo que a lógica tradicional da persecução penal

tem como ponto de partida a existência de indícios de materialidade e autoria. É esse o requisito para muitas medidas que afetam a privacidade de indivíduos - conforme placitado pela Lei de Interceptação Telefônica, por exemplo. A busca reversa, por outro lado, pode inverter essa lógica, gerando potenciais efeitos para garantias como a presunção de inocência e a vedação à autoincriminação.

Bárbara Simão e Vitor Vilanova alertam sobre as restrições à privacidade de indivíduos sem quaisquer relação com determinada prática criminosa: *“o acesso indiscriminado aos dados de inúmeras pessoas não relacionadas ao crime investigado constituiria violação à presunção de inocência.”*. Prosseguem para afirmar que, considerando que as pessoas alvo da medida não têm conhecimento da coleta de dados em andamento, podem inadvertidamente produzir provas contra si mesmas. (SIMÃO, Bárbara; VILANOVA, Vitor. **O acesso a dados de geolocalização de pessoas indefinidas: uma análise sobre a prática de busca reversa**. São Paulo. InternetLab, 2023).

Ora, estamos tratando de restrições de direitos fundamentais de pessoas indetermináveis. Nesse sentido, a limitação da medida é essencial para garantir que o menor número de sujeitos não relacionados ao crime sofram essa limitação. **Portanto, a busca reversa deve ser limitada a termos pertinentes para a investigação criminal e também à janela temporal da medida, de modo a abranger apenas o momento anterior ao cometimento do crime.**

De fato, todas essas considerações com relação à relevância da medida de investigação devem estar refletidas em decisão judicial fundamentada - **quarto requisito** que trato e que observo que já estamos endereçando na tese de repercussão geral proposta.

O art. 22 do Marco Civil da Internet regulamenta o acesso aos registros de conexão e de acesso a aplicações de internet nos seguintes termos:

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.

Assim, para que a autoridade responsável pela investigação tenha acesso a referidos registros no curso da investigação, além de autorização judicial, deve apresentar (i) fundados indícios da ocorrência de ilícito; (ii) a utilidade da diligência; e (iii) o período a que se referem os dados.

Embora esse dispositivo não diga respeito expressamente ao acesso a informações de um conjunto indeterminado de pessoas, a mim me parece, na linha da divergência inaugurada pelo Min. Alexandre de Moraes, que dele podem ser extraídos alguns requisitos necessários para assegurar a tutela dos direitos fundamentais à privacidade e à proteção dos dados pessoais.

O primeiro deles diz respeito à autorização judicial. A submissão da medida cautelar à reserva de jurisdição representa importante limite à ingerência estatal sobre dados pessoais a partir de investigações criminais. Sobre o tema, recupero doutrina especializada:

Essa observação reforça o argumento de que restrições realizadas por autoridades estatais sobre direitos jurídicos de privacidade que em geral teríamos sobre terceiros do público em geral só são legítimas quando presentes certos requisitos e observado certo procedimento, como exigência de fundamentação de sua legitimidade em face da pessoa em cujos

interesses se intervêm, contra erros, excessos e abusos. É uma questão de contenção de poder. É nisso, portanto, que repousa a justificação para a restrição legítima a esses sentidos de privacidade. (ABREU, Jacqueline De Souza. **Privacidade, segurança e tecnologia**. Doutorado Direto em Filosofia e Teoria Geral do Direito—São Paulo: Universidade de São Paulo, 20 abr. 2022, p. 307).

Além disso, a necessidade de crivo do Poder Judiciário pressupõe também que os elementos investigativos estejam devidamente documentados e formalizados, vedando peremptoriamente diligências informais dessa natureza.

A par desse aspecto, a necessária comprovação de indícios de ocorrência de ilícito impedem diligências aleatórias ou desvinculadas de uma hipótese investigativa criminal minimamente viável. **É dizer, medidas probatórias como a discutida nestes autos não podem ser deferidas em ambiência caracterizada pela precocidade da investigação ou serem utilizadas como diligências investigativas iniciais.**

Deve-se, ao contrário, utilizar-se de uma lógica de subsidiariedade ou de última *ratio* investigativa, tendo em vista a gravidade e a restrição aos direitos fundamentais à proteção de dados de um número significativo de pessoas.

A esse critério soma-se a análise da utilidade da diligência. Cabe à autoridade policial demonstrar de que forma aqueles dados pessoais são essenciais e estritamente necessários para a investigação em andamento. Aqui, é inserido verdadeiro juízo de proporcionalidade da medida. Cumpre ao Poder Judiciário, no controle da investigação, averiguar se aquela medida invasiva é proporcional à utilidade que se pode extrair dos dados obtidos e elencar e explicitar tais elementos em decisão devidamente fundamentada.

É necessário ponderar, ainda, o grau de ingerência no direito fundamental dos afetados com os resultados que podem ser alcançados.

Essa análise baseada no princípio da proporcionalidade é incrementada pelo item 2 da tese de julgamento proposta pelo Min. Alexandre de Moraes, segundo o qual os atingidos pela medida devem ser “determináveis a partir de outros elementos de provas obtidos previamente na investigação e que justifiquem a medida”.

Assim, é imperiosa a justificação da medida e o cruzamento de informações que determine, ainda que *a posteriori*, os dados que interessam à investigação, com o descarte daqueles que se revelarem inúteis para o seu deslinde. Essa providência afasta medidas invasivas meramente especulativas e sem objetivo concreto, que constituiriam simples devassa de dados pessoais. **De fato, esse é outro elemento que deve ser incorporado à decisão judicial, qual seja, a previsão de descarte de dados que não se mostrarem úteis à investigação.** Esse ponto é essencial para garantir que essas informações não sejam utilizadas em investigações posteriores - por exemplo, a partir da criação de dossiês sobre indivíduos que não tenham nenhuma relação com o crime inicialmente investigado.

Em outras palavras, no exame da proporcionalidade da medida deve restar demonstrado que, a partir dos elementos probatórios já colhidos, é possível determinar minimamente os alvos da operação e a necessidade e utilidade da diligência requerida. Além disso, a observância à proporcionalidade em sentido estrito requer que sejam descartados os dados de terceiros não vinculados ao inquérito.

Por fim, a delimitação do período dos dados a que se pretende ter acesso também reforça o controle da medida, impondo que esse lapso, além de devidamente limitado, seja justificado pelos elementos probatórios já documentados pela autoridade policial.

Desse conjunto de requisitos extrai-se que medidas como a dos autos devem atender ao princípio da subsidiariedade. A sua deflagração impõe que as investigações tenham avançado a um grau de maturidade que permita sua adequada fundamentação e especificação pela autoridade policial, afastando a possibilidade de devassas ou

medidas especulativas serem implementadas à revelia do controle judicial.

No caso dos autos, o juiz de primeira instância deferiu pedido da autoridade policial para fornecimento de todos os endereços de IP que efetuaram pesquisa por meio do “Google Busca” dos termos “Mariele Franco”, “Vereadora Mariele”, “Agenda Vereadora Mariele”, “Casa das Pretas”, “Rua dos Inválidos, 122” ou “Rua dos Inválidos”, entre os dias 10.3.2018 e 14.3.2018.

Os elementos apresentados pela autoridade policial atendem aos requisitos anteriormente expostos, delimitando temporal e espacialmente o escopo da medida. Além disso, o estágio das investigações naquele momento viabilizava a determinação posterior dos investigados a partir dos elementos colhidos.

Em síntese, não se tratou de devassa ou atividade especulativa. Havia elementos concretos que indicavam a prática de crime gravíssimo, **verdadeiro crime hediondo (art. 1º, I, da Lei 8.072/90)**, bem como a utilidade das informações que se pretendia obter para o desenvolvimento da investigação.

Ante o exposto, reservadas as devidas vênias, acompanho a divergência inaugurada pelo Min. Alexandre de Moraes e nego provimento ao recurso extraordinário, sugerindo a incorporação dos elementos sugerindo ao longo desse voto à eventual tese a ser aprovada por esta Corte, a qual sugiro que seja assim redigida:

1) É constitucional a requisição judicial de registros de conexão ou de registros de acesso a aplicativos de internet para fins de investigação criminal ou instrução processual penal, inclusive o fornecimento de dados pessoais por provedores, em cumprimento de medida de busca reversa por palavra-chave, com fundamento no art. 10 e no art. 22 da Lei 12.965/2014 (Marco Civil da Internet), desde que preenchidos os requisitos de (a) fundados indícios de ocorrência do ilícito; (b) motivação da utilidade dos registros solicitados para fins de investigação ou

instrução probatória; (c) período ao qual se referem os registros.

2) Em casos de investigações relativas a crimes hediondos (Lei 8.072/90) e na hipótese específica de busca reversa de dados de pesquisa em buscadores da internet, a ordem judicial poderá se referir a pessoas indeterminadas, mas determináveis a partir de outros elementos de provas, obtidos previamente na investigação e que justifiquem objetivamente a medida, desde que necessária, adequada e proporcional, justificando-se, ainda, a inexistência de outros meios menos invasivos para obter tais informações e a conveniência da medida em relação à gravidade do delito investigado.

3) A determinação judicial conterà, com precisão, os indexadores utilizados para a busca pretendida na base de dados do provedor, devendo a suspeita estar suficiente e formalmente fundamentada, de maneira proporcional. **Esses indexadores podem envolver tanto as palavras-chave pesquisadas por indivíduos como determinações temporais da busca"**

4) A busca reversa e coletiva de dados de pesquisa não deve ser utilizada como primeira medida investigativa, sendo condicionada, ainda, à delimitação precisa dos termos e do período de busca, ao descarte dos dados de pessoas não vinculadas ao inquérito e à indicação das razões que justifiquem a proporcionalidade da medida por parte da autoridade policial ou do Ministério Público, com análise deste requisito na decisão judicial autorizativa.

É como voto.